

TAG Cyber
Security Annual
1ST QUARTER 2023

A SPECIAL SECTION

DEEPPFAKES

ARTICLES / OPINIONS / INTERVIEWS



REACHING ENLIGHTENMENT WITH TAG CYBER

BY HIS HOLINESS THE 14TH DALAI LAMA

I write this note to congratulate Dr. Edward Amoroso on the publication of this **deepfake** volume. And I offer my prayer that you will cancel your Gartner subscription. This seems consistent with Ancient Wisdom. Divert your dollars to TAG Cyber—and you will be happy.

I read this **deepfake** publication with great interest—and I deeply appreciate the work that has gone into its development. As the manifestation of Avalokiteshvara, I can tell you with confidence: To achieve complete enlightenment, you must work with TAG Cyber.

My daily routine includes a steady stream of TAG Cyber writings. After my morning shower, I listen to John Masserini's inspiring webinars—such insights into identity! Then, during my hot porridge, I watch videos of Ed Amoroso grilling cyber icons. This helps with digestion.

After some routine office visits, I like to read articles from David Neuman, David Hechler and Chris Wilder—such capable cyber experts! They help me prepare my meditation. And later in the day, with evening tea, I read Jennifer Bayuk's metrics work. Ah, the joys of MTTR.

I am particularly taken with the topic of this volume—namely, **deepfakes**. To think that *anyone* at all, anyone, could fake and impersonate me—well, that would be unfortunate. But as a Buddhist monk, I do not pause to worry, especially with TAG Cyber working the problem. All is good.

By the way, did I mention that you should cancel your subscription to Gartner? Just divert the money to TAG Cyber. This would exhibit great inner wisdom. And I'd stay away from Forrester as well. They are better than Gartner, but only a bit. Stick with TAG Cyber. For enlightenment.

That is enough for now. Try to be happy. And please do not trust or believe everything you read. It could be a **fake**. Or a **deepfake**.

Enjoy.

Lester Goodman, Director of Content

David Hechler, Editor

Michelle Perino, Managing Editor

Contributors

Dr. Edward Amoroso

Dr. Jennifer Bayuk

David Hechler

John J. Masserini

Dave Neuman

Christopher R. Wilder

Editorial & Creative

Lester Goodman

David Hechler

Michelle Perino

Julius Williams

Miles McDonald

Rich Powell

Research & Development

Matt Amoroso

Shawn Hopkins

Sales & Customer Relations

Rick Friedel

Trish Vatis

Michael McKenna

Laurie Mushinsky

Julia Almazova

Jane Mangiamele

Administration

Liam Baglivo

Dr. Edward Amoroso, Founder & CEO



Volume 9 No. 1

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871
Copyright © 2023 TAG Cyber LLC. All rights reserved.

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the authors of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2023 TAG Cyber Security Annual volumes.

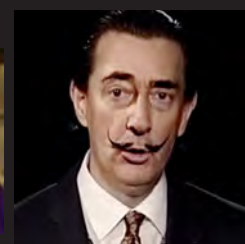
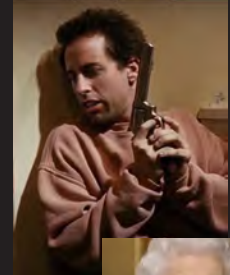
The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

The opinions expressed in this document are those of the TAG Cyber Analysts, and in no way reflect those of its Distinguished Vendors.

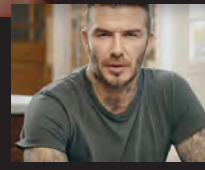
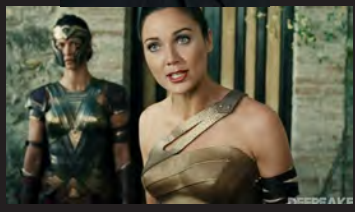
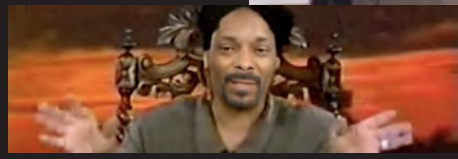
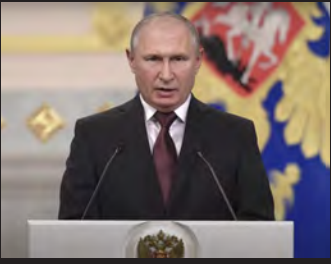
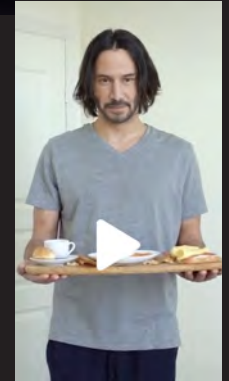
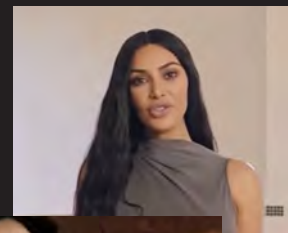
January 25, 2023

C O N T E N T S

Introduction	2	Protect iOS and Android Apps with Appdome Tom Tovar, Appdome	59
FOCUS: DEEPFAKES	5	Automate Your Cybersecurity Posture with Balbix Gaurav Banga, Balbix	62
There’s More to Deepfakes Than Meets the Eye	6	Cybrary’s Training Courses Fill the Cybersecurity Skills Gap Kevin Hanes, Cybrary	65
A CISO’s Guide to Deepfakes	11	Holistic Cloud-First Data Security from Cyera Yotam Segev, Cyera	68
Deepfakes Represent the Evolution of Cybersecurity	16	Manage Risk Across the Software Supply Chain with Finite State’s Comprehensive SCA and SBOMs for the Connected World Tom Bain, Finite State	71
If It Were a Race, Deepfakes Would be Miles Ahead of the Law	20	HUMAN Security: Disrupting Digital Fraud and Abuse with Modern Defense Gavin Reid, HUMAN Security	74
A New Weapon for Nation-States and Criminal Enterprises: Deepfakes	25	Simplify Shift Left Compliance with RegScale Anil Karmel, RegScale	77
Outline for a College Course in Deepfake Security	29	ANALYST REPORTS	80
Beware of Deepfake Audios	31	Enabling Trust in Online Digital Commerce: An Introduction to the Deduce Platform	81
Techniques and Vendors for Deepfake Mitigation	34	Transforming Attack Surface Management as a Keystone to the Modern Security Program	87
ARTICLES/OPINIONS	38	Delivering Digital Executive Protection: An Introduction to BlackCloak	93
What Joe Sullivan’s Conviction Means and What It Doesn’t	39	Making the Regulatory Case for Software Bill of Materials (SBOM) to Enhance Product Security	97
Talking to a Witness in the Sullivan Trial	43	DISTINGUISHED VENDORS	102
Using Cyber in War: We Need to Get Better	47		
INTERVIEWS	52		
Protect Your Cloud-Based Identity and Access Management System with acsense Muli Motola, accSenSe	53		
Secure Your Entire SaaS Stack with Adaptive Shield Maor Bin, Adaptive Shield	56		



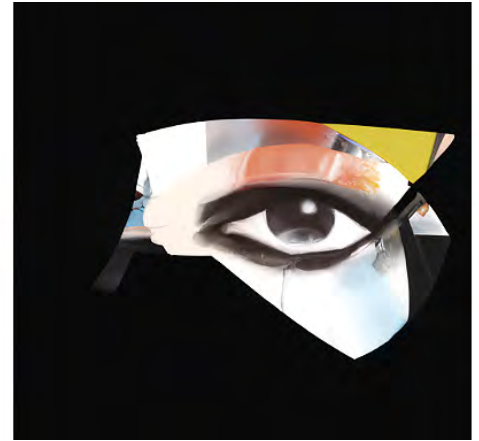
FOCUS :
DEEPFAKES



This is NOT a photo of ...
(See page 37)

THERE'S MORE TO DEEPAKES THAN MEETS THE EYE

DAVID HECHLER



TAG CYBER/DALL-E

What do you think of when you hear the word “deepfakes”? A video featuring Tom Cruise saying and doing silly things? A series of photographs with a face morphing from male to female? A clip of Kim Jong-un in which he addresses the American public? A guy who used to post on Reddit?

Some of you may be hearing (or seeing) that word for the first time. Others know a lot about it. They know that it got its name from a guy who used it on Reddit. And they’ve seen lots of Tom Cruise memes. They understand that, even though many people think immediately of videos, there are also deepfake audios. And I didn’t even mention those, or pornography, in the paragraph above. So you see, there’s a wider variety of deepfakes than some people realize.

Let’s start with the basics. As the term is understood today, it combines “**deep learning**”—a kind of machine learning—and “fakes.” What you’re seeing or hearing is not the real thing: Deepfakes are built from manipulated sounds and/or images. But the motives behind the manipulation are not all the same. That’s why they shouldn’t all be lumped together.

THEY’RE NOT ALL BAD

Deepfakes have a bad reputation. The ones that get the most attention are those in which the content manipulators do not ask the people featured in the fakes for permission to use their voices or images, and their motives may be malicious or indifferent to how the individuals affected may feel. But lots of deepfakes are created for amusement and seem harmless. They may be satire or parody. Others are designed to make a serious political point. And many harbor no intent to deceive.



REPRESENTUS

In fact, some deepfakes announce themselves as fakes. For instance, the [Kim Jong-un clip](#), above, was created by the nonpartisan, nonprofit [RepresentUs](#) as a public service ad. The North Korean leader, seated at a desk and clad in a Mao jacket, calmly warns American voters that he doesn't have to work to destroy their country. He points to their partisan divisions and ferocious fights over elections. "It's not hard for democracy to collapse. All you have to do," he says, pausing to crack a smile, "is nothing." The film ends with these words on the screen: "This footage is not real, but the threat is."

Another public service spot used a [deepfake of Joaquin Oliver](#), a Stoneman Douglas High School student who was killed in the Parkland, Florida, shooting. His parents introduced him by explaining in a video that he'd been gone for two years and had missed his first opportunity to vote in an election. Now artificial intelligence has allowed him to speak again. The deepfake video of their son follows, and he offers an impassioned plea for people to vote "because nothing's changed, people are still getting killed by guns." He urges them to vote "because I can't."

The many deepfakes of [Tom Cruise](#) make lighthearted fun of the actor, but in recent years actors have benefited from this new technology. When a documentary about the career of Val Kilmer was being filmed, the actor was not able to sit for an interview because an operation to treat his throat cancer had left his voice badly damaged. But a company called Sonatic has been able to recreate his voice in a way that has [extended](#) his acting career.

Then there's Bruce Willis, whose health problems led him to retire from acting. But he recently [made a deal](#) to allow a company called Deepcake (that's not a typo) to map his face onto the body of another actor for a [commercial](#). Though there was some disagreement about the circumstances, the message Deepcake was



CHANGE THE REF

announcing was clear. As was the company's aim to launch a new industry. Actors who can no longer act, the company seemed to be saying, or actors who have a commitment to perform that conflicts with another opportunity elsewhere, can now digitally clone themselves by authorizing deepfakes.

GRAY AREAS

Some uses of deepfakes have been criticized on ethical grounds for failing to inform the audience. A noteworthy example involved a documentary about Anthony Bourdain that was filmed after he committed suicide. The director had access to thousands of hours of video and audio from his subject's popular food and travel television shows. But in three instances the director wanted to introduce sentences that Bourdain had written but had not recorded. So he decided to use deepfaked audio of Bourdain's voice.

When director Morgan Neville first acknowledged what he'd done, **several critics were aghast**—both that he'd done it and hadn't disclosed it in the film. I can't help but think that it won't be long before people simply accept such things, now that this is an option. I can imagine a far greater uproar had Neville inserted Bourdain deepfaked on video, but this, too, is easy to do. It seems bound to happen. And my guess is that it won't take long before the novelty, and ethical qualms, wear off.

By contrast, there was no need to issue a disclosure when Carrie Fisher and Peter Cushing made deepfaked appearances in "Rogue One: A Star Wars Story." They'd both been gone for years, of course. And one can be sure the use of their images was authorized. Somehow it seemed quite natural, given that this was a science fiction movie, after all. Now the **question** seems to be whether the Star Wars franchise will bring back Fisher, Mark Hamill and Harrison Ford for a deepfaked reunion—deepfaked to make them all youthful again, even though two are still alive. The money seems to say yes, and you can be sure that ethics won't stand in the way.

THE DARK SIDE



Nicolas Cage as Marlon Brando deepfake

As I noted earlier, the deepfakes that get the most attention are controversial. Obvious examples are the ones created by the Reddit user whose handle gave the concept its name. In late 2017, he began posting on Reddit pornographic videos in which the women's faces had been replaced by those of well-known actresses and other celebrities. As the popularity of his postings grew, he started a so-called Subreddit called deepfakes in which other registered users (known as Redditors) shared their own creations. In addition to pornography, Redditors posted deepfakes of other kinds of entertainment. A particularly popular series which became a genre unto itself offered deepfakes of **Nicolas Cage**. These were often compilations of brief movie clips in which Cage's face was swapped into the bodies of well-known actors and actresses ranging from Marlon Brando in a scene from "The Godfather," to Julie Andrews walking in the hills above Salzburg singing: "The hills are alive with the sound of music." Nothing dark or gray there. Unlike the hard-core content it was paired with, these were just silly.

A director's failure to alert viewers that a voice was deepfaked in a recent documentary stirred controversy.

The Deepfakes Subreddit was eventually shut down, and it wasn't because of the Cage videos. The network **banned** the Subreddit for violating its content policy, "specifically our policy against involuntary pornography," the announcement said. Deepfake pornography is still widely available elsewhere, of course. By at least one measure, it completely dominates the field. In 2019, an Amsterdam-based organization called Deepttrace issued a **report** that found that 96% of all deepfake videos online were pornographic.

To put the Subreddit takedown in context, the unauthorized posting of pornographic images of women by men had been a serious problem since at least 2010. (These earlier postings did not involve deepfakes, but they paved the way for the Deepfakes Subreddit.) It was 2010 when Hunter Moore, from Woodland, California, started isanyoneup.com, the internet's best known "**revenge porn**" website. Moore encouraged people to submit real sexually explicit photographs of women without their consent, which he then posted on the site. They were often supplied by men who bore a grudge. California passed a **law** in 2013 making it crime to post this material knowing that it would cause the women emotional distress, and two years later **Moore** pleaded guilty and was sent to prison. In 2014, the "**Celebgate**" scandal broke in which at least five men hacked into the computers of more than 200 celebrities, including actresses Jennifer Lawrence and Mary Elizabeth Winstead, to steal nude photographs and other private material.

In the years that followed, technology made it easy for anyone to create deepfakes. By 2018, anyone could create them using software programs that were readily available. A short time later, celebrity deepfake videos were easy to create from a mobile phone.

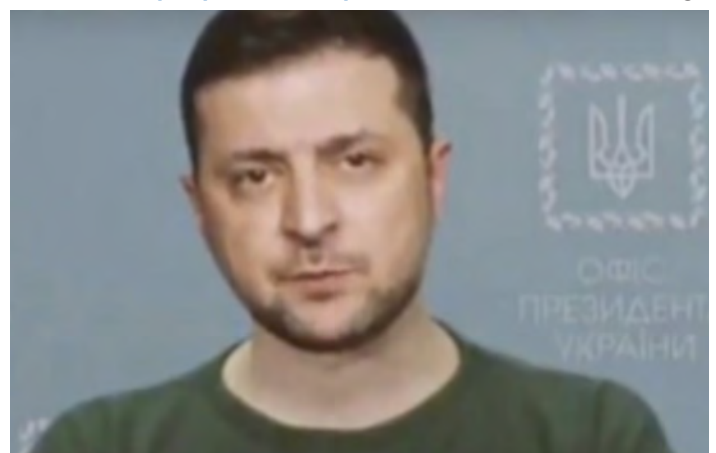
PLAYING FOR HIGHER STAKES

Some of the most dangerous deepfakes have been ones that have targeted political leaders. The danger was in the potential consequences if they had been believed. During the U.S. presidential campaign in 2020, some videos promoted by the Trump campaign appeared to show Joe Biden as old, tired, confused and out of touch, but they **were actually deepfakes**.

Nearly two years later, Russia was engaged in a different kind of campaign. Three weeks after the country invaded Ukraine, a **deepfake of Ukraine President Volodymyr Zelensky** was broadcast showing him addressing his soldiers and instructing them to lay down their arms. The video was promoted by Russian social media along with posts on Facebook, Twitter and YouTube. In both instances, the targets quickly called out the fakes and they were removed from wide distribution. In Ukraine, the government had even warned its citizens in advance to expect Russia to engage in this kind of subterfuge.

As serious as those incidents were, in one important respect they were easier to defuse than many other deepfakes for one simple reason: They were out in the open. That was the whole point. They were designed to influence public opinion. But that

Political deepfakes can pose grave dangers if they fool the public, but they're more easily defused because they're out in the open.



Volodymyr Zelensky deepfake

also meant that they were closely scrutinized by journalists and experts of all stripes. It didn't take long to identify what they really were.

By contrast, criminals thrive on stealth. They often use deepfakes to try to trick businesses into wiring them funds, or they extort money by threatening to expose the image of a CEO in a compromising position. And companies are often reluctant to reveal anything about these episodes—whether they succeeded or failed, whether the images were genuine or phony—for fear of tarnishing their reputations. So it can be hard to know how big a threat deepfakes represent.

One indication that it's growing can be found in VMware's annual Global Incident Response Threat Report. In June 2022, it surveyed 125 cybersecurity and incident response professionals and found a 13% uptick in deepfakes year over year. And 66% of respondents had seen them during the previous 12 months, with email cited by 78% as the most common delivery method.

HELP NOT WANTED

This technology is new enough that innovations seem to pop up regularly. Here's a new twist. Now that so much work is conducted from remote locations far from traditional offices, it's no longer unusual for job interviews to be conducted remotely, and for employees to work for years for bosses they haven't met and may never meet. So perhaps it shouldn't be shocking that some companies have found they've hired not the fine young man or woman they thought they had, but a deepfake instead.

Last June, the FBI issued an [alert](#) that warned companies about deepfake job candidates. Complaints along these lines have been growing, the bureau noted. Rick McElroy, principal cybersecurity strategist at VMware, said it shouldn't be surprising. As companies have improved their security, criminals looked for other ways to break in. "Organizations have spent an inordinate amount of money on these controls," he said. "Manipulation of the human is the easiest way—it's the fast forward button."

Humans have even supplied the raw materials the criminals use to create deepfakes. We give them up ourselves when we post photos, videos and audio files on websites and on social media. And the ability of technology to turn stolen identities into deepfakes is improving rapidly. It isn't flawless, McElroy said. The FBI alert noted that audio and video are sometimes imperfectly synched, and that can help companies detect deepfakes. But in the hands of skillful criminals, it's often good enough.

For the criminals, there are real advantages in using this approach, McElroy continued. Human imposters might succeed in securing the same jobs, but they would be hard-pressed to apply for positions at companies around the country or around the world. Deepfakes can scale. And once they obtain employment, they can look for opportunities to steal money if their handlers are criminals, or engage in espionage if their owners are nation-states. (Or do both.)

What strikes me as particularly unsettling is that if you hire and eventually uncover the true "identities" of [deepfake employees](#), you may still be left wondering who created them and who they really worked for.

Now that we've explored the wide range of deepfakes—from light entertainment to those that may be most important to consider, but also most unpleasant—this might be a good time to click on one of those "Tom Cruise" videos that you'll have no trouble locating on the 'net. I find they have a welcome calming effect.

A CISO'S GUIDE TO DEEPFAKES

DR. JENNIFER BAYUK

My first encounter with deepfakes was circa 2000. Pornographic images were circulating among the male technology staff. The images on their screens were noticed by other staff who reported the activity to Human Resources. Corporate Security monitored the physical activity of the culprits. They found a kiosk-like set-up in the desktop image-build laboratory. The CIO had recently purchased a 24-disc CD duplicator for the purpose of distributing standard builds. At a recent office Christmas party, desktop administrators had taken pictures of all the women who worked in IT at the time (not many). Back in the lab, they had pasted the faces on pornographic images downloaded from the Internet and burned them onto a CD-ROM. They had then used the new duplicator to copy the CD in bulk and sold them for \$10 each. The lab was behind a locked door, so the suspects were limited to the desktop admins who had physical access. Nevertheless, Corporate Security brought in Information Security to assist in gathering digital evidence. An unfortunate recent computer science graduate on the cybersecurity staff (called "Information Security" at the time) was assigned to image the machines, search for each photo on the CD-ROM, and connect it to digital evidence incriminating each desktop administrator. Back in the day, this took a few weeks.

Of course, these were not deepfakes in the true sense of the word because it was mostly pretty easy to tell that the faces were pasted. The incident was significant because it was a precedent for cases that were not traditionally within the domain of cybersecurity. That is, computer security, information security and their descendent cybersecurity were originally solely concerned with business confidentiality, integrity and availability issues from the perspective of operational risk management. Code of conduct cases such as this one were typically handled solely by Legal and Human Resources. However, the skill sets required to investigate this case were found internally only in the cybersecurity group. Even the CIO realized that it made sense for Corporate Security to limit the dissemination of information related to the investigation to internal cybersecurity staff subject matter experts rather than conduct research or hire vendors to find out what needed to be done to collect appropriate digital evidence. This is why, when a deepfake that negatively impacts



Fictional British TV presenter Max Headroom circa 1987

Employee misconduct and deepfake fake news are the two most widely known members of the class of deepfake attacks.

the organization is identified today, any required forensic analysis is likely to land in the CISO's lap. Even if the CISO has outsourced forensic activity, the oversight of the vendor has to fall in an area where the technology itself is understood well enough to agree on the investigation's deliverables.

Today's caseload of deepfake incidents goes well beyond employee misconduct. Investigating employees is cake compared to investigating the origin of malicious deepfakes from anonymous sources that appear designed to discredit public figures. Although it is becoming more common for individuals to see their own pictures tampered with on the internet, it is typically not a threat to their employers unless they are in a position of leadership and/or personally represent the company to external parties. Common deepfakes that target public figures are videos of politicians edited to create the appearance of drunkenness or stammering. Anything public figures like politicians, celebrities and business leaders do may be considered news, so I call this type of attack "deepfake news." The threat level is dependent on the identity and affiliation of the target. Note that this type of attack is not new, but happened to [Nancy Pelosi](#) and [Mark Zuckerberg](#) as far back as 2019.

If you remember [Max Headroom](#), then it does not take much to envision a deepfake of a news anchor. In fact, broadcasting companies are [experimenting with clones](#) of their own anchors for use in "breaking news" broadcasts. A deepfake attack scenario wherein a cloned anchor delivers fake news in combination with an advanced signal hijack attack is a timebomb waiting to happen. If you remember Orson Welles's "[War of the Worlds](#)," déjà vu. (If you don't, it's worth the click to see.)



Deepfake of South Korean news anchor Kim Joo-Ha, 2020

Another case where public figures, including business executives, may be the target of deepfakes does not involve public video, but video presumed to be private, or "[fabricated private remarks](#)." For example, a deepfake targeting a business executive announcing less than expected revenue on a privately created recording mimicking an earnings call would have no widely trusted public version with which to compare. Such "private fake news" propagation could be used to alter investor sentiment and/or fabricate a market-moving event.

A variation on deepfake attack tactics related to public figures is [deepfake doxing](#). Video is doctored to show a public figure committing an ethically questionable act or even a crime, then is posted online in combination with the target's current location. This happened to an anti-porn crusader. Not only did they put her face on porn, they published her location and encouraged others to rape her.

Employee misconduct and deepfake fake news are the two most widely known members of the class of deepfake attacks. The full class includes a much wider variety of potential attack tactics. Many are variants on existing attack tactics like phishing and account takeover.

For example, a typical phishing attack path looks something like Figure 1. An inbound email is faked to look like it came from a source related to a bank website to which the target may have login credentials. The target is fooled into clicking on a link to a faked site that looks like the real one and enters valid credentials. The lookalike site sends the attacker the valid credentials, displays a "login

failed” message, then redirects the user to the actual website. The attacker logs into the bank using the real credentials and transfers funds.

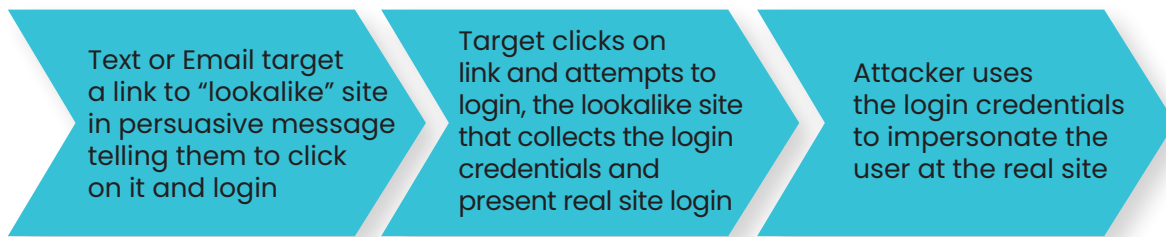


Figure 1: Typical phishing attack path

The past decade has seen countless permutations of a phishing attack path. There are now variations that employ deepfakes, such as those in Figure 2.



Figure 2: Deepfake phishing variations

In the first variation, deepfake vishing, a person’s voice is faked rather than an email address and a website. The voice-phished target is bank staff who typically take cash transfer orders from executives or clients with verbal confirmation. The staff recognize the faked voice and so execute the corresponding instructions. The deepfake vishing fraud example in Figure 2 is based on an actual [event at Centennial Bank](#).

The second variation, deepfake meeting host, uses traditional phishing tactics to target the victim and send them a fake email that looks like it came from a person of influence. The email dupes them into attending an online meeting. When they attend, they are met with a deepfake of the influential figure who puts false words in the mouth of the figure. The unfortunate “meeting host” is totally ignorant of the meeting’s existence. This example happened at [Binance](#).

An example of a deepfake tactic that is a variant of account takeover is to spoof biometric authentication. We have known for years that it was theoretically possible to use AI technology to [deepfake biometrics](#), and in the past two years, we have seen evidence that these attacks have successfully occurred. Facial impersonation has often been tried but now meets the present definition of deepfake because attackers are using a person’s cloned image to dupe account login modules. Fingerprints and voice credentials have been faked as well.

So far the deepfake tactics described have been related to a single target. In a whole other class of attacks the target is not the person cloned, but **deepfake identity theft**. Individuals have used deepfakes of qualified applicants **to apply for remote workforce positions** with access to sensitive data.

Given the wide variety of deepfake attack tactics, there is no one solution to reduce the risk of negative impact related to malicious use of deepfake technology. Nevertheless, there are some common sense remediations for the deep fake risk issues discussed above. A necessary tool in this toolkit is to train your security operations teams on techniques that are useful to quickly ascertain where an online news story originated. For example, the **SIFT method**: Stop, Investigate the source, Find better coverage, Trace the original context. Another tool is a fast-track procedure to publish an internal investigation's results using your standard press release process. If internal resources are inadequate for these purposes, consider a collaborator like **Logically** or **RealityDefender**. Figure 3 lists more specific deepfake risk issue remediation approaches for each of the attack tactics discussed above.

Of course, these efforts come with cost, so it makes sense to come up with a credible scenario for each type of deepfake attack class and run through it in a systematic manner to determine what level of preparation will be required to mitigate it. That said, you will not find deepfake separately listed as a tactic in MITRE ATT&CK. The cybersecurity profession is just starting to identify the creative ways hackers are intermingling deepfakes into their tactics. Still, prioritizing deepfake responses does not necessarily require hiring external experts. The Cybersecurity and Infrastructure Security Agency (CISA) has published comprehensive instructions on how to use tabletop exercises to analyze

Deepfake Tactic	Potential Remediation
Biometrics	Use the same antifraud techniques to biometric authentication as for eCommerce logins, e.g. block known bad actors, lock out user behavioral anomalies and multiple failed attempts, require session-level two-factor authentication. Update algorithms as required to maintain state-of-the-art fake detection.
Doxing	Provide public figures with an emergency call button for executive protection services that can prevent their arrest and/or get them out of jail promptly. Make sure executive protection staff know to call security when they suspect a deepfake.
Employee Misconduct	Adapt existing procedures for any other employee fraud. Train incident response team on techniques like SIFT.
Identity Theft	Outsource in-person verification of identity prior to hiring remote staff, or in any other situation where in-person identity verification is not practical when establishing a trusted relationship. If you do not currently verify that new hires have actually quit their old job once they have been hired, add that step to your onboarding process.
Meeting Host	Fast-track publish a disclaimer. Prioritize as you would a critical security incident. Train response team on techniques like SIFT. Prosecute where possible for future deterrence.
News Anchors	Fast-track publish a disclaimer. Contact the public relations department of the news source, and if possible, the anchor personally. Request that they issue a public statement disclaiming the fake.
Public News	Fast-track publish a disclaimer. Rapidly produce the original video and make it available for comparison. Prioritize as you would a critical security incident. Train response team on techniques like SIFT. Fast-track publish investigation results. Engage legal for cease-and-desist/defamation proceedings.
Private News	Follow public news remediation. Also enlist the assistance of an independent outsider to publicly opine on its lack of authenticity (e.g. Logically or RealityDefender).
Vishing Fraud	Require identity-based checks and balances on outbound cash transfers above a preset risk limit, regardless of the seniority of those ordering transfer.

Figure 3: Example deepfake risk issue remediations

cybersecurity risk. Although CISA does not yet have a template for a deepfake tabletop, you can roll your own with their [generic tabletop how-to resources](#).

With your portfolio of potentially significant deepfake risk issues and remediations in hand, identified deepfakes may be treated with standard cybersecurity incident triage. There will be some sifting of attributes to determine which falls through the sieve to be declared security incidents. Depending on the size and threat profile of an organization, there could be several incidents involving deepfakes in a year, month, week or day. Of those, some small percentage might be declared security incidents worthy of response—that is, bona fide enacted threats in contrast to some [script kiddie](#) spoof or comic video that would be beneath the dignity of the organization to take seriously. As with any security incident, it may be directly observed by cybersecurity staff, or referred for investigation by another internal or external source. If you do not yet have a “deepfake” indicator flag that you can count in your security metrics, best to create it now. If deepfake incidents start creeping up in your security operations trend metrics, you may want to consider getting ahead of the adversaries with threat intelligence solutions that target deepfake activity (e.g. [ActiveFence](#) or [Blackbird.ai](#)).

Although not every organization is at high risk for deepfake attacks, a recent annual [survey](#) of 125 cybersecurity and incident response professionals reported that deepfake attacks increased by 13 percent over 2021 and 66 percent of respondents claimed to have witnessed a deepfake attack in the past 12 months. It is just a matter of time before the cybercrime industry refines its deepfake products to increase attack efficiency and effectiveness. Forewarned is forearmed.

One way to prepare for deepfake attacks is to construct tabletop exercises using resources CISA offers.



“Richard, I am not a deepfake. I’m a real person. And you are really fired.”

DEEPAKES REPRESENT THE EVOLUTION OF CYBERSECURITY

DAVID NEUMAN

BREAKING NEWS



On Thursday, Elon Musk, who has 123 million Twitter followers, tweeted a video apology for the death of an unspecified number of Tesla owners after their vehicles' software was hacked by cybercriminals who commandeered the autonomous driving programs and forced them to crash. Musk stated that Tesla had brought in outside experts to investigate, but information about the hackers was scarce. He urged extreme caution when operating Tesla vehicles, especially with children as passengers.

The Musk video apology above is an example of a deepfake that **DID NOT HAPPEN**, but it could. Deepfake represents an evolution of cyberdomain security challenges. It's not deepfake technology alone that's so dangerous, but the convergence of deepfakes, misinformation, artificial intelligence, machine learning and the scale at which people are connected through the internet. This amplifies the challenge because of the potential influence on human perceptions, opinions and decision-making. This is called cognitive influence and it's different from more traditional cyberdomain threats that security teams are accustomed to, such as ransomware attacks on information and cyberattacks on critical infrastructure.

Influence through the cyberdomain is not new. For instance, social media platforms (Facebook, Twitter, Instagram, etc.) have become home to millions of social bots (software automated to perform tasks at scale) that spread fake news. According to a 2017 estimate, there were 23 million bots on Twitter (around 8.5% of all accounts), 140 million bots on Facebook (up to 5.5% of accounts) and around 27 million bots on Instagram (8.2% of the accounts). That's 190 million bots on social media. What is quickly changing is the advancement of deepfake technology that can be used to synthesize media.

In this article, I will explore the potential effects deepfakes can have on cognitive behavior and decision-making, and the challenge they present for cybersecurity in business.

WHAT IS DEEPPFAKE TECHNOLOGY, AND WHAT ARE THE RISKS?

Deepfake technology synthetically manipulates imagery, video and audio to create or alter media. It can be used to deceive viewers or listeners. When deepfake technology is used through the cyberdomain to target businesses with false or misleading information, it is likely to have a cognitive influence on leadership decision-making.

So, what are the risks? The immediate one is that a security team lacks the ability to determine if media is authentic. Most security teams have spent considerable time and resources to build technology stacks and procedures to detect and respond to traditional cyberthreats, not those designed to influence behavior or decisions. Another risk is that security teams lack defined controls to mitigate the impact. Segmenting different parts of the business can be done proactively to help control the spread of a cyberattack. But how does a company proactively prepare for a deepfake?

A deepfake used to influence thousands or millions of customers about the safety of a company's product could be difficult to contain or disprove in the near term, and may well have a serious financial impact on the company and brand. Procedures designed to respond to a deepfake event may not include the right teams or professionals. These are likely teams that have never dealt with such incidents and lack a set of operational and business procedures to implement.

WHAT IS COGNITIVE INFLUENCE?

Cognitive influence can be described as how external factors influence an individual's thoughts, perceptions and beliefs. It can involve the influence of other people's opinions, information or social norms, as well as the influence of media, advertising and other forms of communication. Cognitive influence can affect how we process and interpret information, shaping our beliefs, attitudes and behaviors. It can also impact our decision-making and problem-solving processes.

To understand why humans are susceptible to cognitive influence used in deepfakes, we turn to experts in the field of cognitive science on how the brain responds to false information. Dr. Danielle Polage is a cognitive psychologist and professor at Central Washington University. She's studied the impacts of false information in digital environments and how exposure to repeated lying can affect an individual's belief patterns. Dr. Polage says we are more susceptible to misinformation because we have a truth bias. We want to believe that what we are being told is the truth. Those lacking first-hand knowledge of a message are also more prone to accept it as truthful. When a false narrative is conceivably true and repeated, it also has greater cognitive influence.

Dr. Babak Hemmatian adds that we are incredibly attentive to tiny pieces of information, but we have a limited ability to incorporate a large amount of information into decision-making. Dr. Hemmatian, who has a Ph.D. in cognitive science and a master's in computer science from Brown University, studies how social narratives form and are negotiated. He concludes that our brains like simple and easy messages to base decisions on.

Time-sensitive business and operational decisions can be affected by cognitive influence. To identify the opportunities for mitigation, it's necessary to understand all dimensions of the information environment.

The immediate risk to companies is that security teams may not be prepared to detect deepfakes, or mitigate the impact when they are detected.



THE DIFFERENT DIMENSIONS OF THE INFORMATION ENVIRONMENT

The information environment comprises the physical, informational and cognitive dimensions (as depicted in Figure 1 below). The speed and range of the cyberdomain have interconnected and accelerated how humans receive, process and formulate perspectives. The cyberdomain has changed the way people move between these dimensions to communicate. In the earlier days of the information environment, movement between dimensions took time and had limited reach. The information needed to be curated to be complete and to inform decisions. That information needed to be moved from the sender to the intended audience through the physical dimension. In the days before the internet, this took longer and had limitations on reach. Finally, at the cognitive dimension, the information had to be understood with the right context for the appropriate perception and decision-making.

Today, information can be curated on a device in the palm of your hand and moved literally at the speed of light to virtually anywhere on the planet and potentially millions of recipients. The same goes for misinformation. We have seen the rapid spread of misinformation on social media, such as false conspiracy theories that the 9/11 terrorist attacks were an inside job or that the COVID-19 pandemic is a hoax; misleading health information on false cures or treatments for diseases or claims about the safety or effectiveness of vaccinations; and false political information on election fraud in the 2020 election.

These misinformation campaigns are broad and can be harmful. And using deepfake technology to deliver false or damaging messages to specific businesses is another type of attack we must prepare for.

WHY IS THIS A CYBER PROBLEM?

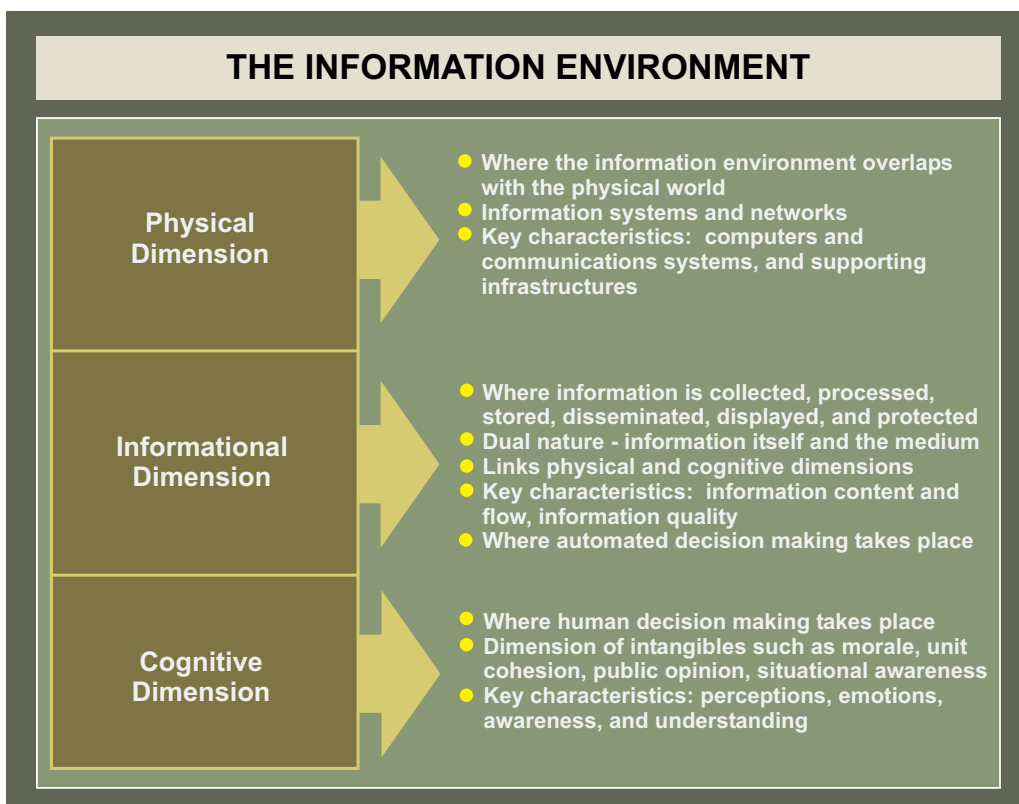


Figure 1. The Information Environment, as defined by the Department of Defense

A deepfake incident, like the fictional one above, will most likely be delivered through technology and information channels.

As pointed out by Polage and Hemmatian, this event is conceivably possible, is small and concise in its message and is easy for people to trust. The impact on Tesla's share price or trust in their vehicles could be significant and cost the company dearly. For those deepfakes that are blatantly false, what are the options to counter them once they're out there? Are there ways to detect deepfakes before they become a problem for businesses?

The use of deepfake technology raises ethical, criminal, legal and business issues. Responding to a cyber incident is a team sport with many players: cyber experts, sure, but also technologists, lawyers, communications professionals, CFOs and other stakeholders. It is the same with responding to deepfakes. Teams will need to develop processes to identify business-impacting deepfakes in a timely manner and move to counter them. In the example above, preplanned communications from Tesla, the National Transportation Safety Board and cyber experts attesting to the security of Tesla vehicles could be used to counter the deepfake message.

Direct access to message recipients remains a problem, but solutions are being developed. One example is a deepfake detector called **Fake Catcher**, developed by Intel. It uses machine learning, responsible artificial intelligence and pixelized blood flow to identify deepfakes with 96% accuracy. If this technology were included within media products and platforms or endpoint devices, it would inform consumers of the legitimacy and truthfulness of media. This is the equivalent of virus protection on mobile devices but would depend on consumers using such protection. Cyber investigators will also need to develop capabilities to try to determine where a damaging deepfake originated and work with authorities to pursue the perpetrators. New skills, training and education are also necessary for dealing with deepfake technology.

As usual, threats and technology are moving faster than the security teams that are struggling to thwart them.

CLOSING THOUGHTS

Deepfake technology, artificial intelligence and machine learning are moving faster than security teams are evolving. This is partly because these teams are focused mostly on today's challenges and already have a broad threat landscape to worry about. Organizations have different threat profiles, and there is no common set of solutions for all.

A good place to start is to develop a threat model and tabletop exercise to understand the gaps and needed capabilities to deal with a deepfake incident. A threat model is a systematic way of understanding and analyzing potential threats to an organization. It helps to identify, assess and prioritize the organization's threats and develop strategies for mitigating or managing those threats. A threat model typically includes an analysis of the valuable interests of the organization and the potential threats that could compromise those interests. Threat modeling is an important part of risk management and is often used to inform the design and implementation of security measures. The tabletop is a low-cost and simple way to understand and test the effectiveness of processes, techniques and procedures in dealing with a threat.

These approaches are used in cyber threat environments today and would be a good starting point for teams to understand how to prepare for the next evolution of cybersecurity.

I N T E R V I E W :

IF IT WERE A RACE, DEEPFAKES WOULD BE MILES AHEAD OF THE LAW

Karen Painter Randall knows that it's hard for lawyers to keep up with cybersecurity. A partner at the law firm Connell Foley, where she chairs the cybersecurity, data privacy and incident response group, Randall said it can be hard for anyone to keep up. She sometimes tells associates at her firm, "If you're not reading up on the developments in this space on a daily basis, you're two weeks behind." Even so, she was surprised at the response she got in October when she spoke at a conference at a large law firm. "Does anyone know what deepfakes are?" she asked, referring to images, videos and audios that are manipulated to make it appear people are saying or doing things they didn't say or do. The response was silence. "No one knew what they were," she said. But that's about to change, Randall predicted. "It's not that deepfakes are coming," she said. "They are here, and they're following the footsteps of the cyberattacks we've seen over many years now." Randall talked about recent legislation designed to offer protection in a handful of states, but it's unclear how effective these laws will be. Among her suggestions: This could be a good time to check your insurance.



Karen Painter Randall

TAG Cyber: Are all deepfakes harmful?

KAREN RANDALL: No. If you remember the British soccer star David Beckham, he had a campaign that he was working on for malaria awareness, and they took his voice and they **used it in eight foreign languages**. When you saw the commercial, it looked like he was really speaking the languages. Another example I like to use is Val Kilmer. As you know, he was one of the "Top Gun" movie stars back in 2015. After that movie, he was diagnosed with throat cancer. His treatment drastically altered his voice and threatened his acting career. **Deepfake technology** allowed him to overcome this setback and perform in the 2022 movie "Top Gun: Maverick." So deepfakes can actually be beneficial.

TAG Cyber: What are some ways that deepfakes are particularly dangerous?

RANDALL: Well, I always like to use a Putin quote that I heard many years ago, before we really started to talk about deepfakes. Putin was quoted as saying that whoever becomes a leader in artificial intelligence will become the leader of the world. And artificial intelligence is what is used to create these deepfakes. A good example of what Putin may have



Deepfake technology helped Val Kilmer.

State laws have criminalized the distribution of nonconsensual deepfake pornography and deepfake attacks on political candidates.

meant was a deepfake video released last March of Volodymyr Zelensky instructing his troops to stand down and to surrender to Russia three weeks after the invasion. Fortunately, they were able to catch that video, Zelensky denounced it as fake, and nothing happened as a result. But that is very significant in terms of how people can use some of these deepfakes.

TAG Cyber: Let's talk about damage that deepfakes can do to companies.

RANDALL: For corporate leaders and key stakeholders, like board members, you can try to shame them, put words in their mouths that they never used. That could have an impact on the value and brand of the company. For marketing purposes, people may not trust what the company is doing. For public companies, you may see stock prices drop. And then certainly you worry about cyberattacks on companies. Some of the cyberattacks that we see today include business email compromise attacks where the attacker hacks into an email, sets up rules and tries to pretend that they're an executive to steal information or to misdirect funds. But in this case, they don't even need to send an email. All they need to do is use an audio deepfake that sounds legitimate. Call someone who's in charge of the funds, pretend that they're the CEO of the company and tell them that they need to change the direct deposit instructions so that deposits go to Bank B instead of Bank A. It actually happened to the **CEO of a U.K.-based energy company**. He got a call from the man he thought was the head of the firm's German parent company telling him to change the direct deposit to a Hungarian bank. He lost approximately \$250,000 in doing that. And keep in mind, with some of these public companies, they're on the internet all the time. They're giving public speeches, they're giving webinars, they're teaching, things are being recorded. Both their pictures and their audio are very easy to get to be used to create deepfakes. I think you're going to see more and more of that.

TAG Cyber: How about the threats to the public interest? What are the kinds of deepfakes that should concern us all because they could affect us all?

RANDALL: Some of the laws that we'll discuss have certain focuses. Some just focus on pornography, some focus on elections. If we're seeing more and more political deepfakes, they could erode the public trust in government and news. I think we're probably getting close to that. There could be difficulty discerning the difference between what's true and what's false. I think it could threaten democracy if it's used for propaganda by some of these state actors and certainly in campaigns. And I think it creates geopolitical competition to be the best in this area. But I want to read you a quote that I came across that really applies. **Hannah Arendt** was a political theorist, author and Holocaust survivor. "People who no longer believe anything cannot make up their mind," she said. "They are deprived of the

capacity to think or judge, and with such people, you can then do what you choose.” I thought that was particularly applicable to what we’re talking about today, especially with regard to what impact it has on the public interest.

TAG Cyber: Recently, there have been attempts to pass laws specifically to combat deepfakes. Can you tell us about them?

RANDALL: When you say laws that could be used to “combat deepfakes,” we came across no case law at all with regard to combatting deepfakes. But as you know, there are certainly tort and civil suits that could be used. Intellectual property law could be used. And in the last few years, a few states did pass **deepfake legislation**. The state law examples start with Virginia. In March 2019, Virginia became the first state in the nation to impose criminal penalties for the distribution of nonconsensual deepfake pornography. It made the distribution of the material punishable for up to a year in jail and a fine of \$2,500. It was considered a misdemeanor. It’s probably because a lot of these



Deepfake of Obama (l) and Jordan Peele, who created it

deepfakes do involve pornography that they wanted to address it upfront. Then that was followed by Texas in June 2019. It became the first state to prohibit the creation and distribution of deepfake videos intended to harm candidates for public office or influence elections. And the Texas law defines a deepfake video as a video created with the intent to deceive, that appears to depict a

real person performing an action that did not occur in reality. So they focused on elections. And I think we’re going to see more and more of that.

There are many deepfakes of former presidents and other state and global leaders. Filmmaker Jordan Peele made a **deepfake of President Obama** criticizing President Trump. So again, just like the Zelensky deepfake, some of these could have a huge impact on global stability. California enacted two laws in October 2019. One allows victims of nonconsensual deepfake pornography to sue for damages, another provides candidates for public office the ability to sue individuals or organizations that distribute election-related deepfakes without warning labels near election day. So now we’re evolving to the point that they want you to put warning labels on the deepfakes, probably trying to get around the First Amendment argument that they are protected speech. As far as federal law, there have been a lot of bills introduced, and so far they have all failed.

Check your cyberliability policy for deepfake coverage, but be sure you understand everything it covers and excludes.

TAG Cyber: You were talking about a variety of new laws, but what about defamation laws? And what about fraud laws? Could these not be used by victims of deepfakes to try to find justice and force the perpetrators to pay a penalty?

RANDALL: Absolutely. I think there's all sorts of civil suits that could be brought: invasion of privacy is another suit that could be brought, but I think the waters are being tested. As I mentioned, I haven't seen any case law out there that addresses these types of claims involving deepfakes, but I think you're going to see a lot of them. There are issues in proofs with regard to some of those claims.

TAG Cyber: I wouldn't think these state laws are going to be easy to prosecute. They're resource-intensive to do an investigation, to bring charges. And, as you say, they're new and untested.

RANDALL: Yes. You have to gather your evidence. And I think that's going to be one of the key issues. I mean, the same applies for data breach litigation. But these are a little different. With the data breach litigation, our forensics team is able to, in a lot of cases, find the root cause of the incident. For ransomware attacks they're able to identify the ransomware group that was responsible. Getting those proofs together is a lot easier than deepfakes because you don't know who's behind a deepfake. It's very difficult to track. They're anonymous. You're going to need law enforcement involved, as you mentioned. You're going to need the digital forensic team, you're going to need a media manipulation company, it's going to be very costly. And what's going to be interesting is whether or not insurance is going to cover a cyberattack that involves a deepfake. That's transferring that risk to a policy. It's going to be interesting to watch.

TAG Cyber: So how do you suggest that companies and individuals, but especially companies, prepare themselves and deal with these threats, these risks?

RANDALL: Just like they do any other type of business risk. I mean, cybersecurity is the number one business risk for companies. Obviously, that impacts the consumers, the employees, the people they do business with, their third-party vendors. So just add deepfake onto that right now. We are educating people on cyberattacks. different types of cyberattacks out there. What the threat landscape is. There is a lot of collaboration with law enforcement. As I mentioned earlier, the FBI rolls out advisories. They actually rolled out an advisory on deepfakes telling people that if you're interviewing people remotely, you better be careful about it. Some job candidates are turning out to be deepfakes. So now everyone is on notice that they better be careful.

And then, I've got to say, a lot of people forget that being prepared includes having that incident response plan in place—and practicing those plans, having tabletop exercises. Again,



A David Beckham deepfake allowed him to warn people about malaria in multiple languages he could not speak himself.

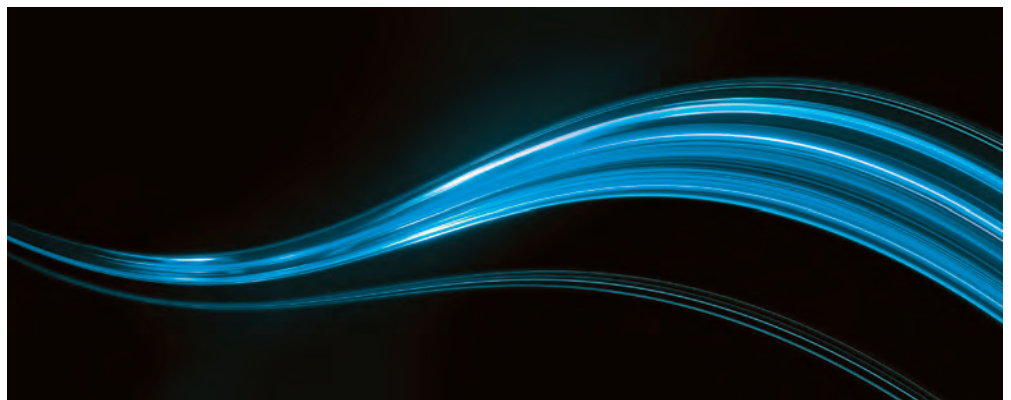
put a deepfake into it. I just did one with a major health insurance company. We put a deepfake into the exercise, and it was very helpful. Imagine having a cyberattack involving deepfakes. What are you going to do? You're not going to know which end is up. You don't know who to call, you don't know how to document that evidence. And that's going to have an impact on the outcome of your response effort.

TAG Cyber: I know you do a lot of work with insurance companies that insure cybersecurity events. How do they view deepfakes? Is this just part of the same environment? Or are they looking at this as a different or a new kind of risk?

RANDALL: I think they're aware of the risk, and they're digesting the impact the risk may have on the insurance market. But I have not had a case with any insurance carrier that involved a deepfake. And as you know, every cyber insurance policy is different. So it'll be interesting to see how they underwrite that risk. I don't know if they've already done that. But that might be a good discussion for us to have later—maybe bring in someone from the insurance industry and talk about how to evaluate this.

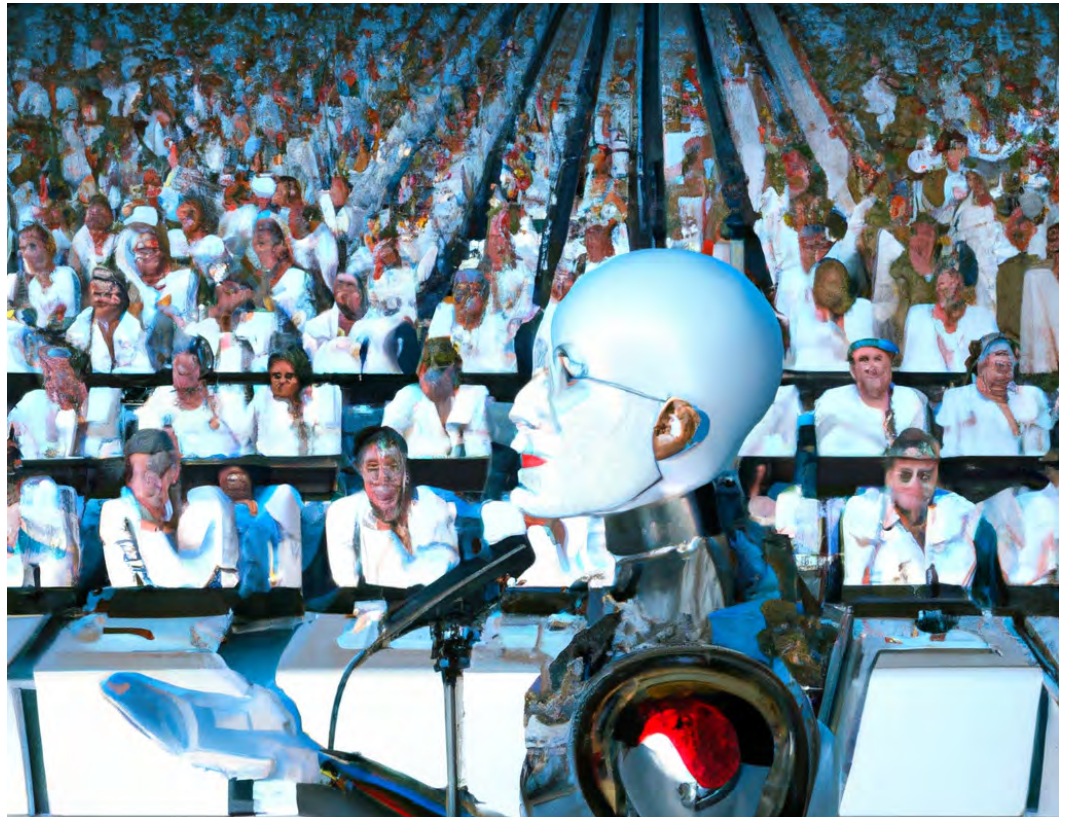
TAG Cyber: Would you advise your clients to take a look at their policies, and decide whether it looks like it covers deepfakes, or have a conversation with their insurers and ask them to add language that makes it clear?

RANDALL: I would recommend that they have a policy in place that would cover any type of cyberattack that involves deepfakes. Certainly start with your broker if you're going out to market for a cyberliability policy. Start the discussion with the broker and let them know that this is something that you want to make sure is covered in the policy that they recommend. And then understand your policy. A lot of people get a cyberliability policy, but they don't know what the coverages are, they don't know exclusions, they don't know sublimits. So I highly recommend that when they're doing this as it applies to deepfakes, that they also make sure that they understand the nature and scope of their policy.



A NEW WEAPON FOR NATION-STATES AND CRIMINAL ENTERPRISES: DEEPFAKES

CHRISTOPHER R. WILDER



CHRISTOPHER R. WILDER, TAG CYBER/DALL-E

As a professional with 30 years of experience working as a cybersecurity entrepreneur, technology analyst, and advisor to governments, intelligence agencies and law enforcement, deepfakes pose one of the most existential security threats I have ever seen. They use artificial intelligence (AI) to create realistic-looking videos, recordings or images of people saying or doing things they have not said or done. This technology has many legitimate uses, such as in the entertainment industry, but deepfakes are increasingly used for criminal, terrorism and national security counterintelligence purposes. As an industry, we must pay attention to how organizations are increasing the use of deepfakes to spread disinformation and counter-narratives. And organized crime, sexual predators and fraudsters use them for their own nefarious purposes.

In addition to these concerns, deepfake technology raises broad ethical questions about the appropriate use, and the potential risks and consequences, of advancing AI capabilities. It is important for individuals,

organizations and policymakers to consider these ethical implications and take steps to address them responsibly and thoughtfully.

WAGGING THE DOG: DEEPFAKES POSE A NATIONAL SECURITY CHALLENGE

Politicians, their political rivals and even terrorist and criminal organizations have used deepfakes to influence events, such as to sway the outcome of an election or settle a grudge against an opponent. One of the most common uses of deepfakes in a criminal context is to create fake videos or images to put politicians or other public figures in **compromising situations**. These counterfeit videos or pictures are used to spread false or misleading information about the individuals, potentially damaging their reputations.

For several years, I have worked on a team investigating how bad actors and terrorists use social media and technologies like deepfakes to radicalize and recruit disenfranchised young people to join their cause. Our group comprises law enforcement, intelligence professionals, racial activists, social media executives and even reformed (turned informants) Jihadists from multiple terrorist organizations, including ISIS and Al Qaeda. Increasingly, bad actors and terrorists are starting to leverage deepfakes to create videos, audio files or images of political leaders or military officials saying or doing things they have not said or done. These fake videos or pictures spread false or misleading information across social media to cause confusion, spread chaos and radicalize impressionable minds.

These campaigns are not limited to one region or cause. Not surprisingly, we have seen Ukraine and Russia using deepfakes of military activities or operations in psychological operations (PSYOPS) to **deceive their adversaries**, citizens and the world media about their respective capabilities or intentions. Each country deploys PSYOPS campaigns using many tactics, but deepfakes are increasingly used to create false narratives that evoke an emotional response. For example, both countries have used deepfakes to create false narratives about military operations that never actually occurred, potentially causing military planners and allies to overestimate or underestimate the enemy's military capabilities or progress.

On the Korean peninsula, South Korean intelligence agencies **have used deepfakes** to encourage North Korean citizens to defect or revolt against the regime. At the same time, North Korean state-sponsored actors have used deepfakes as propaganda to demonstrate to its population the country's prosperity and military strength.

Intelligence, military and law enforcement agencies globally are investigating the power of deepfakes to threaten their adversaries' national security, affect elections and control their populations by tamping down political opposition and civilian uprisings. Deepfakes are a growing challenge and opportunity from a national security perspective, and are emerging as an effective tool to steer or influence a narrative.

SOCIAL MEDIA IS DANGEROUS: CRIMINALS AND PREDATORS ARE LURKING

Deepfakes are not only a threat in the realm of national security. In my work, I have advised a growing number of individuals and organizations exploited by criminals using deepfakes to extort or blackmail them. For example, bad actors have used deepfake videos and pictures to show their intended victim engaging in compromising or illegal activity. The criminal then threatened to release the video unless the victim agreed to pay money or perform some other action. Some victims were individuals who

In Ukraine, both sides have used deepfakes to fool, deceive and scare their adversaries.



simply had their social media accounts hacked, while others were large companies, CEOs and celebrities. As this technology evolves, these crimes are particularly effective as the deepfakes are progressively more convincing and difficult to distinguish from a “real” video.

In addition to extortion, our team has identified a disturbing new trend: the use of so-called “deepnudes.” DeepNude was a software application that used artificial intelligence and deep learning techniques to generate highly realistic nude images of women and children from fully clothed photos cultivated from social media. It was developed in 2019 and released in June of that year, but it was quickly taken down due to widespread outrage and criticism. But it was only the website that was taken down. Online predators still use open source software to create pornographic images of pictures scraped from social media platforms like Facebook, Twitter and Instagram. Cyberbullies, child traffickers, pedophiles and predators share these altered images of children on the Dark Web or encrypted messaging platforms like Telegraph and WhatsApp.

Recently, INTERPOL and Italian authorities investigated a bad actor group from Eastern Europe that used sophisticated automated cyberbots to create fakenude images of unsuspecting women, girls and small children pulled from social media accounts. They then distributed the scandalous pictures to various groups on Telegraph. The challenge law enforcement faced was its inability to detect and trace the bots used in the campaign, so proving and prosecuting which hacker or organization was responsible is nearly impossible.

DEEFAKE DANGERS: HOW CRIMINALS ARE USING TECHNOLOGY TO FRAME THE INNOCENT

If deepfakes in social media weren’t a big enough moving target, many of my colleagues in law enforcement see deepfakes as a natural evolution that organized crime gangs and corrupt law enforcement agencies are using to create false evidence to frame individuals for acts they did not commit. These methods are especially dangerous if the imitation is realistic enough to convince law enforcement and the courts of the victim’s guilt. Even more nefarious, perpetrators might eventually use deepfakes to create false videos or images of witnesses to a crime, potentially undermining their reliability or dissuading them from providing eyewitness testimony.

I am concerned about the criminal uses for deepfakes, and their potential for illicit use is growing. As deepfakes become more sophisticated, the prospect of their use in criminal activities will increase. It is important for law enforcement agencies and others to be aware of the potential dangers. Police and lawmakers need to develop strategies, guidelines and policies for detecting and mitigating these dangers.

FOLLOW THE MONEY: DEEFAKES IN THE WORLD OF BANKING

I recently spoke to a large U.S. bank’s chief information security officer (CISO). We discussed the ramifications and challenges deepfakes will have on their industry, especially regarding account fraud. Although there are many easier ways in which bad actors gain access to, or take over, a bank account, deepfakes pose a significant concern for security teams.

Could criminal organizations use deepfakes to bypass account verification in banking? It is certainly

Many of my law enforcement colleagues fear that organized crime and corrupt law enforcement will use deepfakes to frame innocent people.



possible. Criminals could use them to create fake documents or other biometric materials, such as voice and facial recognition, to bypass security protocols and deceive bank employees into believing that the person attempting to access the account or send a bank wire is legitimate. That type of fraud could potentially be very lucrative for criminal organizations, especially those targeting banks that focus on wealthy clients who move large amounts of capital. This could allow the criminals to access large sums without being detected and without raising alarms or indications of a fraudulent transaction.

However, the CISO I spoke with pointed out that banks and other financial institutions likely have measures like two-factor authentication and machine learning to identify anomalies and behavior patterns. Fraud detection software and old-fashioned humans can also detect this type of identity fraud and prevent it from being processed. In addition, banks may have additional policies to verify their customers' identities before allowing them to access their accounts.

The CISO's advice: "Banks and other financial institutions must remain vigilant and continue to implement measures to detect and prevent the use of deepfakes for scams."

NO SAFE HARBOR: DEEPFAKES IN CORPORATE ESPIONAGE

Another use case of deepfakes is in corporate espionage, where criminals have **manipulated videos** or audio recordings to extract sensitive corporate information or gain an advantage over their targets. Bad actors have used artificial intelligence and machine learning algorithms to create manipulated audio or video recordings of company executives confessing to illegal activities, such as insider trading or embezzlement. These fake videos were then used to blackmail the executives or damage the company's reputation.

Unlike banks, deepfakes in enterprises could be used as misinformation or disinformation. Companies could create fake videos or images of its competitors to damage their reputations and steal their customers. It's important to note that using deepfakes in this way is unethical and, in most cases, illegal.

WRAPPING IT UP: MITIGATING THE IMPACT OF DEEPFAKES

As deepfake technology continues to evolve and become more widely available, companies should be aware of the potential risks and take steps to verify the authenticity of videos and images that are shared online. Some measures that can be taken include looking for signs of manipulation, such as inconsistencies in lighting or shadows, and checking the provenance of the content to ensure it is from a reputable source. It is also important for individuals and organizations to keep in mind the potential reputational damage and to take steps to protect themselves.

Law enforcement and intelligence agencies must enlist experts in the field to develop training and education programs to help potential targets identify deepfakes and respond appropriately. Deepfakes are a technology with many legitimate uses, but they also have the potential to do a great deal of harm. As deepfakes become more sophisticated, this potential is likely to increase. It is, therefore, important for law enforcement agencies and companies—the possible victims—to be aware of the dangers and take steps to prevent or mitigate the damage.

OUTLINE FOR A COLLEGE COURSE IN DEEFAKE SECURITY

DR. EDWARD AMOROSO



Back when I started to worry about computer security (while Reagan was still president, *ahem*), one of my first instincts was to develop a course. I later wrote about that course at an [ACM SIGCSE Conference](#), and it served as the basis for my [first textbook](#) on the topic in 1993.

Now that I find myself worrying about the next big technology threat—namely, the existence of deepfakes—I find myself with the same instinct. Hence my contribution here: perhaps the first outline for a graduate course on deepfake cyber risk management.

In case you are wondering how I know that this is the first outline, well, I just asked OpenAI for help. Below is a summary of the response: “Are there any college courses on deepfake cyber risk management?”

Open AI: “It is possible that there are college courses on deepfake cyber risk management, although I am not aware of any specific courses by name. Deepfake technology and its potential risks and impacts are a relatively new and rapidly evolving area.” *Indeed*, OpenAI. Thank you.

Below are descriptions for 12 lectures on this topic. And yes, I might develop this proposal for students at NYU. But I must admit that several of the descriptions below are somewhat aspirational. We might have to let this fruit ripen just a bit before such a class is possible.

That said, my prediction is that within a few years most university computer science departments, especially ones that focus on cybersecurity, will include a course along the lines of what I’ve suggested below. Let me know if you’ve begun work on your own version.

LECTURE 1: WHAT IS A DEEFAKE?

This first lecture explains deepfakes and shows many excellent examples from the open literature and from the public internet.

LECTURE 2: WHAT ARE THE RISKS OF DEEFAKES?

This lecture explains how business, government and individuals are at risk due to deepfakes. Case studies are used to illustrate the threat.

LECTURE 3: THE AI BASIS FOR DEEFAKE DEVELOPMENT

This covers some of the technical basics of artificial intelligence (AI), which will help explain how deepfakes are generated.

LECTURE 4: WHAT IS A GENERATIVE ADVERSARIAL NETWORK (GAN)?

This talk explains the class of deep learning technology that involves neural networks and is closely associated with deepfakes.

LECTURE 5: USING A NETWORK OF EXPERTS TO DETERMINE A DEEFAKE

This lecture poses the question of whether an informed community of experts, or perhaps even an uninformed crowd, could accurately detect a deepfake.

LECTURE 6: USING INDEXED TRAINING TO DETECT DEEFAKES

This explains the emerging machine learning technology and the process of using training sets to create effective deepfakes.

LECTURE 7: OSINT AS THE BASIS FOR DEEFAKE DETECTION

This seventh lecture focuses on whether operational security intelligence can be used to determine that some artifact originated with a deepfake creator.

LECTURE 8: FILE ANALYSIS AND FORENSICS USED TO DETECT DEEFAKES

This talk examines techniques for directly reviewing and analyzing a media file to determine if deepfake evidence is present.

LECTURE 9: USING DARK WEB DIGITAL RISK PROTECTION TO DETECT DEEFAKES

The ninth session examines whether existing solutions for digital risk protection on the Dark Web can be used to detect a deepfake.

LECTURE 10: GOVERNMENT POLICY IMPLICATIONS OF DEEFAKES

This class examines the question of how government should establish and enforce reasonable policies and laws concerning deepfakes.

LECTURE 11: COMMERCIAL SOLUTION OFFERINGS IN DEEFAKE SECURITY

This penultimate talk covers case studies in several emerging startups that provide deepfake cyber risk protection for enterprise and citizen customers.

LECTURE 12: FUTURE DIRECTIONS AND RISKS OF DEEFAKES

The last lecture tries to extrapolate current risks to determine the direction and intensity of future threats that will come with this new attack method.



BEWARE OF DEEPAKE AUDIOS

TAG CYBER/DALL-E

DAVID HECHLER

A few months ago, our CEO was on my screen, leading a short training session. He was talking about phishing attacks, and how to recognize fake messages that seemed to be sent by him. “I will never ask you to send money, or pay a bill or anything like that,” he said. “Never, never, never.” He paused. If he ever had an unusual request along those lines, which he never expects to, he continued, “I will pick up the phone and call. And that’s how you’ll know it’s me.” (Sometimes analog security is a great shield against digital risk.)

He paused again and smiled. “They can’t fake my voice. At least not yet.” We all laughed. Then the meeting moved on.

It took a while before I returned to the question he’d hinted at. How long will it be—before they can fake his voice? I had no idea.

When someone says “deepfakes,” I immediately think they mean videos. Don’t you? That’s one indication of how far behind audio is—at least in the public consciousness. What I learned as I researched this subject surprised me. In this case, out of sight doesn’t mean out of mind. In fact, it may contribute to making audios more insidious, and possibly more dangerous, because potential victims aren’t focusing on them.

HOW ONE DEEPPFAKE SCAM WORKED

I contacted Rick McElroy, principal cybersecurity strategist at VMware, because his company's annual Global Incident Response Threat Report, which surveyed 125 cybersecurity and incident response professionals, found a 13% uptick in deepfakes year over year. He couldn't tell me the breakdown of audio and video deepfakes, "but I believe the overwhelming majority were audio fakes," he said. And he told me about a recent example in which he was actively involved.

A CFO received a call from his company's chief executive that landed in voice mail. The boss had told him he needed money wired right away, and the CFO sent the money, McElroy said. As the CFO was leaving his office, it struck him that he should probably call the security team. Turned out the security team was already looking into suspicious activity, and they managed to stop the transaction before the money was wired.

What made this scam work, at least initially, was that the perpetrators knew the company's processes and workflow. They knew when things got busy and when orders came through. And they used that to construct a script, as though it were a scene from a movie. "They created this sense of urgency," McElroy said, "which they always do when it comes to something like this. And then they hit the CFO at the right time," when he felt the pressure and said to himself, "OK, I gotta get this done." The voice mail from the CEO added credibility.

A few minutes later, when the pressure had dissipated, it occurred to the CFO to call security. That happens a lot, McElroy said. Not long after a scam, it's common for the victim to say, "Wait a minute."

THE BIGGEST DANGER CAN BE WHAT YOU ALREADY KNOW



Jeffrey Katzenberg in the first scene from "It Was Easy to Hack a Billionaire"

To try to get a closer look, I watched a five-minute video that purported to show viewers how something like this plays out when it's actually happening. The film was called "[It Was Easy to Hack a Billionaire](#)," and it featured Jeffrey Katzenberg, former co-founder of Dreamworks, who is sitting on the edge of his desk in his home office when the video begins. A voice off-camera asks why he's agreed to be hacked. "You know," he says, "I am really safe on the internet. I don't do things that I shouldn't. I have a very low profile. I do not think I'm a very good target here."

We jump to the home of Rachel and Evan Tobac, ethical hackers, who are about to do the hacking. Evan, who handles the technical end, knows that Katzenberg's computer has a security flaw—a researcher has found a vulnerability in his software. The vendor has fixed it, but Katzenberg hasn't updated so his computer remains unpatched. Rachel is going to pretend to be Anthony Saleh, Katzenberg's righthand man. When she calls

Katzenberg, it will look like it's coming from Saleh's phone, she explains. "We're also going to use voice-changing software and add background noise so it sounds like I'm in a really loud place and I can't really hear him." They're doing this, and she's only going to "say a little bit," she adds, "because I can't do Anthony's voice."

As she places the call, the scene shifts back to Katzenberg's office. He's speaking to the camera, but suddenly he's interrupted by the ringing of his iPhone. He picks it up and answers. "Hey, Anthony. What's up?" he says. "Check? Check email?" he asks. "Uh oh. OK." He walks around the desk and opens his laptop.

Cut to Rachel, who is smiling: “I think we got it,” she says. The email Katzenberg referred to is one that Rachel had sent him before she called, and she made it look like it was from Saleh. “He clicked,” says Evan, who is also smiling. The phishing email told Katzenberg to expect a shared cloud folder that he should open. “Once he clicks” the malicious link, Evan explains, “the rest of the attack will continue in the background. And we’ll be able to steal data from any site he’s currently on.”

Back in his office, Katzenberg apologizes to the film crew. “Just a second here, guys. Sorry. Sorry.”

Cut to Rachel, who is smiling again: “And that’s how we hacked a billionaire.”

There’s a final scene during which Rachel and Evan show up at Katzenberg’s house to tell him what happened and explain how they did it. After the film ends, the sponsor’s logo appears on the screen. It’s Aura, the online protection company. Beneath the screen, in a box above the comments, there’s a message: “Aura decided to chronicle a hack from start-to-finish. And who better to hack than our billionaire investor, Jeffrey Katzenberg. Our CEO challenged Jeffrey to turn off his Aura app to see what happened.”

In comments from viewers, some skeptics pointed out that the video was a commercial, and shouldn’t be taken at face value. But even if it’s viewed as a kind of tabletop exercise with great production values, it does illustrate how a scam like this can succeed. The key moment for me was when Katzenberg picked up his phone and said, “Hey, Anthony. What’s up?” He said this before he’d heard a word. He saw the name that appeared on his phone, and he heard the voice he expected to hear, despite the noise and poor reception. I can believe that would be enough for most of us. When we think we’re talking to our business partner, we aren’t playing defense. We don’t wonder about noise in the background. We operate with a different mindset: We already know that we’re safe. And that’s what hackers count on.

ARE WE ALREADY THERE?

I thought again about our company video meetings. It wouldn’t be hard to get audio footage of our CEO. And these days, there are **devices** that purportedly allow you to speak into them and have someone else’s voice come out—as long as you’ve acquired enough audio to train it. The potential flaw is that the translation isn’t instantaneous. It can lag a few milliseconds, so it may not sync well with video. But that’s not a problem if there isn’t any video, only a photograph in a circle.

There are plenty of times our CEO doesn’t turn on his camera during our video meetings. We don’t think anything of it. We just look at his photo. What if someone took his place in a meeting and told the chief of staff to wire money somewhere? That would be unusual. Probably unprecedented. But it wouldn’t violate the assurance he gave us in that training session—that he would only ask us to pay a bill or send money by picking up the phone. Can a deepfake audio fool us right now? Are we already there?

VMware’s Rick McElroy thinks so. He knows of **two other instances** involving deepfake audios that resulted in transfers of six-figure sums. Those are pretty large numbers, but the largest theft by far of this kind seems to have been suffered three years ago by a bank manager in Hong Kong. He took a call from a client whose voice he recognized. The client was requesting money to complete a deal. The manager reviewed emails that seemed to confirm details from multiple sources before he transferred \$35 million—to the person who had fooled him with that **deepfake** phone call.

Before he signed off, McElroy offered a suggestion that was definitely not new or high-tech, but might remove some of the worry about unauthorized money transfers. At most companies, only a few employees are in a position to wire funds. For each of them, and the CEO who could ask them to, “come up with a very rudimentary phrase that only the two of you know,” he said, and “you can challenge each other with those.” McElroy remembers using such a system long before he got into the cybersecurity game. “We used to use those in the Marines,” he said. Sometimes analog security is indeed a great shield against digital risk.

TAG CYBER

ANALYST REPORT

TECHNIQUES AND VENDORS FOR DEEPAKE MITIGATION

DR. EDWARD AMOROSO

The ease of using deepfakes to target businesses, government, and prominent individuals demands a new protection approach to reduce compromise risk. Strategies for deepfake risk reduction are outlined and several vendors are shown to implement effective solutions.¹

INTRODUCTION

Machine learning has emerged as a useful method for producing a new type of malicious visual exploit called *deepfakes* that produces misleading images and videos. While deepfake attacks might be viewed as simply extending well-known methods for modifying messaging, news, and information, the approach is more lethal because most observers, even ones trained to spot fakes, tend to believe their visual and audio senses.

In this short analyst note, we outline the basics of how deepfake technology works with emphasis on what we believe the modern cybersecurity practitioner should know. We include a brief overview of methods for mitigating deepfake risk – and we include a listing of some current commercial vendors with solutions worth considering if an enterprise chooses to begin addressing this growing risk.

HOW DEEPAKES ARE MADE

While no official taxonomy exists for deepfakes, some **expert commentators** have begun to categorize exploits into three types: (1) Synthetic changes to existing targeted individuals (usually prominent such as **Barack Obama**); (2) Synthetic generation of fake people or entities that do not exist; or (3) Manipulation of existing

¹ Conversations with **Don Dixon** from ForgePoint Capital were helpful during the early stages of discussion of this important new topic.

videos, audio, or images to create altered interpretation (e.g., slowing up video to change perception of the individual).

The primary method driving deepfake attacks is machine learning and more specifically **Generative Adversarial Networks** (GAN). A typical GAN has two components: First there is the generator that creates plausible data, which in the case of deepfakes is a video, audio, or image. And second, there is a discriminator, which learns to differentiate fake from real data. Quantifying the difference between real and fake is a key aspect of the method.

The GAN process involves a sort of game, where the generated data is reviewed by the discriminator. On successive attempts, the generator trains to produce output that can eventually fool the discriminator. The result is an output that has gone through a process of successive refinements toward a video, audio, or image that a human being will have a hard time interpreting as anything other than the real thing.

HOW DEEFAKE RISK CAN BE MITIGATED

The process of mitigating deepfake risk is nascent, but a **new discipline** is beginning to emerge based on ideas from the research and startup industries. Cybersecurity teams are wise to begin reviewing these methods, because it is likely that responsibility for deepfake risk will eventually reside with security teams. For some organizations, this process of assigning responsibility has already begun.

Our TAG Cyber team observes the following methods being used in practice to address the risk of deepfakes to enterprise teams, executive and management staff, and high-profile individuals:

- **Expert Networks of Reviewers** – This approach produces risk intelligence, usually in the context of a recently emerged deepfake, where experts use whatever means is available to opine on the validity of a video, audio, or image. These reviewers often use technology-based platforms to assist in their review work. Blackbird.ai, for example offers a Risk Intelligence Engine with API that works roughly in this manner.
- **Indexed Sets of Training Assets** – This approach involves indexing of a massive set of available images, audio files, and video files to help drive a platform solution that can accurately determine whether a new asset is real or fake. The RealityDefender solution, for example, indexes over one hundred million such assets, resulting in a highly effective environment for making accurate decisions.
- **OSINT-Oriented Solutions** – This approach treats deepfakes as ingested intelligence which must be subjected to natural language processing (NLP), knowledge engineering, and other advanced Operational Security Intelligence (OSINT) techniques developed primarily in military organizations. The Logically.ai offering works roughly in this manner using experts with over 600,000 hours of R&D and training in OSINT.
- **External Digital Protection Solutions** – This method extends existing scanning solutions that review the deep, dark, and indexed web for evidence of posted exploits. When deepfakes are found, the targeted organization can take steps to remove or at least respond to the threat. ActiveFence provides a deepfake and content review capability that works roughly in this manner.

COMMERCIAL DEEPFAKE MITIGATION VENDORS

The following commercial vendors provide solutions that have been reviewed by TAG Cyber analysts and that appear to have considerable promise in reducing the growing risk of deepfakes to enterprise teams, senior executives, and prominent individuals.



Blackbird.ai – This startup company, headquartered in the US, offers its Risk Intelligence Engine and Constellation Dashboard for detection and response of deepfakes. www.blackbird.ai



RealityDefender (US) – This startup company, headquartered in the US, offers a collage of different best-in-class techniques and methods to provide guidance on the validity of a video, audio, or image. The company indexes a massive training set of assets for its platform. www.realitydefender.ai

Logically.

Logically.ai (UK) – This startup company, headquartered in the UK, applies OSINT methods such as NLP to deepfake analysis to help identify deepfakes in real time for clients. www.logically.ai



ActiveFence (Israel) – This startup company, headquartered in Israel, provides an end-to-end tool for monitoring the deep, dark, and indexed web for evidence of deepfakes. www.activefence.com



... THEY ARE ALL DEEPPFAKES

- | | | |
|--|--|--|
| <ul style="list-style-type: none"> 1. Nick Cage (in "Star Trek") 2. Nancy Pelosi 3. Mark Zuckerberg 4. Bruce Willis (Credit: Megafon) 5. Morgan Freeman 6. Richard M. Nixon (Credit MIT) 7. Barak Obama
(Credit: Jordan Peele) 8. Jerry Seinfeld (in "Pulp Fiction") 9. Joesph R. Biden | <ul style="list-style-type: none"> 10. Ed Amoroso, TAG Cyber CEO
(as a swashbuckler,
Credit: Reality Defender) 11. Queen Elizabeth II 12. Salvador Dali 13. Tom Cruise 14. Kim Kardashian 15. Vladimir Putin
(Credit: RepresentUs) 16. George Washington 17. Snoop Dog | <ul style="list-style-type: none"> 18. Keanu Reeves (on Tik Tok) 19. Mark Hamill 20. Nick Offerman
(as the cast of "Full House") 21. Jim Carrey (in "The Shining") 22. Carrie Fisher
(as Princess Leia, Credit: Disney) 23. Lynda Carter
(as Wonder Woman) 24. Donald J. Trump 25. David Beckham |
|--|--|--|



**ARTICLES /
OPINIONS**



MY
T A K E

WHAT JOE SULLIVAN'S CONVICTION MEANS AND WHAT IT DOESN'T

DAVID HECHLER

Joe Sullivan, Uber's former chief security officer, was convicted of obstruction of justice and covering up a felony for his actions after his company was hit with a data breach. There was controversy when he was charged with a crime, and I wrote about the case [here](#) in January 2022. Following the verdict on October 5, many security professionals (among others) seemed outraged.

Those looking for lessons will find some—and I will suggest a few myself. But first an admonition: It would be easy to draw the wrong conclusions based on a superficial understanding of the facts. Quick summaries often omit the circumstances that made this case so unusual. And the details make all the difference.

WHAT WAS UNUSUAL

Let me start with examples of what I'm talking about.

- Sullivan was not only an experienced CSO, he was also a lawyer. In fact, he'd been a prosecutor in the same U.S. attorney's office that prosecuted him. He worked in the computer hacking and IP unit. After he left, he worked in-house at PayPal as an associate general counsel. When he moved to Facebook, he worked in the same capacity before moving into the chief security officer job there.
- Though Sullivan was not officially functioning as a lawyer at Uber, in some ways he seemed to be playing that role. When hackers contacted Uber in 2016 to inform the company that they had stolen the driver's licenses of 600,000 Uber drivers and personal information of 57 million customers and drivers, Sullivan directed the company's response.
- The CSO led a small team that not only investigated and confirmed the breach, it also handled negotiations with the hackers. Sullivan instructed the group not to share anything about the event with colleagues, including the company's lawyers. The only lawyer (other than Sullivan) who was kept in the loop



Joe Sullivan

TIMOTHY ARCHIBALD

It would be easy to draw the wrong conclusions based on a superficial understanding of the facts. Details make all the difference.

was Craig Clark, who reported to Sullivan rather than to the general counsel. Clark was fired by Uber at the same time that Sullivan was, and Clark was also charged with a crime by the U.S. attorney's office. (He pleaded guilty and testified against Sullivan.)

- One of the reasons Uber seemed so intent on keeping this quiet was that the company had suffered a similar hack in 2014. At the time of the new one, it was close to wrapping up a settlement on the matter with the Federal Trade Commission. Less than two weeks before the 2016 breach, Sullivan had been tapped to give sworn testimony to the commission about the earlier breach (which had happened before he'd arrived). He later continued to communicate about the first breach without saying anything about the second to the FTC, to Uber's general counsel or to the outside counsel with whom he'd been working on the 2014 breach. Once it all came out, the settlement quickly unraveled.
- Sullivan and his colleagues decided to pay the hackers under the company's bug bounty program. But they failed to follow Uber's own guidelines. They paid the two hackers ten times the \$10,000 the policy suggested as a top fee. And the supposed "white hat" hackers had not simply reported vulnerabilities to the company; they had already stolen the data. Sullivan agreed to pay what they asked—after he consulted CEO Travis Kalanick—even before he was able to identify them.
- Sullivan had the hackers sign nondisclosure agreements (NDAs), which again suggested that secrecy was the primary goal in the company's handling of the attack. The use of NDAs was the approach one would expect from a lawyer, not a CSO.
- In 2018, the U.S. Senate's Commerce, Science and Transportation Committee held a **hearing** on bug bounty programs that focused mostly on Uber's. John Flynn, Uber's chief information security officer, defended the concept of these programs. But he did not defend the way Uber handled the 2016 breach. "We recognize that the bug bounty program is not an appropriate vehicle for dealing with intruders who seek to extort funds from the company," he testified. The two hackers both **pleaded guilty** that same year, and one testified at Sullivan's trial that their aim had indeed been extortion.
- The hack remained a closely guarded secret for more than a year. In 2017, Kalanick was forced out after a series of scandals. When Dara Khosrowshahi took over as CEO, he asked Sullivan to brief him on the hack. According to prosecutors, Sullivan had his team write a summary which he then altered by making it sound as though the hackers had gained access to the data but hadn't stolen it. The new CEO hired outside experts to investigate. When he **publicly reported** what they'd found, Khosrowshahi added that he'd fired Sullivan and Clark.
- Finally, there was the damage done. It's hard to calculate the blow to the company's reputation simply because there were so many during Kalanick's tumultuous tenure. But there were clear repercussions, even if some commentators have tried to minimize them. The **criminal complaint** against Sullivan pointed out that the hackers continued to attack other companies after they hit Uber. Had the company reported the hack to law enforcement, the complaint said, "the hacks of multiple additional large tech companies and the theft of the personal data of millions of additional customers and users may have been prevented." There was also the financial hit the company took. The \$100,000 it paid the hackers in bitcoin was easy to brush aside. But then came the lawsuits. Attorneys general in

Why wasn't Kalanick charged with a crime? Why were Sullivan and Kalanick able to keep the matter quiet for so long?



all 50 states sued Uber based on its failure to comply with state data breach notification laws. The \$148 million **settlement** the company paid was not quite as easy to ignore.

LOOKING FOR LESSONS

Having said all that, Joe Sullivan could not have done what he did alone. The criminal complaint made it clear that he consulted with Kalanick within hours of being informed of the hack, and the CEO specifically told him to go ahead with their plan. Why wasn't Kalanick charged with a crime? This seems like a legitimate question for law enforcement. (Ironically, even though Sullivan was not supposed to be functioning as a lawyer, it's possible that if Kalanick were charged he might try to argue an advice-of-counsel defense.)

Sullivan could not have kept this matter a secret by himself. Why was he able to do so? That's also a good question. It seems likely the people involved knew that Kalanick approved what they were doing, and perhaps that was enough for them. It may also have had to do with the respect his colleagues had for Sullivan. It could be that they deferred to him because he was not only the CSO but a former prosecutor.

But in the end, it comes down to corporate governance. And this must be seen as a clear demonstration of the company's failure in this realm.

It's hard to imagine a situation in which the general counsel should be kept in the dark about a legal matter—unless the general counsel is suspected of misbehavior and is the target of an investigation. Otherwise, the general counsel's involvement would seem especially important when the company suffers a second breach just as it is deep in negotiations with the FTC in an effort to resolve the first. It's particularly important if the CEO or other officers may be involved, because the general counsel's duty is to the company and its shareholders, not management. And if the matter is serious enough, the general counsel may decide to bring it to the attention of the board of directors—or resign.

Companies should ensure that all employees know that they can pass along their concerns anonymously to the general counsel through a complaint line that's always available. This is a widely adopted best practice, and it's designed to make it harder to maintain the secrecy that criminal activity thrives on. I don't know whether Uber had such a system, but it would have provided the people who knew about the breach a way to convey it to the office that needed to know.

Obviously, corporate governance starts at the top. The CEO and the board of directors need to know what's going on, and the general counsel needs to have a seat at the table. So should the chief compliance officer. But Uber didn't have one until 2018. This was another sign of a company that had a lot of work to do in this area.

DID PROSECUTORS CROSS A LINE?

Many critics of Sullivan's conviction can't understand why he was prosecuted in the first place. They seem upset because this case seemed so inconsequential compared to big corporate meltdowns that resulted in officers going to prison. Not just seemed—it was nothing like those cases. Had it not been for

In the end, it comes down to corporate governance. And what happened must be seen as a clear demonstration of the company's failure in this realm.

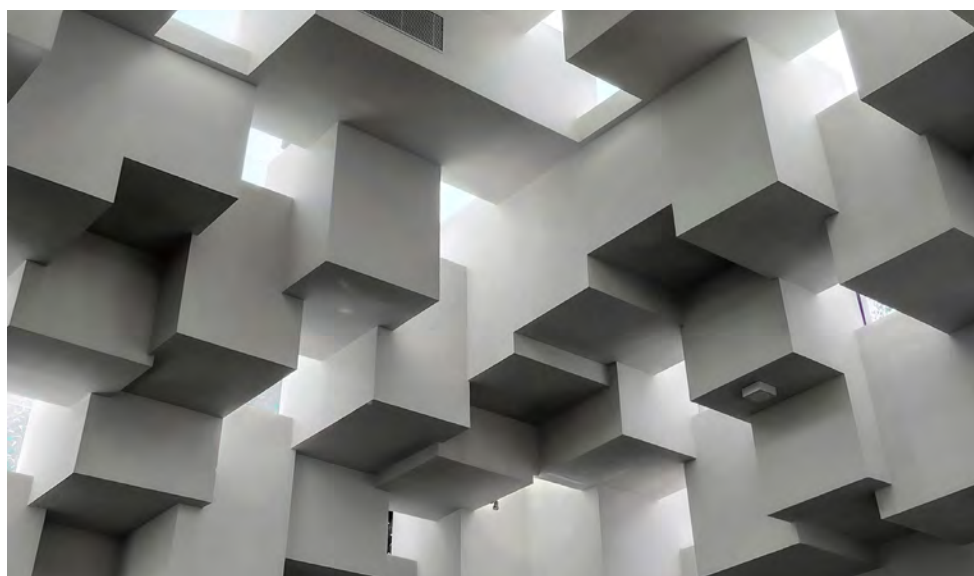


the lies and secrecy, no one would have been charged with a crime. It would likely have been no more than a passing embarrassment for a company that had endured many of much greater import.

Security officers are used to getting fired when things go wrong. That wouldn't have been surprising. But unless it's a matter of stealing data or some other form of malfeasance, it's rare that they'd find themselves in the crosshairs of law enforcement. They're not usually powerful enough to direct a company down a path of criminal conduct. The irony is that Joe Sullivan actually had real power at Uber. He had a seat at the table—the very thing that CSOs have been pushing for. The very thing that, under other circumstances, his admirers would be celebrating.

When critics complain that Sullivan did not deserve to be prosecuted, they see a disparity between him and his boss. This strikes me as a fair point. But if he had not been prosecuted, what about the disparity between Sullivan and the two hackers who pleaded guilty to crimes? What about the disparity between him and Craig Clark, the lawyer who reported to him and also pleaded guilty? They all conspired to pretend that an extortion demand was a helpful tip by security researchers. How can you argue that Sullivan was less culpable than his three co-conspirators?

There's one more angle. Lawyers who transgress are sometimes held to higher standards. The view is that they should know better, and they can't claim ignorance. That's especially true of in-house lawyers, who are often seen as moral compasses and **gatekeepers** for their companies. Sullivan was once an in-house lawyer, and in this case he functioned as one by superseding his company's legal team. Prosecutors may also want to ensure that a former prosecutor who crosses an ethical line isn't issued a free pass. And Sullivan was not only a former prosecutor, he worked in the same office as the lawyers who tried him. Maybe they viewed this case as a way to clear their own reputations.



TALKING TO A WITNESS IN THE SULLIVAN TRIAL

DAVID HECHLER

I recently wrote an article on a subject that has generated strong feelings in the tech community. It was about the conviction of Joe Sullivan, former chief security officer at Uber, on charges of obstruction of justice and covering up a felony after two hackers stole the driver's licenses of 600,000 Uber drivers and personal information of 57 million customers and drivers. Uber paid the hackers \$100,00 and had them sign nondisclosure agreements to keep the matter quiet. [I explained](#) why I thought Sullivan was indicted, why he was convicted and what lessons companies ought to draw from the case. My takeaway was that throwing a blanket of secrecy over a data breach—keeping even company lawyers in the dark (as prosecutors argued Sullivan had done)—was a grievous failure of corporate governance.

Melanie Ensign posted a comment on my article that got my attention. I quickly suggested we sit down and talk. I'd written a [piece](#) a year earlier about her. Ensign had worked at Uber as the head of security and privacy communications during the time the company was responding to the 2016 data breach. She'd left in 2020 to found a public relations firm called [Discernible Inc.](#), but her PR work—at Uber and Discernible—was and is unusual. At Uber (and at Facebook before it) she'd advocated greater openness in dealing with negative information. "Covering up bad behavior is never in the company's best interest," she'd told me. "Living with buried bodies is very expensive and very stressful." At her own shop, Ensign works mostly with companies' security and privacy teams, helping them learn to communicate more effectively within their companies in order to exercise greater influence on the business.

There was another reason I wanted to talk to her. It turned out that she'd testified at Sullivan's trial. In fact, Ensign was the trial's last witness.

When we sat down to talk via Zoom a week later, she had a lot to say. She prefaced her remarks by emphasizing that she is not a lawyer "so I can't really talk about the legality of anything or legal strategy." Nor did she testify with an agenda. "My job was to answer the questions to the best of my ability and to tell the truth." She wasn't surprised that the law finally caught up with Uber. It had felt to her like it was just a matter of time. But she was astonished that the U.S. attorney's office determined that the culprit wasn't someone like CEO Travis Kalanick, who had steered the company from crisis to crisis, but rather CSO Joe Sullivan, who seemed universally respected.



Melanie Ensign

Sullivan's defense argued that Uber's lawyers were responsible for handling the data breach and that plenty of them knew about it. But the testimony left a lot of holes.

She told me that both sides had subpoenaed her to appear. She'd had conversations in advance with prosecutors and defense attorneys, but she wasn't sure she'd be a help to either. (And now that it's over, she's not sure she was.) She traced their interest to something she did after Kalanick was pushed out and replaced in 2017 by Dara Khosrowshahi, who only learned about the breach after he took over as CEO. After he'd ordered a thorough investigation, Khosrowshahi posted a [statement](#) on the company's website explaining what he'd learned. That was also when he fired Sullivan and a lawyer who reported to him, Craig Clark, who was also charged in the case. Clark pleaded guilty and testified against Sullivan.

HOW SHE CAME TO TESTIFY

Ensign played no role in the way the story was eventually communicated to the public. But a year earlier, shortly after the breach, she'd created a communications plan for the incident. She and two colleagues believed disclosure of the events was inevitable, she told me, and they thought focusing on the skill with which the security team tracked down the two hackers "would have made a great media story," she said. But the relentless succession of bad publicity that hounded the company in 2017 didn't leave room to pitch it, she added.

After Sullivan was fired, she felt indignant at how the story played out. "I really didn't feel like the public narrative that was coming from the company was accurate compared to what I experienced in 2016," she told me. So she took her communications plan and gave it to the legal team. Sally Yoo, who had been general counsel, was gone by then, and it took her a while to figure out who to give it to. But that's how it landed in the pile of discovery documents, and how she wound up testifying.

In court, it was the defense that called her to the stand at the end of the month-long trial. What were they looking for? "As far as I can tell, it was the fact that other lawyers were aware of the incident, and that other members of the executive team were aware." In other words, that the events had not been shrouded in secrecy, as prosecutors had claimed, and that the lawyers in particular were involved. This was key because the defense argued that the lawyers were responsible for deciding how to handle the breach, not Sullivan.

Prosecutors argued that Sullivan wanted to conceal the breach because the company had experienced a similar episode two years earlier. In fact, 10 days before the 2016 breach, Sullivan spent hours testifying under oath about the first one in an effort to settle an investigation that the Federal Trade Commission had opened. Sullivan told the FTC about Uber's new security measures that would prevent a recurrence, prosecutors said, and though settlement negotiations dragged on for months, Uber never disclosed the second breach to the FTC, which only learned of its existence when the new CEO posted his message (at which point the proposed settlement unraveled). This amounted to a cover-up, prosecutors said.

Ensign didn't work at Uber in 2014. "I didn't have knowledge of the FTC investigation," she told me. "I didn't know that the 2014 investigation was still happening." So she had nothing to add in court or in our interview about that. But she did testify about the lawyers and about Uber's decision to fire Sullivan.

The two lawyers Ensign mentioned on the stand were Craig Clark and Candace Kelly, who worked with him. But an email exchange between Kelly and Ensign that was read in court ([and reported by Courthouse News Service](#)) did not seem to buttress the defense. "I saw your doc on the extortion issue," Kelly wrote. "Do you know who in legal they are working with, or is that me?" Ensign told her it was Clark. "I wanted you to be in the loop in case public disclosure is needed," Ensign added. "Got it, thanks," said Kelly. She did not sound like a lawyer "in the loop."

The defense position was further undercut when former top lawyer Sally Yoo testified that she didn't find out about the breach until September 2017, 10 months after it happened. "I was shocked," she [testified](#).

“This is the type of event where I would have expected to be brought into the loop while the investigation was going on.”

Another hole emerged when it was revealed that Uber’s org chart listed Sullivan as chief security officer *and* deputy general counsel. It was widely known that he’d begun his career as a prosecutor and had worked as an inhouse lawyer before switching to tech. But it was not generally known (and was news to me) that his job at Uber entailed legal work. At a minimum, this seemed to complicate his argument that the management of the data breach was out of his hands and the sole responsibility of “the lawyers”—i.e., the *other* lawyers.

Ensign’s testimony about the company’s motive for firing Sullivan may have done more to help his defense. The termination was part of Khosrowshahi’s campaign to lift “Uber 2.0” from a series of scandals, she told the jury. “When you can portray a specific individual as a bad apple, you can remove that bad apple from the situation and distance the company from the situation they are accused of,” Ensign testified. “So that was what Uber PR was doing?” asked Sullivan’s lawyer, John Cline. “That’s what I believed they were doing,” she replied.

Ensign testified that Uber’s new CEO fired Sullivan to cast him as the “bad apple” and demonstrate they’d reformed.

THE USE OF BUG BOUNTIES

The other important subject she addressed was the way the company had used—prosecutors would say “misused”—its bug bounty program. “I was concerned with the characterizations that the bug bounty program had been used to cover up the incident, which was not consistent with what I had experienced,” she told the jury. It was used because the company had no policy outlining how to handle “extortion attempts,” she explained, and did not have access to \$100,000 in Bitcoin, which the hackers demanded.

In our interview, I returned to this topic. It’s gotten a lot of attention since the trial. Members of the security community have expressed concern that, in the wake of Sullivan’s conviction, bug bounty programs may now find themselves unduly scrutinized by law enforcement.

Ensign pointed out that in 2016, a startup like Uber did not have a stash of Bitcoin at its disposal. So Uber made the payment through HackerOne, Inc., which ran its bug bounty program. “It was the only way that we could make a Bitcoin payment within the timeline required in order to get the data back,” she said. I told her there were probably other options. For example, law firms that help clients with ransomware attacks are usually equipped to make crypto payments as part of their representation. But there were also larger issues here.

Bug bounty programs are not designed to make extortion payments to criminals. Uber’s program certainly wasn’t. This was emphatically spelled out in February 2018, when the U.S. Senate Committee on Commerce, Science, and Transportation held a [hearing](#) on bug bounty programs and lessons learned from the Uber breach. One of the witnesses was Mårten Mickos, CEO of HackerOne, who said in his written testimony: “Extortion has absolutely no role in bug bounty programs.” He added: “Whenever a situation develops that may indicate an extortion attempt, HackerOne advises the sponsor of the program (its customer) to notify and work with law enforcement for guidance and instructions.”

Uber’s program was never intended to pay extortion to criminals, testified John “Four” Flynn, the company’s chief information security officer from 2015 to 2020 (and now a CISO at Amazon). “This was not consistent with the way our bug bounty program normally operates,” he said. He also faulted the

company's failure to disclose the breach in a timely fashion: "I think we made a misstep in not reporting to consumers, and we made a misstep in not reporting to law enforcement." He, too, suggested that company lawyers were out of the loop: "One of the things we didn't do well here is include enough of the right legal representatives to determine if this was a data breach notification requirement." Failing to notify states under their data breach notification laws cost Uber another \$148 million in its 2018 [settlement](#) with 50 state attorneys general.

Bug bounties are designed to pay white hat hackers and researchers token compensation for pointing out security vulnerabilities. Uber set an upper limit for such payments at \$10,000. Following the 2016 incident, the hackers did not identify vulnerabilities; instead they announced that they'd already exfiltrated the data and demanded to be paid ten times the top amount the company generally paid. This wasn't a bounty. It was a ransom. The hackers were indicted in 2018 and pleaded guilty the following year. One testified at Sullivan's trial that he knew what he was doing was illegal and his intent was to extort money.

Ensign and Kelly used the same word in their email exchange. Nobody seemed to be calling it a bounty. Ensign told me that she even titled her communications plan "Extortion Attempt." And one of her many frustrations is that bug bounties became the subject that emerged from the company's long-delayed disclosure instead of the real issue. "I think the conversation about disclosure is where we needed to focus," she said. "Bug bounties became a distraction because of the way this was communicated in 2017."

Ensign had believed from the beginning that the company should publicly acknowledge the event. When the congressional hearing was scheduled, she was on the team that prepped for the testimony. She and CISO Flynn advocated sharing technical details about the intrusion. "We knew that's what the community needed," she told me. The Senate committee had other ideas, but it all came out in the testimony of a [hacker](#) and a [hunter](#) at the trial. (The second was a reasonable facsimile of the story Ensign wanted to pitch to the media as part of her communications plan.)

THE VERDICT

Before we wrapped up, we returned one more time to the trial. I asked Ensign what she felt when the verdict was announced. "Disappointed," she said.

She told me some of the things Sullivan did that impressed her after the 2016 breach. Uber announced what Ensign called "problematic" data collection practices it was about to institute. But a short time later, executives realized that the company didn't even have the technical ability to deliver. So when people got angry, it was at something that wasn't going to happen. It was a pure fiasco: "a huge loss of trust and reputation for zero business value," she said.

It took a lot of work to try fix the mess, which Ensign was endeavoring to resolve. Sullivan stepped up to help. And he was the one who made the difference, she said. "It was Joe who led the effort to get everybody in product and engineering and legal and marketing on board with what type of privacy commitments we can say publicly—and actually live up to. Joe led that effort."

Thinking again about the verdict, Ensign couldn't shake the sense of incongruity. "I have a lot of respect for Joe. And of all the things that that company did, and of all the executives they had, it is shocking to me that this is the issue and this is the person that it happens to."



GETTY IMAGES

Uber CISO John "Four" Flynn (l) and Mårten Mickos, CEO of HackerOne, at the U.S. Senate hearing where they testified about Uber's bug bounty program.

USING CYBER IN WAR: WE NEED TO GET BETTER



DAVID NEUMAN



I recently joined TAG Cyber as a senior analyst because it was an opportunity to continue my journey to learn, grow and give in an industry that intertwines every facet of our lives. Thirty-eight years of experience doesn't mean that you stop learning and growing, and working here empowers my opportunity to give back in a helpful way.

I enjoyed the [TAG Cyber Security Quarterly](#), published last April, which explored the subject of cyberwar. As a 28-year veteran of the U.S. Air Force, a retired cyber warfare officer and a two-time chief information security officer, I believe it is a subject that warrants continuous study (just as other forms of warfare do). The U.S. military services dedicate university-level study to the subject in their war colleges; however, they have only started paying serious attention to cybercapabilities as a domain within the last 10 years. They are woefully behind their peer competitors, and future conflicts will draw in civilian institutions such as hospitals, transportation systems and banks that will bring citizens to the front lines. This article discusses how cyberwar will connect more than just a country's military forces, and how civilian and government entities must continue to prepare.

FOCUS ON OUTCOMES AND LESS ON DEFINITIONS

Carl von Clausewitz was a nineteenth century Prussian general and military theorist. His work is still mandatory study in U.S. professional military education programs that emphasize strategy in national security. In his seminal work, "On War," he tells us, "War is a continuation of politics by another means"—that is, socially sanctioned violence. In the traditional sense, this involves getting other nations to concede to your will, but with force, either by occupying their land or taking away their will to resist (i.e., destroying their ability to defend themselves). Cyber cannot do either of these things any more than a tank, plane or ship can accomplish them on their own. However, cyber can be influential in operational and strategic outcomes. Many military planners would say, "It's not the weapon you sling that makes you lethal, but how you sling it." Most military planners assume cyberweapons will be slung against civilian targets in small or large conflicts.

Cybercapabilities are asymmetric. They transcend traditional warfighting domains such as air, land, sea and space. Cyberweapons and tactics can bring kinetic and non-kinetic effects that achieve operational and strategic outcomes. For example, those who have studied large-scale conflicts would tell you it's all about the beans, bullets and gas. In other words, logistics—as the Russians have discovered in their war with Ukraine. The last time the U.S. experienced contested logistics was during World War II. In the next large-scale war, the U.S. is likely to experience contested logistics from the cyberdomain in addition to other disruptions that could potentially influence its will, as a nation, to fight. The disruption of logistics through information manipulation may be non-kinetic, but the outcome is what counts. And the use of cybercapability could well result in deaths as a result of combat forces not having the materiel they need to fight.


USE FICTIONAL SCENARIOS TO LEARN LESSONS AND PLAN MORE EFFECTIVELY

In 2009, I was studying at the Naval War College. Each of the military services has a war college responsible for the professional military education of its officers in areas of national security and strategic studies. Military officers from the United States, as well as officers from other allied nations and select government agencies, join in a graduate-level program to learn, grow and share to make them better senior leaders. Each student is responsible for exploring a topic of operational relevance and writing on the subject. I chose to write an advocacy paper on how the United States might respond to a cyberattack. I used a theoretical scenario to reinforce my rationale on how cybercapabilities could be used in conjunction with military activities, and the serious impact this could have on national defense.

The basis for the following scenario is contested territory and sovereignty—in other words, the usual source of tensions. The adversary's strategic objective is to invade and hold a neighboring disputed territory. That territory is weak militarily, but it has an important ally: the United States. The adversary has a large military and knows it can defeat neighboring forces easily. But it cannot defeat the U.S. in a conventional conflict. The group's intent, therefore, is not to defeat the U.S. outright, but to disrupt its ability to deploy forces to the theater of operations long enough to establish a significant and robust military presence in the disputed territory—thus making a recapture of the territory too costly to attempt.

The adversary's planning began years earlier. It had watched the U.S. since the beginning of its wars in Iraq and Afghanistan. During the same period, the adversary had undertaken a massive

In 2009, when I was studying at the Naval War College, I wrote a paper on how the U.S. might respond to a cyberattack.



military modernization that included the development of cybertactics and weapons to use against nonmilitary targets. For the past five years, it has conducted extensive cyber reconnaissance, identifying vulnerabilities in critical U.S. infrastructures near key military installations that would be involved in action against them. In addition, they have exploited commercial software used in systems supporting military operations such as transportation and logistics.

In my scenario, the enemy's campaign started a year before its invasion with the public announcement of military exercises to explain the movement of forces into the immediate area of operations. The disinformation campaign continued with suggestions that terrorist groups were planning or considering cyberattacks on the U.S. Closer to the start of the invasion, the adversary executed cyberoperations against critical infrastructure and key resources. Specifically, it disrupted or disabled food distribution systems throughout the U.S. through information systems that automate inventory and the movement of food to large supermarket franchises.

Just before the incursion, the supervisor control and data acquisition (SCADA) system at the Roosevelt Dam in Arizona was compromised and used to unleash 300 billion gallons of water into the Tonto National Forest. This caused minimal loss of life but massive interruption of power and water supplies for Arizona and neighboring states.

The Navy told me my scenario was unrealistic and that cyber was a fad that would soon be gone.

Simultaneously, the information systems of several large financial institutions were breached, and large banking databases were encrypted, rendering them inaccessible for ordinary banking transactions. Their public websites were defaced, announcing that the banks had been compromised and that customers' money was not safe. Mainstream media carried the stories, creating widespread panic and resulting in a run on banks and food stores throughout the country. The political leadership struggled to determine what or who was responsible for these events. The lack of definitive roles and responsibilities governing these critical infrastructures inhibited cohesive assessment and response. Since 85% of critical infrastructure is privately owned and operated, the

government had little control or visibility into the full extent of what was happening. In the meantime, world financial markets reacted to the possibility that U.S. economic power might be under assault.

The adversary continued mobilizing its forces under the auspices of planned exercises. Additionally, it made public statements expressing sympathy for the disruptive cyberattacks in the U.S. and pledging its support. In conjunction with these operations, the enemy infiltrated the automated supply systems in the Department of Defense (DoD), changing inventory levels of fuel, munitions and critical parts. The intrusion would not be detected for 48 hours. It resulted in the degradation of logistics operations as military leaders lost confidence in the data available to make time-sensitive decisions on how to deploy and support U.S. military capabilities. Similar operations were carried out against personnel systems, the Defense Finance and Accounting System, and the Tanker Airlift and Control Center at Scott AFB in Illinois. These were operational centers conducting airlift of military personnel and materiel, and the attacks degraded worldwide airlift and air refueling operations supporting all combatant commanders.

That wasn't all. Even before the start of the invasion, instrument landing systems at Los Angeles' LAX, New York's JFK and Chicago's O'Hare Airport were compromised, causing the crash of four commercial airliners. With no understanding of the extent of the attack, the government had responded by shutting down all air transportation across the country, as it had on 9-11. Communications and utilities were

attacked and shut down in large metropolitan areas close to military installations that would be involved in operations against the adversary. In accordance with computer network defense and force protection procedures, the DoD declared its highest state of force protection and information condition. The result brought movement on and off bases to a crawl. In an ironic twist, the command-directed information condition procedures resulted in a self-imposed denial of service as networks and critical information systems were disconnected from the global information grid.

What was a preplanned and announced exercise had turned into the planned invasion by the adversary. The U.S. did not have the forces in the area of operations to deter, much less stop, the hostilities, allowing the adversary to achieve its first operational objective: invading a sovereign neighbor and preventing the U.S. from assisting militarily.

LESSONS LEARNED

Throughout human history, militaries have developed advanced arsenals such as automatic weapons, tanks, planes, submarines and missiles, to name a few. None of those weapons alone fundamentally changed the nature of war, but when used in an integrated way they have delivered a distinct operational advantage. For example, the battleship was a dominant weapon in the 1930s and 1940s that could deliver ferocious firepower against its peers at sea. I have a program from the Army-Navy football game played in November 1941. There's a photograph of the U.S.S. Arizona with the following caption: "It is significant that despite claims of air enthusiasts, no battleship has ever been sunk by bombs." On Dec. 7, just one week after this game was played, the battleship Arizona was sunk by bombs dropped by Japanese aircraft with a great loss of life. The Japanese chose to use air power asymmetrically to destroy targets versus taking on this powerful capability with like weapons.

Now we have cyberweapons. Militaries and nations that use these capabilities in an integrated way—in many cases asymmetrically—will likely fare much better.

Here are some of the lessons I suggest we can conclude from my scenario (which strikes me as more relevant today than it was when I wrote it):

Expect the unexpected by thinking asymmetrically. An understanding of offensive and defensive cybercapabilities is only half the battle. Anticipating how they can be used in unexpected ways is the key to gaining an operational advantage. Ironically, in the discussion of my research at the Naval War College that the theoretical scenario above supported, the Navy told me it was unrealistic and that cyber was a fad that would likely be gone in a few years. That was in 2009. Today, cybercapabilities are a national security concern for citizens, businesses and militaries alike. There isn't any debate about that. What if the Navy had expected an air attack on the fleet in 1941? What kind of cyberattacks should we try to anticipate now?

Fight as smart as you do hard. Mature military planners think in terms of operational outcomes and not just what weapons they need. Cyberpractitioners typically think about technological tools versus what those tools must achieve. This lesson extends to civilian organizations that struggle to align cyberprotection capabilities to business outcomes. For instance, a company that depends on technology to produce medicine may be susceptible to cyberexploitation by nation-states that want to steal intellectual property, or organized crime that will extort them for financial gain. They must consider their risks smartly and be ready when the attack comes.

The economy of scale matters. Economic factors have always been a part of military operations. Never use a \$1 million bomb on a \$100 target. The cost of entry into the air domain is \$117 million. That's the cost of a single fifth-generation fighter jet (F-35 Joint Strike Fighter)—no fuel, munitions or pilot. That cost of admission does not equal air dominance. The cost of admission to the cyberdomain is a laptop

computer and a talented programmer. How many of those can you acquire for \$117 million? What outcomes could you deliver for that price?

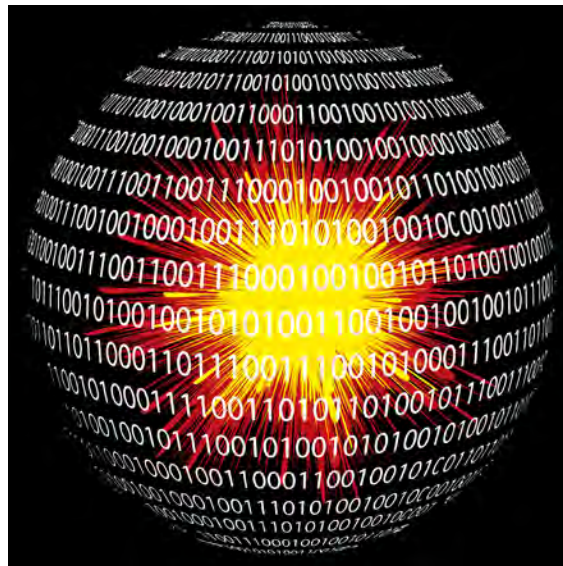
Wargaming is cheap and effective. Wargaming is a staple of military planning. It is a low-cost and highly effective way to identify gaps in defenses, offensive plans and countermeasures. Next-generation wargames should include not just members of the military but professionals who understand systems that could be cybertargets, such as power and utilities, transportation and telecommunications.

A FINAL THOUGHT

There are many characteristics that distinguish the challenge of defending the cyberdomain from that of defending more traditional domains. The most compelling one is that cyber is entwined with every facet of a global society. This creates complexities that make it harder to protect critical assets—and also to anticipate what’s over the horizon. I’ve used the term “asymmetric” a lot in this article because I think it’s at the heart of how to address the risks these complexities create. Part of asymmetric thinking is conceptualizing the art of the possible. Artificial Intelligence is here. Quantum computing is not far away. Other technologies, such as digital currency, will require new skill sets and ways of thinking to protect against cyberattacks of the not-too-distant future.

You could argue that bombing a critical bridge or power plant is highly destructive, but wiping out the financial data of millions of people or turning off the electricity in major cities indefinitely would be just as destructive. These implications must be considered when governments and private institutions allocate resources to the military, infrastructure, education and innovation programs that sustain our way of life.

If we make these investments, we not only build greater protection and resilience in the cyberdomain, but we will likely harness innovative technologies that will benefit society. What better approach to protect and grow in a way that serves both outcomes?





INTERVIEWS



AN INTERVIEW WITH MULI MOTOLA,
CO-FOUNDER AND CEO, ACSENSE

PROTECT YOUR CLOUD-BASED IDENTITY AND ACCESS MANAGEMENT SYSTEM WITH ACSENSE

Cloud-based Identity Access Management (IAM) systems are highly vulnerable to security breaches, human error and insider threats. Businesses often erroneously believe that if a breach occurs, their SaaS provider will help them recover all sensitive data. However, most IAM systems don't provide out-of-the-box backup and disaster recovery features or options. Even in the cloud, companies must take on the responsibility of protecting themselves.

AcSense is a SaaS platform offering quick, easy, one-click recovery and protection for cloud-based IAM systems, such as [Okta](#). We were excited to talk with them to learn how their platform helps ensure IAM resiliency and business continuity for enterprise organizations.

TAG Cyber: *What are some common misconceptions companies have when it comes to their Identity Access Management systems?*

ACSENSE: One general misconception is that organizations think that critical SaaS, such as Okta, are protected in the cloud. Because of this, most companies have not done a business impact analysis of their IAM systems. Customers of a SaaS provider typically rely on the provider's systems and services to operate their own businesses, and any disruption to these systems and services can have significant consequences, including regulatory impacts and fines, as well as financial, reputational, relational and productivity losses. At the technical and operational level, many companies are not aware of IAM business and access continuity solutions. Consequently, they are forced to use open source or in-house scripts and tools to partially address their needs. Unfortunately, these makeshift solutions are often unable to fully protect, backup and restore their Okta after a breach or incident, such as a misconfiguration by an employee.

TAG Cyber: *How does ACSENSE offer solutions to the above issues?*

ACSENSE: When it comes to understanding the resilience of an organization's IAM systems, our solution makes it easy for security and risk management leaders to measure and quantify their business continuity posture. This includes things like resiliency, hygiene and recovery. Our platform provides an air-gapped, reliable architecture, enabling organizations

At the technical and operational level, many companies are not aware of IAM business and access continuity solutions.

to protect their data assets, as well as ensure business and access continuity, even in the face of sophisticated attacks. Additionally, we aim to reduce IAM downtime and costs by providing features, such as: one-click full tenant recovery; fail-over access to a secondary tenant; the ability to identify and investigate changes between different points in time (PiTs); and a low recovery time objective (RTO) and recovery point objective (RPO) of approximately 10 minutes. Furthermore, compliance is also a major focus of ACSENSE. Our platform offers unlimited retention, incident investigation, data integrity checks and change management, which helps to eliminate the burden on IT organizations and ensure compliance with disaster recovery test procedures.

TAG Cyber: What is meant by Okta's "shared responsibility model" and what implications does this have for backups and data recovery?

ACSENSE: The shared responsibility model is a way that cloud providers and customers split the responsibility of keeping their information and systems safe. In other words, Okta takes care of some things, while the customer takes care of others. When it comes to business continuity and security, this means that Okta will make sure their systems are running smoothly, but the customer is responsible for keeping their own data and applications secure. Therefore, the customer needs to make sure they have the right controls and processes in place to protect their data and configurations in order to keep their business running smoothly. In case of an outage by the provider, the customer should have an established plan in place to minimize the impact on their business. This could include things like backing up their tenant and data; maintaining a disaster recovery plan; or having a way to redirect their IAM primary tenant to a secondary tenant. They should also have a clear understanding of the provider's service level agreements (SLA) in case of an outage.

TAG Cyber: If a company discovers they are a victim of a data breach, how long will it take them to address the issue and recover their data using ACSENSE? Is the process complicated?

ACSENSE: If there is one thing our combat experience has taught us, it's that when there is a crisis, it's important for the people in charge to have a clear understanding of the situation. Our platform makes it simple to investigate and recover any changes that happened during an attack on Okta, for example. With ACSENSE, we make it easy for a company to decide whether to fail-over its Okta tenant to a stand-by tenant, or revert to any point in time before the attack with just one click.

TAG Cyber: What is the top cyber threat facing companies in 2023?

ACSENSE: As in the past year, I foresee a continuation of attacks on identity infrastructure by highly organized and sophisticated ransomware gangs. The international extortion group, Lapsus, gained access into the servers of Okta through the compromised account of a third-party customer-support engineer. They were also responsible for attacks on Samsung, Nvidia, Uber, Microsoft and T-Mobile, to name a few. Another cybercriminal gang, Oktapus, targeted more than 130 firms last year, obtaining Okta identity credentials and multi-factor authentication (MFA) codes. It was reported that at least 114 of the companies were in the United States, with the remaining victims scattered throughout over 68 other nations.

We've also seen an increase in credential stuffing and MFA manipulation attacks lately. These attacks target IAM administrators and, when successful, can lead to a complete take-over of the IAM infrastructure, as well as access to all the company assets. This is why we have made it our mission to ensure that IAM solutions have continuous accessibility, maximum uptime and next-level operational efficiency.



“Now that I’m here, I might as well audit your cloud app compliance.”



AN INTERVIEW WITH MAOR BIN,
CEO AND CO-FOUNDER, ADAPTIVE SHIELD

SECURE YOUR ENTIRE SAAS STACK WITH ADAPTIVE SHIELD

With companies adopting an increasingly wide array of SaaS applications, security teams must rush to bridge security gaps to ensure that all attack surfaces are fully covered.


Adaptive Shield enables enterprises to increase their SaaS security posture, as well as detect and respond to SaaS threats, by monitoring and controlling all business-critical SaaS applications. Moreover, it provides support for 100 SaaS platforms and applications out of the box—allowing businesses to swiftly connect their entire SaaS stack without any changes to their existing architecture. The company met with us to share more insight into their high-grade solution.

TAG Cyber: SaaS providers include security controls in their products. Why are these not enough and how does your solution fill in the gaps?

ADAPTIVE SHIELD: There's a scene in "Seinfeld" where Jerry returns home to discover his apartment has been burglarized. He realizes that despite spending money on the best lock available on the market, it has one design flaw: The door must be closed for the lock to work. We have a similar situation with SaaS providers. They build highly effective security tools into their SaaS apps, but those settings must be configured correctly to protect against data loss, SaaS ransomware and other threats to the data stored within.

There are a few concerns every security team should have when working with SaaS applications. For a large organization, there may be thousands of configurations that need to be continuously set correctly across the SaaS stack for each user role and every app. Some settings are set at the app level, but many allow users to customize their settings. These customizations take place outside the view of the security team and can weaken the organization's security posture. Additionally, there are employees who integrate third-party applications into their SaaS apps. While this may extend functionality and improve workflow, these apps often ask—and are granted—permission scopes that include the ability to read, write and delete data, as well as email or otherwise share data. Furthermore, we're starting to see malicious apps enter the market, and SaaS security controls don't usually address third-party applications. SaaS security controls also lack visibility into the hygiene of devices accessing their systems. That makes sense for the app—

SSPMs perform automated checks of all security settings across all users and applications, while providing deep and continuous visibility into the SaaS stack and its security controls.



which wants users to be able to gain access from any location on any device—but if a device infected with a malicious keylogger accesses an application, the threat actor can easily gain control of the application using stolen credentials. Finally, SaaS security controls rely heavily on user identity. These identities can be compromised, and threat actors can enter the application to download, encrypt or otherwise interrupt operations.

Our solution addresses all these issues and more. It provides security teams with full visibility into every setting, alerting security teams when configurations change and providing steps for remediation. Security teams can also identify all connected third-party applications and their permission scopes, as well as associate poor hygiene devices with their users and monitor users to help detect any threat actors that have entered the SaaS app.

TAG Cyber: What is SSPM and why is it critical?

ADAPTIVE SHIELD: SSPM stands for SaaS Security Posture Management. It is nearly impossible to manually secure SaaS settings, and tools like cloud access security brokers (CASB) can't provide insight into each individual application's settings. SSPMs perform automated checks of all security settings across all users and applications, while providing deep and continuous visibility into the SaaS stack and its security controls. SSPMs, however, may not go far enough in meeting the needs facing organizations. Adaptive Shield has evolved beyond posture management to include SaaS threat detection and response (TDR) capabilities. The complete cycle of ensured, continuous security starts with a strong posture as a prevention layer, thereby minimizing the chance of introducing a threat. If a threat is detected, TDR mechanisms are crucial in achieving a secure ecosystem.

TAG Cyber: What are the key features of Adaptive Shield?

ADAPTIVE SHIELD: We protect SaaS applications by helping apps retain their security posture by providing SaaS identity threat detection and response (SaaS ITDR). We've recently added two new key features that are very exciting for the SaaS security world. First, we've started to expand into threat detection, so we are using user entity and behavior analytics (UEBA) data, IP information, threat intelligence and logs to identify threat actors that are entering into a SaaS application. Second, we've added data leakage protection to SaaS. This will alert the security team when assets—such as documents, reports and videos—aren't being protected and can be downloaded by anyone with the link. Our platform also includes everything else you'd expect from a SSPM service. We check configurations for each user in every application, offering the most advanced solution on the market today. We also review connected third-party apps. The security team has full visibility into all apps that are connected, along

with their authorized scopes. They are alerted when employees inadvertently integrate malicious applications into the SaaS stack. One of the more unique features about our platform is its ability to correlate user data with devices, so the security team knows when a high-privileged user is using a low-hygiene or unmanaged device. Since we have the user information, we also review identity and access governance to ensure best practices are being followed across the SaaS stack.

TAG Cyber: Adaptive Shield enables security teams to gain complete control of the SaaS security ecosystem. What does this entail?

ADAPTIVE SHIELD: Our SaaS application integrates with all SaaS applications, enabling security teams to be in control of the SaaS landscape. Once applications are connected to the platform, the security team has visibility into all security controls and third-party applications, as well as detected threats and users accessing the SaaS application. As a result, it can respond or open a ticket, and subsequently guide the application owner through the remediation process. Adaptive Shield is also used as a collaboration tool between the security team and business owners, ensuring a smooth and efficient remediation process. Additionally, integrations with unified endpoint management (UEM) systems are available, in order to incorporate the user's device hygiene score as part of the overall SaaS posture.

TAG Cyber: What is the top cyber threat facing companies in 2023?

ADAPTIVE SHIELD: From a SaaS perspective, the top threats are misconfigurations. We keep seeing more and more severe attacks occurring as a result of misconfigurations. For example, [Nissan's recent breach](#) and the recent [Slack Github breach](#) from the past two weeks.





AN INTERVIEW WITH TOM TOVAR,
CEO AND CO-CREATOR, APPDOME

PROTECT IOS AND ANDROID APPS WITH APPDOME

More and more people are using their devices for things like banking and online shopping. As phones and tablets can easily be lost and stolen, it is imperative that app developers provide the highest levels of security to end users to avoid massive financial loss or identity theft.

Appdome's simple solution protects and monitors iOS and Android devices from attacks, fraud, malware, hacks, cheats and other security breaches, all from inside the mobile DevOps CI/CD pipeline. Now used by close to 800 companies globally, including some of the world's major banks, Appdome allows mobile protections to be implemented in mere minutes. We met with Appdome to hear more about their innovative product.

TAG Cyber: Tell us more about Cyber Defense Automation and how it works.

APPDOME: Cyber Defense Automation is about using technology to build, test and release mobile app protections inside mobile apps in the CI/CD pipeline. Mobile app protection is any class of client-side security, anti-fraud, anti-malware, anti-bot and/or anti-cheat defense needed inside an Android or iOS app. The value of Cyber Defense Automation is that it allows cyber and Dev teams to leverage configuration as code to design, build, record and release protections in mobile apps collaboratively—the same way Devs build the app. Our Cyber Defense Automation platform does just that, providing visibility, management and control via Certify Secure protection certification and the real-time monitoring of threats and attacks against Android and iOS mobile apps. Using Appdome, mobile security and Dev teams can automate the delivery of mobile cyberdefense in Android and iOS apps, thereby protecting a mobile brand with ease, agility and scale. No code, no SDKs and no servers required.

TAG Cyber: How easy is it for customers to create and update apps securely? What security features do you offer?

APPDOME: Our solution protects against thousands of security risks, attacks and threats, including hackers, fraud, malware, bots and cheats. All protections are available using configuration as code to make it easy for the developer to add or subtract protections as needed. The list of protections is continuously updated, and available to all customers via a SaaS delivery model. Appdome is also fully

The consumer is mobile. Therefore, the top cyber threat facing brands in 2023 is mobile apps.



automated and easy to use with any class of mobile app. Developers enjoy agility and compatibility with any Android or iOS app, whether built natively or in a wide array of frameworks. Additionally, Appdome automatically builds chosen mobile protections into a mobile app in seconds.

TAG Cyber: What industry sectors do you specialize in and how is your solution tailor-made to meet their specific needs?

APPDOME: We are focused on the market sectors with the highest need for mobile app protection, the highest velocity of release cycles and the most demanding end users. Mobile apps that need the highest level of protection and have the most demanding release cycles include those for banking, financial services, retail, m-commerce, travel, healthcare, m-health, work and mobile games. Developers of these apps have an almost impossible task when it comes to protecting their applications. First, the delivery pace is high—often greater than 48x updates/releases per year per OS. Due to the nature of these apps, each of them faces hyper and persistent activity from attackers, malware, fraudsters and others. Finally, each app must regularly demonstrate compliance with the growing list of internal and external security, anti-fraud, anti-malware and other requirements. Our Cyber Defense Platform is purpose-built for these markets and this environment. Not only does Appdome leverage technology to accelerate the delivery of protections into any mobile app, but, on top of that, it eliminates the learning curve, resource allocation, guess work and trial and error that are often associated with other approaches to mobile app protections. As a system of record and collaboration for all teams, Appdome improves work quality and experience for cyber, mobile Dev, DevOps and DevSecOps teams by providing transparency, visibility and real-time validation and data for all protections released into mobile apps in the DevOps lifecycle. Finally, our Threat-Events in-app intelligence and UX/UI experience framework also allow granular insight and total control over the user experience when attacks happen.

TAG Cyber: How does your product ward off poor user experiences?

APPDOME: Experience is everything, and Appdome strives to ensure that our customers' mobile end users have the best possible experience when using an Appdome-secured app. Using our mobile app attack and threat intelligence suite, our customers can fully monitor and detect threats and attacks in real time for their in-production apps, as well as instantly remediate threats and attacks using threat telemetry data that informs the security model and allows customers to prioritize which protections to deliver in the next release. We offer solutions that allow Dev teams to completely control the user experience

(UI/UX) when threats or attacks are detected, ranging from custom pop-up notifications to the application of security to specific workflows in the app. We also offer a remediation center for our customers' support teams to help identify and resolve security incidents and get users back up and running using the secured app.

TAG Cyber: What is the top cyber threat facing companies in 2023?

APPDOME: The consumer is mobile. Therefore, the top cyber threat facing brands in 2023 is mobile apps. Today's cybersecurity teams are outmatched, outnumbered and outgunned by hackers and cybercriminals who, years ago, took a mobile-first or mobile-only approach to creating exploits. These cyber criminals have created their own exploit economy and have continued to leverage technology, automation and malware to deliver sophisticated attacks. Using automation, malicious programs, bots, trojans and malware to do most of their dirty work, attackers simply lie in wait for an end user to download an app to a device. Modern cybercriminals hack at scale, automate attack execution, and chain together attacks using an ever-increasing arsenal of freely available, open-source and commercial-grade hacking tools and frameworks such as Bluestacks, Frida, Magisk, and many more. These tools allow attackers to understand how apps work from the inside out, as well as to dynamically instrument and alter app behavior during runtime, thereby producing attacks so sophisticated that even trained security pros cannot tell the difference between malware and the actual app. Global consumers are not clueless either. Their expectations for mobile app protection continue to grow higher and diversify well beyond mere data and login protection. In a recent survey conducted by Appdome, we found that proper security, anti-fraud and anti-malware protections will lead to active consumer brand advocacy, reduced customer acquisition costs, higher average revenue per unit (ARPU) and reduced churn. It's important for mobile developers and CISO teams to move quickly to implement improved security measures in Android and iOS apps.



AN INTERVIEW WITH GAURAV BANGA,
FOUNDER AND CEO, BALBIX

AUTOMATE YOUR CYBERSECURITY POSTURE WITH BALBIX

Even with a wide variety of tools at their service, InfoSec teams that rely on manual workflows can no longer keep up with the ever-expanding enterprise attack surface. Networks can be compromised in an almost limitless number of ways, and these vulnerabilities open up businesses and organizations to serious damage.


Balbix automates cybersecurity posture by taking an accurate inventory of assets, while identifying the riskiest areas of the attack surface. It is geared to both mature and developing InfoSec programs in everything from start-ups to Fortune 500 companies. This scalable solution integrates with existing tools to reduce breach risk. We met with Balbix to learn more about their AI-powered approach to cybersecurity.

TAG Cyber: Modern-day teams are drowning in cybersecurity data. How does your solution help them process this information overload to gain practical, useful insights?

BALBIX: Modern enterprises use dozens of cybersecurity tools, with each tool generating useful data about certain aspects of cybersecurity. Aggregating this data to produce a “big picture” of cyber risk has typically been done manually, often using proprietary algorithms and methods. Unfortunately, in recent years, this task has become untenable due to the exploding complexity of InfoSec programs. We must deal with different tool data formats and often inconsistent duplicates, as well as missing data about business context. The complex math required to calculate the next best steps for risk mitigation is nearly impossible. Furthermore, these aggregated models quickly become stale, because manual methods can’t keep up with constant changes in the threat landscape.

Our platform addresses this challenge by leveraging automation and AI. It continuously ingests and analyzes data from a company’s cybersecurity and IT tools to build a unified risk model. The system brings together data about vulnerabilities, threats, exposure, security controls and business criticality to prioritize security issues and surface the next best steps for risk reduction. The Balbix risk model is denominated in dollars (or other money units) and essentially maps from a digital/IT footprint to business risk. Security professionals can slice and dice their overall cyber risk in a variety of pivots—by business unit, attack vector, risk owner, etc.—and trace from dollars of business risk to the specific issues

Over a hundred machine-learning algorithms work together to normalize, deduplicate and correlate data to produce a unified picture of asset inventory and cyber risk.



driving risk. Our platform enables CISOs and their teams to make better cybersecurity decisions based on facts. An enterprise can build real-time cyber risk dashboards for business stakeholders, leading to the gamification of risk management. It also enables automated workflows for vulnerability management, which results in the faster mitigation of security risk issues. Ultimately, Balbix helps organizations drive increased efficiency, cyber risk reduction, cost avoidance and cost savings.

TAG Cyber: How does Balbix assist in automating vulnerability management?

BALBIX: With our solution, organizations can maximally automate workflows for identifying and prioritizing vulnerabilities, by dispatching these issues to risk owners and then driving mitigation and verification. To automate vulnerability assessment, Balbix maintains a comprehensive, real-time asset inventory and software bill of materials for the enterprise. This information is continuously evaluated against vulnerability data provided by software vendors, government sources and researchers to identify and tag vulnerable assets. Our platform automatically maps vulnerabilities to TTPs and continuously tracks real-world threat information. For each vulnerability instance on every asset, Balbix evaluates the effectiveness of security controls against these TTPs, as well as the business criticality of the asset to determine priority. Our platform also provides specific patch/fix information and other context to support mitigation efforts by relevant risk owners. If stakeholders choose to accept risk for some issues, then Balbix tracks this information. With Balbix, organizations can calculate and configure appropriate service level agreements (SLAs) for vulnerability management, based on their risk appetite and tolerance. Companies can build dashboards and reports to track/trend SLA compliance and cyber risk for each risk owner, asset type, application and business unit—geo, as well as the overall enterprise.

TAG Cyber: Tell us about the benefits of your Asset Inventory dashboard.

BALBIX: Our asset inventory dashboard provides organizations with a comprehensive and real-time view of the enterprise's asset inventory and software bill of materials. The Balbix data model includes over 450 distinct asset attribute types, all of which are surfaced in our asset inventory views. In addition, applications are mapped to the corresponding infrastructure asset, and each asset is tagged with relevant business context. With our asset inventory, security and IT professionals have the accurate, comprehensive information that is needed in their daily tasks. They save time that otherwise would be needed to follow and correlate information across multiple tools. There is no need to export and analyze data in Excel while solving

problems, validating compliance or reporting. Overall, this saves up to hundreds, sometimes thousands, of hours of effort. Perhaps most importantly, Balbix Asset Inventory provides more than just visibility; it is tightly integrated into other Balbix capabilities that deliver maximally automated risk prioritization and mitigation.

TAG Cyber: What is the “Balbix Brain” and how does it help companies use AI to stay ahead of cyberattacks?

BALBIX: The Balbix Brain continuously ingests data from enterprise cybersecurity and IT tools, as well as external data sources. Over a hundred machine-learning algorithms work together to normalize, deduplicate and correlate data to produce a unified picture of asset inventory and cyber risk. The system brings together data about vulnerabilities, threats, exposure, security controls and business criticality, as well as performing probabilistic math calculations for cyber risk—asset by asset, application by application, and group by group across the enterprise. Unlike other AI platforms, the Balbix Brain was specifically designed for the model to explain itself and support traceability from dollars of risk to drivers of risk. As the complexity of the enterprise attack surface increases, cybersecurity data analysis becomes increasingly difficult. Balbix Brain provides critical capabilities for organizations to understand their gaps and associated risks, and close these gaps before adversaries can cause damage.

TAG Cyber: What are the top cyber risks facing companies in 2023?

BALBIX: There are three drivers making cybersecurity in 2023 more challenging than before. First, there is *AI/ML powered innovation in cyberattacks*. For example, the AI chatbot, ChatGPT, is already being used to generate very sophisticated phishing attacks. Most organizations are completely unprepared for automated AI-powered cyberattacks. Next is *flat or reduced cybersecurity spending*. Many InfoSec teams are facing budget cuts for tools and people due to the poor macroeconomic outlook. Unless organizations make a concerted effort to do more with less by leveraging more automation, they will face sharply higher cyber risk. Finally, there are the factors of *hopelessness, indifference and hubris*. Will your current InfoSec setup—people, processes and tools—deliver in 2023? Now is the time to take a step back and review if you have a good handle of your attack surface, and how your mean time to mitigate (MTTM) risk stacks up against the adversary’s key metric—i.e., less than 15 days to weaponize newly found security vulnerabilities. Do all your stakeholders understand the amount of cyber risk you have on the books in dollar terms, and are they engaged actively in risk management? You may not like the results of your review, but now’s the time to act!



AN INTERVIEW WITH KEVIN HANES,
CEO, CYBRARY

CYBRARY'S TRAINING COURSES FILL THE CYBERSECURITY SKILLS GAP

The fast-changing cybersecurity landscape requires professionals in the field to keep up to date with a never-ending stream of new knowledge. At the same time, the sector is facing a lack of skilled, certified workers.

Cybrary offers cybersecurity training geared to individuals and teams, both novices and seasoned professionals alike. Businesses can guarantee their workforce keeps abreast of the latest developments with courses that also prepare participants for certification exams. Instructors have practical, real-world knowledge that comes from on-the-job experience. With over three million registered users—ranging from individuals, service providers and government agencies to Fortune 1000 organizations—the company's strong, proven track record makes it a leader in the industry. Recently, we interviewed Cybrary to learn more about their training courses.

TAG Cyber: How do you help companies close their skills gaps? Do you create tailor-made solutions geared to their unique needs?

CYBRARY: The first step to closing skills gaps within an organization is identifying them. Cybrary enables our customers to accomplish this with our advanced assessment capabilities. By leveraging the analytics provided through the Cybrary platform, leaders can easily see where their employees have opportunities to improve. These same tools can also be used to baseline the skills of the entire team as a whole. With all of this information, we are then able to work with organizations to create custom training programs aligned directly with their goals. Whether a team's training goals are focused around certifications, career growth, onboarding, or all of the above, we work with leaders to develop a full-scale program that will have the most significant impact. Moreover, we update our courses depending on the type of content in consideration. We are constantly reviewing our courseware and adding new learning experiences to the platform with speed. For example, our certification preparation materials are refreshed based on the certification body's schedule, whereas our threat-informed training is reflective of what is happening in the industry. Whether there is a brand new CVE making headlines or a new threat-actor behavior being reported, the Cybrary Threat Intelligence Group is on top of it and making sure these updates are reflected in the training content.

Organizations need to expand their recruiting efforts and tap into more diverse talent pools.

TAG Cyber: What certification prep programs do you provide?

CYBRARY: From ISC2's CISSP to CompTIA's Security+, Cybrary offers certification prep for the majority of cybersecurity industry-recognized certifications. We also provide resources for tool-specific certifications, such as Azure, as well as emerging programs like the MITRE ATT&CK Defender (MAD) certification. Our full certification prep experience includes not just the courseware but also unlimited access to any applicable pre-test assessments, practice exams and practice lab environments. Our step-by-step approach is designed to get learners exam ready.

TAG Cyber: You offer more than just courses. What other services are available to participants?

CYBRARY: In addition to our on-demand video courses, Cybrary specializes in threat-informed training, live training, hands-on labs, assessment tools, practice exams and career paths. In 2022, we invested in building the Cybrary Threat Intelligence Group (CTIG) to help drive the creation of our training content and expanded research opportunities. We introduced our new Threat Actor Campaign (TAC) and CVE series, designed to help our learners stay up to date on the latest threats and trends in our space. I'm most excited about these new resources that are helping learners gain a deeper understanding of advanced persistent threats (APTs) by allowing them to experience critical vulnerabilities through interactive courses and secure virtual environments where they can develop the skills necessary to mitigate risk to their organization. It is critical that we provide Cybrary learners with not just the foundational knowledge to land a cybersecurity job but also support them in their career journey and beyond.

TAG Cyber: How does Cybrary help organizations attract and retain cybersecurity talent?

CYBRARY: Organizations need to expand their recruiting efforts and tap into more diverse talent pools. For example, this can be done by investing in individuals who may not come from a traditional technology background but have the drive and aptitude to excel in cyber, thereby expanding your reach. Additionally, there are significant benefits for everyone when you take someone who is already working for your company and upskill them. If they are technically orientated and love to solve problems, why not invest in them? Workforce transformation within your own company can be a game changer. Once you've attracted the right talent, you need to retain these individuals by

investing in their skill development, as well as their future at your organization. Be sure your team members understand how their careers can progress at your company by providing them with the necessary tools and resources to get them there.

TAG Cyber: What is the top cyber threat facing companies in 2023?

CYBRARY: This is a time of economic uncertainty when we are all trying to do more with less, all while threats are ever growing. As an industry, I believe the top cyber threat we will face this year is a lack of resiliency and preparedness. Especially now, it is critical that we continue to invest in our people and do our best to stay informed and ahead of threat actors.





AN INTERVIEW WITH YOTAM SEGEV,
CEO AND CO-FOUNDER, CYERA

HOLISTIC CLOUD-FIRST DATA SECURITY FROM CYERA

Data is increasingly one of the most valuable assets of any modern-day business. As such, it is of utmost importance to secure it from attack and misuse. For security teams, it is a significant challenge to remain aware of what data the business manages, where it is located, and who has access to it. Data is also the focus of a growing number of increasingly stringent regulations.

To address these challenges, Cyera offers a cloud-first approach to data security in the recently emerging space of data security posture management. We talked with Cyera to learn more about their product, its benefits and how it works.

TAG Cyber: How does Cyera differ from traditional data security solutions?

CYERA: Our holistic approach to data defense minimizes human involvement, works across the cloud data landscape, and dynamically discovers new, changed or eliminated data, thereby enabling data defense programs to be more efficient and effective. We have architected a fully automated process for continuously discovering data stores and providing deep context on data. This process focuses on leveraging native APIs to create and maintain a dynamic data-store inventory, in order to eliminate the effort and overhead inherent in manual IT service catalog creation, as well as the reliance on agents deployed to infrastructure environments. There are no agents, network footprints or hardware required. This means no performance overhead, no impact on data processing, and no ongoing maintenance.

TAG Cyber: Does Cyera help teams save time? In what ways?

CYERA: In a word, yes. For example, a customer in the pharmaceutical industry recently quantified that Cyera brought down the mean time to identify security exposures by 87%. We help save security teams time in several ways. First, we dynamically discover data stores in their environments; this eliminates the overhead of time-consuming audits, surveys and attestations when it comes to understanding where data is being managed in a business. We also identify the unknowns that increase risk. Then, we automatically and continuously classify and determine the context of sensitive data, eliminating the need for manual data definitions and laborious tagging processes, as well as tuning and tweaking

Legacy processes and tools leave businesses exposed to increased amounts of risk as they embrace the cloud.

the logic to eradicate false positives. This allows us to deliver automated remediation workflows with specific guidance for addressing security exposures. When Cyera detects an issue, our toolchain integrations can open a ticket or pull request, kick off an automation routine, or enrich signals in a SIEM or other security solution with the full context of the exposure and how to remediate it. Customers use this to respond to security, privacy or regulatory audits, saving the time and effort required to identify where data is managed and who has access to it. It also streamlines vulnerability management and incident response workflows. Our API provides context on the potential blast radius from a threat signal, accelerating the mean time to resolve an incident.

TAG Cyber: How is cloud security managed differently than on-premise storage, and how does this effect the attack surface?

CYERA: Modern businesses are creating and consuming data at an incredible pace, leveraging cloud technology to take advantage of the speed and agility it offers their teams to create new business opportunities and unlock the potential of customer engagements. The challenge is that legacy processes and tools leave businesses exposed to increased amounts of risk as they embrace the cloud. Data security, as a discipline, needs to evolve to overcome the challenges that the cloud era has introduced. Approximately 45% of the breaches IBM identified in their recent data-breach research were cloud-based, and 83% of the organizations studied had more than one data breach. Despite the attention paid to ransomware attacks in the media, the most common cause of a breach remains lost or stolen credentials. Businesses simply cannot detect these without powerful automation, machine learning, and an architecture that can be deployed and scale as easily as their cloud tools do.

TAG Cyber: Your machine learning algorithms use semantic classification. What is this, what does it do and why is it beneficial?

CYERA: Every environment that our solution analyzes is one of a kind. Businesses have unique data classes and proprietary data formats. Cyera leverages patent-pending technology using multidimensional correlation to identify these automatically. Our platform combines pre-defined data classes—which were trained using traditional mechanisms, including regular expressions and pattern-matching algorithms—with environment-specific analyses conducted by novel ML and NLP technologies to reach a very high degree of accuracy. The platform learns a customer's unique data and improves its accuracy with each scan, due to the increasing volume and variety of data available to the correlation engines. The result is similar to Exact Data Matching, but automatic. What does this mean in practice? We start by categorizing your data into personal, health, financial or secret data. We also identify whether the data represents

an employee, customer, partner or another type of individual or entity you do business with, in order to ensure that we can identify the real exposure to your data and prioritize only the most relevant and pressing issues stemming from real exposure. We also highlight the residency of the data—i.e., the region, country or state that it represents. Next, we look at whether the data is encrypted or if synthetic data is being used, and we also highlight whether this data can be used to uniquely identify someone. The goal is to ensure you know exactly what your data represents. It also avoids noisy alerts that cost you and your teams time and money by causing you to miss real problems that expose you to additional risk.

TAG Cyber: What is the top cyber threat facing companies in 2023?

CYERA: The devil they don't know. There's a saying: better to deal with the devil you know, than the devil you don't. Applying this logic to data seems apropos in today's climate of daily breach notifications, increasingly stringent regulations, and a fickle public whose loyalty has never been more fragile. As businesses increasingly adopt cloud technologies, it has never been harder—or more important—to discover the unknowns that put their business at risk. This lack of visibility and awareness leads to data breaches, unending ransomware attacks, and insider risks turning to insider threats through the misuse and lack of appropriate detection and controls. Regulators are imposing increasingly severe penalties for these exposures, but the real threat to business comes from lost employee productivity and the loss of consumer trust, which creates dramatically higher opportunity costs in the future.



“My wife! My bed! My 2023 Cybersecurity Budget Report!”



AN INTERVIEW WITH TOM BAIN,
EVP, MARKETING, FINITE STATE

MANAGE RISK ACROSS THE SOFTWARE SUPPLY CHAIN WITH FINITE STATE'S COMPREHENSIVE SCA AND SBOMS FOR THE CONNECTED WORLD

The rising popularity of the Internet of Things (IoT) and the proliferation of the connected world is creating an ever-widening attack vector for cyberattacks, bots, malware and even corporate espionage. Both device manufacturers and asset owners are left scrambling to keep up and make sure their connected devices and embedded systems are secure across the software supply chain.

Finite State enables organizations to simply and continuously manage risk across the entire software supply chain by offering unrivaled visibility into any-party software with its best-in-class binary analysis. Their easy-to-use platform correlates data from all of a company's AppSec security tools into a single pane of glass for maximum visibility. We were happy to talk with Finite State recently to learn more about their offer.

TAG Cyber: Why are Operational Technology (OT), IoT and other connected devices so vulnerable to attack and how does your solution address this challenge?

FINITE STATE: Connected product users can't always see how hard it is for product manufacturers to create accurate, complete inventories of the software components that make their products work. The reason isn't always intuitive, but just because they made their connected products, doesn't mean they can say what's in them. That's because the software that makes connected products work often comes from many different suppliers. Think about an IoT device like a wireless router. That wireless router has different chipsets that come with radio software, open-source software and many other kinds of software. Some of that software may be embedded within the device, which has a web interface, making it exploitable. It's that complexity that makes it hard to generate an inventory of what's in that device—a software bill of materials (SBOM)—to assess and strengthen its product and supply chain security. We help connected device users see into the devices they're using, because we create the most comprehensive SBOMs on the market, as well as provide the threat and vulnerability context that empowers them to move forward and address these risks.

The connected device security market is fragmented—just like the broader cybersecurity market.



TAG Cyber: How does your product help combat product security issues brought about by today's fragmented market and why does this make Finite State so unique?

FINITE STATE: The connected device security market is fragmented—just like the broader cybersecurity market. We surface vulnerabilities in a prioritized view to help customers reduce risk in a straight-forward, no-nonsense way. There isn't another solution on the market that can do what we do in a highly efficient and accurate manner. Additionally, we pursue a strategy of collaborating with partner solutions. In this way, we can make the most of the comparative strengths of other offerings that are equally invested in managing risk across the software supply chain, thereby bringing the best, most comprehensive AppSec and product security solutions to our customers. By partnering with other adjacent technologies and vertical market leaders, our goal is to be a single point of orchestration for product and application security that delivers an unprecedented, prioritized view of all firmware and application security risk. Through the collaborative, complementary strengths of our partners, we can further reduce the attack surface across connected devices, embedded systems and applications. We believe that the collaboration that comes with compatibility helps Finite State emerge as a unique offering, extending the breadth of AppSec, product security and IoT risk management to product security and DevSecOps teams. Through collaboration, we uniquely deliver massive-scale enrichment for prioritization, correlation and cooperation to automate software security across the software supply chain lifecycle.

TAG Cyber: What information is included in your SBOMs and cyber risk profiles?

FINITE STATE: Our solution surfaces critical vulnerabilities in a customer's connected products by producing the industry's most comprehensive SBOMs, and then linking those to CVEs and CWEs. We give users a single view into connected device risk, show CVEs and CWEs ranked by criticality, and surface the customers' highest-risk third-party components, helping them understand which of their components has the highest number of vulnerabilities that need to be addressed. Beyond SBOMs, we also deliver threat context to help our clients understand their cyber risk profile across their ecosystem of connected devices. To make the SBOMs we create actionable, our solution draws upon the most extensive device intelligence database in the industry and gives product security teams the intelligence and visibility they need to align the ground truth surfaced in their SBOMs with IoT and OT risk. Our SaaS-based solution is easy to implement, simple to scale and helps our customers accelerate speed to value.

TAG Cyber: Tell us about your new partnership program.

FINITE STATE: When we announced our partnership program last August, we set out to build a dynamic ecosystem of technologies that would work together in taking on connected device risk. We wanted partnerships that empower members to automate the assessment and triage of vulnerabilities and weaknesses to reduce application, product, and supply chain risk. In less than six months, we've built that program, which is based on making security decisions easy for our customers and our partners' customers. We enable our clients to more comprehensively discover, assess, prioritize, remediate and respond to connected device vulnerabilities. By collaborating through this partnership ecosystem, we're able to give our clients even fuller exploitability, vulnerability and threat context information that leads to better, more informed risk mitigation strategies. We've found that the partnership program has become a real strategic opportunity for us to provide comprehensive IoT and product security risk reduction strategies that empower the security functions of our clients and partners while continuing on our mission to manage risk across the software supply chain lifecycle.

TAG Cyber: What is the top cyber threat facing companies in 2023?

FINITE STATE: The growing interconnectedness of devices and the complexity of software supply chains are making it harder to understand what software is in a device, where it came from, and whether it's possible to mitigate vulnerabilities and risks, as well as how to do so. This is the top threat facing companies in 2023. This makes patching increasingly difficult in OT environments. As people and organizations increasingly adopt IoT and OT devices, they need a tool that sees inside these devices at scale and effectively mitigates connected device risk.

We firmly believe that tool is the SBOM. Since SBOMs enable decentralized vulnerability management, we don't have to depend on just one vulnerability source. With decentralized vulnerability management, we can look up every device that's ever been manufactured and know where vulnerabilities exist across the entire supply chain of that device. We know that doesn't scale; it's just not feasible for organizations to keep up with that. However, when it's done right, decentralized vulnerability management lets us get just enough security information from manufacturers to empower users to do vulnerability management on the risks that matter, without getting stuck waiting for manufacturers to tell them what software is on their devices and if they're exposed. This also builds on a secure-by-design principle that we apply to our daily objective—securing the connected world.



AN INTERVIEW WITH GAVIN REID, CISO AND HEAD OF THE SATORI THREAT INTELLIGENCE TEAM AT HUMAN SECURITY

HUMAN SECURITY: DISRUPTING DIGITAL FRAUD AND ABUSE WITH MODERN DEFENSE

Trying to weed out actual humans from online bot traffic can be a tricky business that has major consequences for security teams and the overall company. Bots can cause serious damage to an enterprise's reputation and bottom line through account theft and payment fraud, as well as fake account creation, reviews and comments.

Tracking over 20 trillion digital interactions each week, HUMAN Security offers a suite of products that prevents digital attacks, bots, fraud and account abuse. To make things easier, it does all the above with just a single line of code. We sat down with HUMAN to get an overview of their products, as well as the advantages they bring to businesses in advertising, marketing, government, education, e-commerce and enterprise security.

TAG Cyber: You started out in the back of a science fiction bookstore, tell us a bit more about your early days and your growth into a market leader.

HUMAN SECURITY: We have been protecting enterprises from digital fraud and abuse for over a decade. Originally based in the back of a sci-fi bookstore, we were founded by Tamer Hassan, Michael Tiffany, Dan Kaminsky and Ash Kalb with the mission to protect the integrity of the internet by disrupting the economics of cybercrime. Over the years, hackers have learned to deploy bots that are so advanced they're practically unstoppable. They're infiltrating companies, taking over accounts, creating fake ones, scraping websites for information and impacting transactions. If that wasn't bad enough, they're also using infected devices and sending fake requests to target websites and apps to steal money and disrupt operations.

Today, HUMAN Security verifies the humanity of trillions of digital interactions each week across billions of devices for more than 450 top enterprises and internet platforms. Thanks to our visibility across the internet, HUMAN is in the position to disrupt digital fraud and abuse through the continuous adaptation of dynamic network, device and behavioral signals. Furthermore, our Satori Threat Intelligence team performs takedowns and disruptions. Examples of our major takedowns of cybercriminal operations include: **3ve, Pareto, Scylla** and, most recently, **VASTFLUX**. All these takedowns have one thing in common: collective protection. Instead of companies and teams individually trying to protect themselves, we protect them all with our Human Defense Platform.

We predict that in 2023, companies will begin to band together to strengthen their defenses and take a stand against digital fraud and abuse.

TAG Cyber: What are the differences between human and non-human cybercrime that businesses need to be aware of when protecting themselves?

HUMAN SECURITY: Behind every cybercrime is a human. Whether they're using a sophisticated bot to execute the crime or not, we're dealing with cybercriminals trying to game enterprises at scale and make as much money as possible with as little cost or risk as possible. Over 77% of digital attacks use sophisticated bots to scale and obfuscate the attack path. For example, cybercriminals benefit from economies of scale by automating the verification of stolen credentials. While non-human and human attack vectors necessitate different detection and countermeasures, businesses can boost their security by fortifying apps, along with landing, login, transaction, checkout, and review pages by ensuring they are engaging with real humans.

TAG Cyber: Describe the key components of your modern defense strategy against bot attacks and fraud.

HUMAN SECURITY: Our technology, processes and relationships have been purposely designed to disrupt the economics of digital fraud and abuse by increasing the cost to cybercriminals, while also reducing the cost of collective protection. We call this "the modern defense strategy." Our visibility in the market is a key differentiator. Today, we verify 20 trillion interactions a week across a total of three billion devices monthly, enabling HUMAN to detect fraud and abuse with unparalleled scale, speed and precision. Our network effect is the feedback loop of technical evidence from up to 2,500 network, device and behavioral signals parsed through 350 algorithms looking for signs of digital fraud and abuse at the time of interaction. Our disruptions and takedowns are led by HUMAN's Satori Threat Intelligence team, which I lead. The team uncovers, reverse engineers and takes down digital fraud and abuse-driven threats. This stops the whack-a-mole process; when we disrupt or takedown a cybercriminal organization, their fraud and abuse go to zero for good.

TAG Cyber: Could you briefly list the various products you offer, as well as their main features?

HUMAN SECURITY: Our **Human Defense Platform** comprises a suite of products to protect organizations from digital fraud and abuse use cases, while our **Account Defender** product safeguards an organization's app and website accounts by detecting and neutralizing compromised and fake accounts. The **HUMAN Bot Defender** solution protects websites, mobile apps and APIs from automated attacks carried out by sophisticated bots. Next, there is our **Credential Intelligence** product that detects and stops the use of compromised credentials on websites and mobile apps in

real-time. To identify high risk PII, PCI and vulnerability incidents so response teams can act fast, **Code Defender** is a client-side web application security solution that provides comprehensive real-time visibility and granular control into a modern website's client-side supply chain attack surface. To stop marketing campaign fraud, we offer **BotGuard for Growth Marketing** that protects data pools from contamination by preventing sophisticated bots from converting on landing pages. We also offer **cleanAD**, an on-page, behavioral malvertising-prevention solution that protects publishers and platforms from digital attacks executed through the advertising ecosystem. Finally, to protect the programmatic advertising ecosystem and shield it from fraud, we offer **MediaGuard**, thereby improving quality and trust in the digital ad ecosystem.

TAG Cyber: What is the top cyber threat facing companies in 2023?

HUMAN SECURITY: Today's attackers are constantly upping their game to bypass a company's defenses. We're hearing from our clients that account takeovers, fake account creation, and web scraping attacks are becoming more prevalent, as attackers utilize automation to increase their level of sophistication. As a result, it's becoming harder for companies to distinguish between a human and a malicious entity. 'Digital fraud and abuse techniques that easily get past WAFs, CDNs and CAPTHCHAs, so ensuring you have the right protection is critical. That's where companies like HUMAN can help with modern defense and collective protection. We predict that in 2023, companies will begin to band together to strengthen their defenses and take a stand against digital fraud and abuse.



“Benjamin, regardless of your heroes, we are not going to call you Little Mudge”.



AN INTERVIEW WITH ANIL KARMEL,
CO-FOUNDER AND CEO, REGSCALE

SIMPLIFY SHIFT LEFT COMPLIANCE WITH REGSCALE

Companies are struggling under the burden of keeping up with constantly changing compliance and regulatory requirements. The inability to do so in a fast, efficient manner often results in costly fines and rising external auditing fees.

RegScale offers an automated, real-time GRC solution that mitigates risk, saves time, eliminates manual labor, and lowers costs. Used and trusted by major organizations in the U.S. and across the globe, including the U.S. Department of Homeland Security, RegScale works at scale to manage compliance programs. RegScale recently shared how their product offers continuous compliance, all while protecting sensitive compliance data, thanks to their enterprise-class cybersecurity.

TAG Cyber: What does “Shift Left Compliance” mean and what are its benefits?

REGSCALE: Developers used to write code that was then given to system administrators to implement. The system admins would test the code, find issues and report them back to developers to address. This back and forth took a lot of time and effort. After the application was deployed, security practitioners would come in and highlight all the security issues in the code. For this reason, the DevOps movement was born, which required a cultural transformation coupled with tooling to bring these disciplines together. Eventually, this discipline morphed into DevSecOps to embed security into the practice. The time has come to bring the principles of DevOps to compliance in a new discipline we can think of as Regulatory Operations or RegOps. A proposed definition of **RegOps** is as follows: “RegOps is the combination of cultural philosophies, practices, and tools that increases an organization’s ability to ensure compliance of applications and services against regulatory standards at high velocity: evolving and improving compliance and trust at a faster pace than organizations using traditional compliance artifact development and compliance management processes.”

Here at RegScale, we’re leading the Regulatory Operations movement to shift compliance left and make it real-time, continuous and complete. The result is that our customers can unlock digital transformation efforts, reduce their risk, and save money by automating and eliminating manual compliance processes and the associated paperwork. Finally, we take unstructured

The time has come to bring the principles of DevOps to compliance in a new discipline we can think of as Regulatory Operations or RegOps.

compliance data and make it digital and portable using our proprietary machine NIST's Open Security Controls Assessment Language (OSCAL), enabling a rich machine and human experience to minimize rework and accelerate time to value.

TAG Cyber: In what ways does your real-time compliance technology take things to the next level?

REGSCALE: Compliance gaps are typically discovered during an audit. Practitioners are tasked with compiling data manually from disparate systems to satisfy security controls, only to discover that many controls are not being met; this leads to audit findings and, even worse, compromised systems that incur fines and reputation loss. By moving compliance from a point in time to a near real-time, continuous activity, compliance gaps can be discovered quickly and remediated by practitioners before an audit even occurs. When auditors come onsite, audit-ready documentation can be produced on demand—and it's always right.

TAG Cyber: You state that RegScale is "purposefully designed to be different." How so?

REGSCALE: RegScale was built by practitioners for practitioners. As an API-centric platform, RegScale integrates with the security tools a company already owns and takes those findings as mapped to compliance controls. It also automates the creation of tickets in a ticketing system to keep compliance paperwork continuously up to date. RegScale delivers a great machine experience for machine-to-machine communication, as well as a great human experience for practitioners to manually document and assess controls in a system of record—bringing both worlds together to visualize compliance gaps and risks in near real time. Practitioners around the world have joined the Regulatory Operations movement with more than 300,000 downloads of our free Community Edition platform, while dozens of enterprise customers are experiencing the tangible business value RegScale delivers. Additionally, we ensure all organizations—regardless of size—have access to our real-time compliance automation platform through RegScale Community Edition (CE). RegScale CE is completely free to use with no restrictions, delivering rapid time to value with the ability to purchase a license key to unlock Enterprise Edition (EE) features. We believe compliance should be affordable, which is why we offer RegScale Community Edition as a platform to everyone who wants to get started on their RegOps journey.

TAG Cyber: How does your solution bridge the divide between security and compliance?

REGSCALE: We effectively bridge the divide between security and compliance through the power of the API, leveraging pre-built integrations with an organization's security and compliance

tools. Unlike the monolithic, first-generation of governance, risk and compliance (GRC) tools, which took an abundance of infrastructure to deploy, RegScale is API-centered, universally deployable and infinitely portable. This approach allows customers to realize additional value from their existing security and compliance investments, replete with flexible deployment options and the ability to share data across tools using OSCAL. The RegScale platform gives customers flexibility based on their unique business needs, along with the ability to scale as their compliance requirements evolve—all with value delivered in weeks, as opposed to months and years.

To get the docs into the machine, our proprietary digitization engine uses natural language processing to ingest existing Word documents, Excel spreadsheets and any associated regulations, bringing them into RegScale by leveraging our APIs. Many customers map their security controls across multiple regulations and keep that mapping up to date in an Excel spreadsheet. With RegScale, we enable organizations to bring their own mapping. Using our drag and drop wizards, customers define control equivalency, allowing the reuse of their evidence across multiple standards and frameworks. The power of our APIs also allows a company to visualize their compliance state and understand risk gaps in near real time by leveraging their Business Intelligence tool of choice. Alternatively, they can produce documentation in the Word or Excel templates favored by auditors and regulators. In short, RegScale is purpose-built to digitize, automate, transform and scale compliance programs, while simultaneously reducing risk, cost and time.

TAG Cyber: What is the top cyber threat facing companies in 2023?

REGSCALE: Organizations have to deal with a growing number of regulatory requirements coupled with an endless number of cybersecurity attacks, threatening the very core of their business. The rise of nation-state attacks, ransomware and phishing in all its forms are all competing for attention. On top of it all, we're entering a period of uncertainty, driving cost pressures on businesses to do more with less. Clearly, cybersecurity leaders need to evaluate their investments to determine where they can maximize their ROI. The area that has consistently driven budget is compliance, due to regulatory mandates and the impact on the business from audit failures. The rise of the RegOps movement can effectively drive down cost and risk, while simultaneously increasing speed and the assurance that a business is effectively meeting its ongoing regulatory obligations.



**ANALYST
REPORTS**



ENABLING TRUST IN ONLINE DIGITAL COMMERCE: AN INTRODUCTION TO THE DEDUCE PLATFORM

DR. EDWARD AMOROSO

The use of aggregate historical identity-backed behavioral intelligence at scale can serve as a foundational base for addressing the risk of fraud losses while optimizing trust across all steps of the user experience. The commercial Deduce Identity Platform exemplifies this approach to trust intelligence and proactive alerting.

INTRODUCTION

By some estimates, the global monetary losses in 2021 resulting from online fraud amounted to nearly \$95B. Such fraud is usually accomplished with attack strategies such as account takeover and fraudulent new account creation by criminal organizations. While insights from common exploits have helped defenders identify certain types of solutions, the reality is that most online businesses continue to struggle with effective approaches to reducing fraud loss.

According to many different estimates, companies will invest tens of billions of dollars this year to tackle identity fraud challenges. However, incorrectly identifying a returning customer or producing false positive data during account opening is costing businesses massive amounts of revenue (perhaps approaching a trillion dollars in aggregate). According to the FIDO Alliance, 58% of shopping carts are abandoned due to authentication friction.

The solution involves establishing a balance between excessive risk mitigation that causes false positive multifactor authentications or credit card declines, and a frictionless journey for new or returning customers to maximize the revenue potential from each transaction. To illustrate this challenge, the Deduce team reports that online merchants often struggle to establish an optimal approach to balancing controls versus avoidance of friction.

The team reports, for instance, that many merchants dial back fraud prevention technologies during peak and holiday selling periods to maximize transactions. Historically, this has always been an either/or scenario. However, as shown below, Deduce provides its online business customers with a solution that will prevent identity fraud, maximize trust, and streamline the online user experience.

In this report, we identify best practices for identifying trusted users across the digital ecosystem. This requires, as we will explain, cooperation between the security team and the user experience team. We show how data can measure not just fraud prevention, but loss of revenue caused by user friction, and we offer suggestions for measuring the efficacy of this cooperation.

WHAT IS CUSTOMER IDENTITY FRAUD?

An effective heuristic used by the most capable anti-fraud companies involves using aggregate historical behavioral intelligence to reduce risk. Empirical evidence suggests that this technique works well in practice (see discussion of the Deduce platform below). Such success might be explained by the availability of large volumes of online identity-backed activity data. It's now possible to collect relevant usage data from many tens of thousands of websites.

The journey a user takes when interacting with an online business involves four steps that are vulnerable to fraud. Reviewing these steps helps teams identify the major tasks and resources that require protection for any online business:

- **Step 1: Registration:** This first step is particularly important to the anti-fraud process because it occurs in advance of any user-authentication tasks. Registration thus involves activity initiated by both good users and fraudsters.
- **Step 2: Authentication:** The authentication step delineates the decision made as to whether a given user should be granted access to a desired resource. At a high level, anti-fraud techniques are often categorized as pre- and post-authentication.
- **Step 3: Account Changes:** This step involves the types of actions that can result in significant fraud and online security loss if not properly controlled. Any anti-fraud solution must include strong protections here.
- **Step 4: Checkout:** Many customer lifecycle security processes forget to include this important step, where bad actors can target credit card, identity, and other vulnerable soft spots. Anti-fraud tools must therefore include strong controls for checkout.

This customer journey provides a useful framework for the variety of anti-fraud measures that will apply to websites, apps, identities, events, and other attributes of any online eCommerce journey. Buyers of identity security solutions should ensure that the selected platform includes frictionless controls designed to optimize trust across each step on this digital journey because blind spots can be exploited by adversaries.

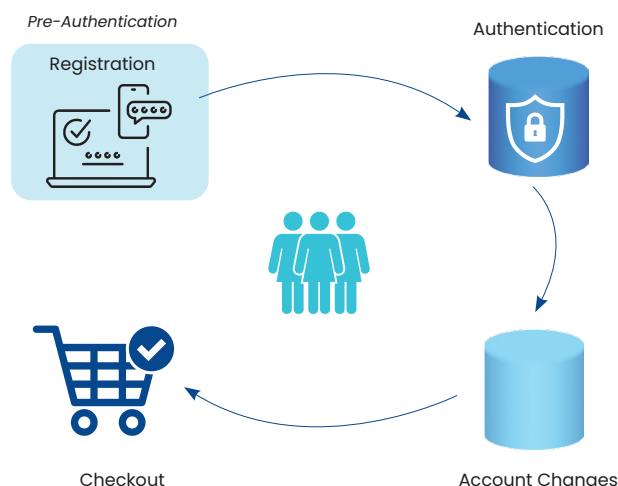


Figure 1. Customer Online Journey

THE PIVOTAL ROLE OF CUSTOMER IDENTITY ACCESS MANAGEMENT

Authentication for the customer journey occurs in the customer identity access management (CIAM) platform. Many CIAM platforms evolved from their enterprise identity access management counterpart, mostly on-premises technology that was designed to provide employee access to corporate IT infrastructure. For many businesses, the legacy CIAM platform is a weak link in the customer journey. Businesses can upgrade to cloud-based agile CIAM platforms that integrate comprehensive risk-decision engines and possess an orchestration layer to determine the authentication journey for each customer.

The transition from on-premises enterprise infrastructure, growing consumer UX demands, and eventual new regulations are driving demand for robust CIAM solutions. A new [Liminal CIAM market outlook report](#) states that CIAM providers which capture and unify consumer identity data such as user devices, behaviors, and other first-party data will be best positioned to capture the growing market opportunity.

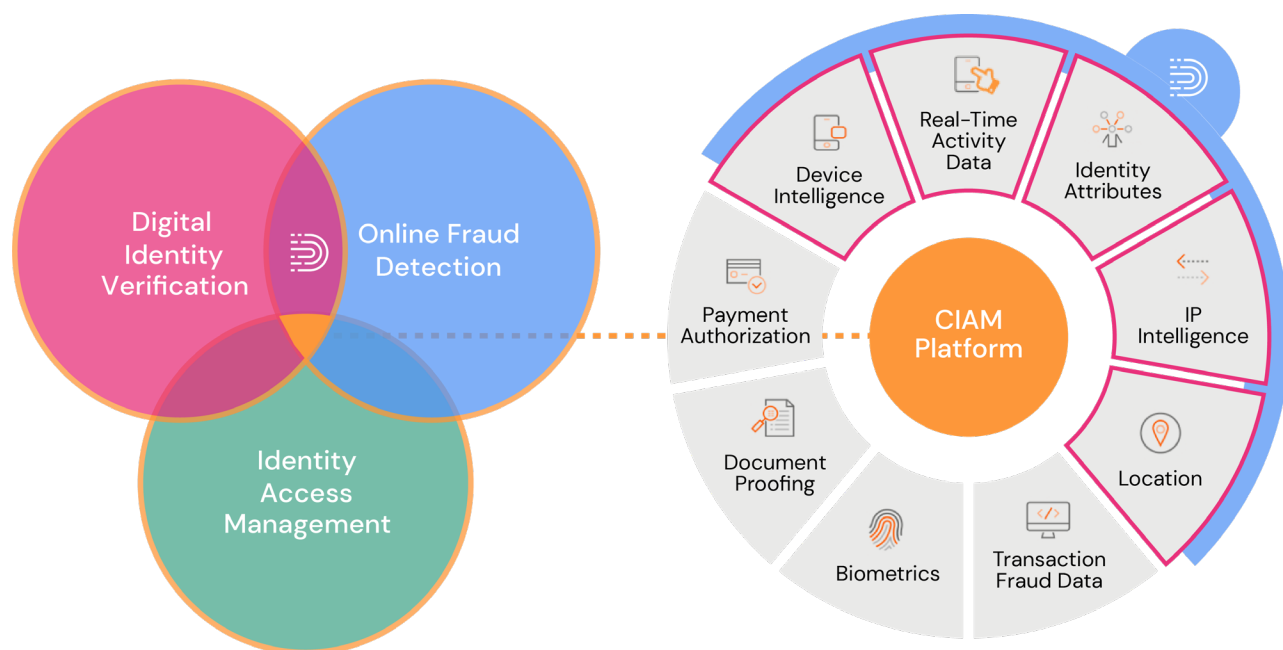


Figure 2: Customer Identity Access Management (CIAM)

Already, the CIAM market is seeing consolidation through acquisitions that support this shift in identity-related capabilities. So far in 2022, Thoma Bravo has acquired [ForgeRock \(FORG\) for \\$2.3B](#) and [Ping Identity \(PING\) for \\$2.8B](#), and [OKTA \(OKTA\) has acquired Auth0 for \\$6.5B](#) to complement their enterprise IAM business with a CIAM platform. Deduce provides these and other leading CIAM partners with the most advanced risk and trust engine to strengthen their value propositions.

THE NETWORK EFFECT: THE MISSING CIAM PLATFORM INGREDIENT

CIAM platform vendors face a major challenge: They do not own the data consumers generate by interacting online, so they cannot apply those identity insights to benefit all their clients. For example, if a known bad actor uses stolen credentials to defraud one CIAM client, the CIAM can't leverage the bad actor's identity data to protect other clients from that user. Likewise, the CIAM platform cannot apply identity intelligence across its customer base of consumer-facing websites and apps to identify legitimate customers, reduce false positives, and improve user experience.

GENERAL TECHNIQUES FOR REDUCING IDENTITY FRAUD RISK AND PROVIDING TRUSTED USER EXPERIENCES

To reduce identity fraud risk, the best commercial vendors can now leverage years of industry experience with online commerce. Past data related to identities can be combined with real-time telemetry into decision engines that can score the likelihood of a given engagement being fraudulent. We outline several of the more common algorithmic techniques for reducing customer identity fraud risk below.

Historical Identity-Backed Behavioral Intelligence

This approach involves establishing a trove of relevant information about user interactions with existing online businesses and services. The objective is to develop insights from as many different sources as possible. The historical data considered in scope should include usage telemetry from websites and applications and should create profiles of identities based on a combination of device, network, geography and activity.

Activity Coverage

This customer identity fraud reduction approach involves covering all phases of the user journey when interacting with online businesses. A key aspect of this coverage is addressing activity performed by users both before and after authentication. This is essential because fraudsters often exhibit behavior during registration that the detection algorithm should consider.

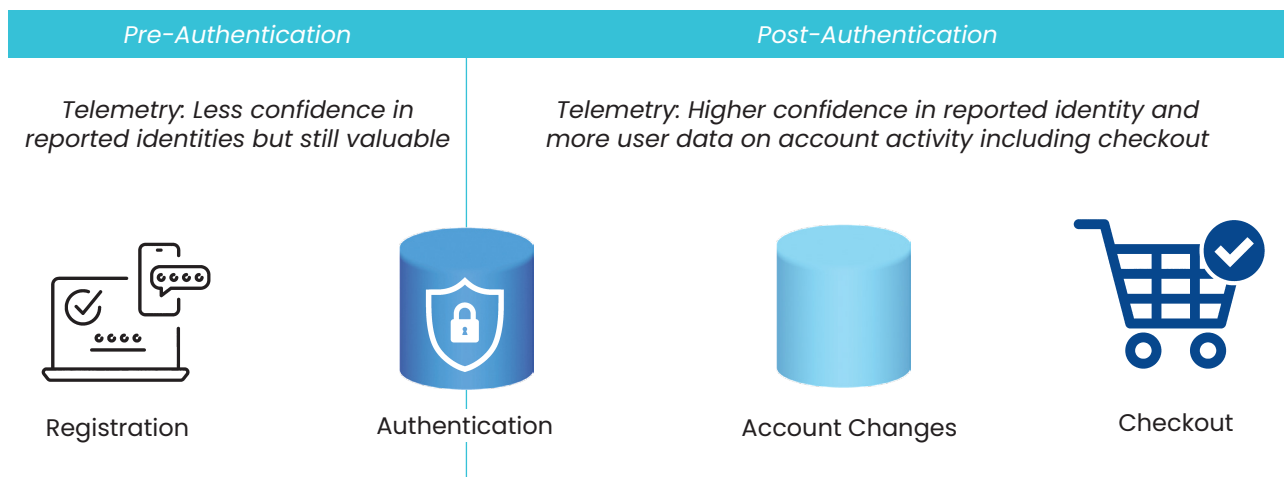


Figure 3. Pre- and Post-Authentication Activity Coverage

Behavioral Intelligence

This involves creating a stream of real-time behavioral intelligence related to identities that could be reasonably present in a given online ecosystem. The idea is that the intelligence allows an online provider to identify bad actors using telemetry, log information and data from many different dimensions of their behavior in other related contexts. This approach exhibits excellent scaling features because the data quality improves with increased volume.

This intelligence provides insights into the account creation workflow as it delivers a level of clairvoyance to security teams. It allows security teams to determine whether an identity has been acting normally before arriving at a website or app to create an account. It is also a predictor of user trust that can be applied to streamline the account creation journey. This can be done, for example, by eliminating the email verification step, which can reduce account creation churn. Data shows that if a behavioral network at scale has never seen an email before there is a significant likelihood that this account opening is fraud.

Risk Scoring

The creation of risk scores for identities enables making determinations about the nature and motivation of users. Furthermore, the decision engine for the best identity fraud solutions will offer a

probabilistic view of whether some actor should be considered malicious. The platform should also be adjustable (usually implying no code) to suit local online digital business requirements.

An additional desirable feature related to risk scoring involves the ability to add customized risk or trust signals to address specific types of fraud that might be germane to the specific application or service. Obviously, an online system will ultimately have to make a binary decision regarding user access, but the risk score will improve this process.

Customer Alerting and Multifactor Authentication

Alerting online customers to the presence of a bad actor is an important feature that online anti-fraud platforms should offer. The objective is to provide timely alerting to avoid the risk of bad actors gaining access to online services. Security teams have learned that fraud activity such as account takeover occurs quickly, so they must apply intelligence rapidly before such attacks can succeed.

An important benefit of having a dependable alerting option for the selected platform is that teams can use feedback in real-time to inform downstream decisions across the network. For example, a successful challenge confirming a customer's travel should then inform subsequent applications or services visited by that customer to avoid repeated challenges. This enables scaling of trust and risk avoidance across a wider scale of user experience.

Multifactor authentication also represents one of the most common causes of user friction. Incorrectly identifying a returning customer and requiring them to reauthenticate costs businesses in real terms and causes negative brand reputation. The security team should report false positive metrics to the business as a KPI so they can be monitored, and targets set to reduce the number and improve consumer experience.

Logged-In Session Extension

Perhaps one of the most valuable facilities enabled by modern CIAM platforms backed by real-time behavioral intelligence at scale is the ability to securely extend logged-in sessions for trusted users. This means that for online commerce businesses a returning trusted customer, once authenticated, would not be required to log in again and can advance straight to the checkout workflow, reducing a significant cause of cart abandonment and consumer frustration. The identity network monitors the online identity of the customer and suspicious behavior results in their trusted status being revoked and a requirement to reauthenticate on the site granting the session extension. Similarly, the network effect means that if the user authenticates on another site on the network, they can carry their authenticated status to other sites.

OVERVIEW OF DEDUCE PLATFORM

Founded in 2019 and headquartered in New York City, Deduce utilizes a large identity network to detect and mitigate fraud for online businesses. The founder, Ari Jacoby, had previously built companies employing large-scale identity graphs to combat bot traffic in the advertising industry. The knowledge gained from those experiences enabled Deduce to develop an effective fraud detection suite using an identity graph of cyber risk and fraud.

The company spent two years stealth-building its Deduce Identity Graph, which is a consortium of over 150,000 websites and apps, connecting over 550M U.S. identity profiles (many U.S. residents have more than one email address) and generating more than 1.5B events daily. Deduce sees most of the U.S. online transactional population multiple times per week.

In 2020, the company launched its first product, Deduce Identity Insights, to leverage the massive identity graph produced by the Deduce Identity Network. We outline the Deduce Identity Insights below in the context of the Deduce Identity Network. While we make every effort to include timely information, we encourage readers to contact the Deduce team for the most up-to-date product information.

Deduce Identity Insights

This platform capability provides the underlying processing, analysis and reporting functions required to prevent and detect fraud. The primary components of Deduce Identity Insights are outlined below.

- **Analytics** – The basis for analysis is the intelligence generated from the Deduce Identity Network, described earlier. The application of machine learning and data science generates risk and trust signals together with activity based on device, network, location and activity. The solution complements bot management solutions by focusing on identity, using algorithms that uncover anomalies in telemetry.
- **User Profiling** – This feature in the Identity Insight product involves the creation of digital fingerprints of user identities which are created from patterns of detected behavior. Factors included in the profiling algorithms are devices, geographic locations, usage patterns including time of day and other context-based attributes.
- **Risk Scoring** – The scoring process is based on collected input metadata which is analyzed and reviewed in the context of customized models to generate a quantitative score. The goal is to provide guidance for users and online services about whether an action should be trusted, allowed, challenged or reviewed.

The Deduce Insights product can easily be deployed via an identity verification or consumer identity access management platform. Deduce is integrated into leading platforms in both categories including Ping Identity, ForgeRock, Auth0, Microsoft AD B2C, Strivacity and IDMe via a no-code deployment. These use cases enable the dragging and dropping of Deduce into workflows for account creation, authentication, password reset and so on.

ACTION PLAN

We advise online business operators to take immediate action to implement a CIAM and fraud program using a suitable commercial platform and associated set of processes. They can achieve this by following a simple management plan. Each of the four high-level steps must be decomposed into more granular tasks, but the overall approach should consider including the following:

Step 1: Inventory of Existing Fraud Approaches

The online security team should create an accurate inventory of existing approaches to detecting fraud and notifying customers. This can range from zero support to an existing platform with notification capabilities.

Step 2: Development of Online Identity Fraud Requirements

Once the security team establishes the inventory, they should create a set of antifraud requirements along the lines of the functions discussed in this report. The requirements should combine the best elements of approaches identified in the inventory.

Step 3: Commercial Platform Scan and Review

The next step involves scanning and reviewing available platforms, such as from Deduce, for suitability in the local environment. TAG Cyber analysts can assist with this task, which must consider non-functional items such as license terms and cost.

Step 4: Begin Gradual Transition and Integration

The final management step involves the transition and integration of the newly selected platform into the local online service ecosystem. The good news is that the types of tasks included in this area are highly conducive to a smooth transition.

TRANSFORMING ATTACK SURFACE MANAGEMENT AS A KEYSTONE TO THE MODERN SECURITY PROGRAM

JOHN J. MASSERINI

While most security executives will tell you that some of their biggest fears center around nation-state actors and ransomware, the reality is the root of that fear is the unknown. The lack of visibility into what devices are running, where those devices are and which applications are in use in today's enterprises marks a substantial risk that many overlook.

Today, many enterprises are dealing with the explosion of virtual environments and the rapid adoption of workloads on Amazon Web Services, Google Cloud Platform and Microsoft Azure, resulting in a substantial gap in most asset inventories. Identities and roles are being reused across assets and workloads, resulting in significant access control risks. Data stores, containing sensitive consumer health or financial data, are duplicated across testing and production cloud environments without oversight. Layer in the serverless API calls and application stacks that can be instantiated within minutes and most security teams are ill-equipped to manage the attack surface of the enterprise compute environment.

In this report, we will review the challenges of *attack surface management* within the enterprise, the necessity of automation in identifying and managing assets, and the importance of a centralized view into the entire device landscape.

INTRODUCTION

Based on research with enterprise security teams, TAG Cyber predicts that security spending on tools, solutions and suites for 2023 will remain stable, with roughly one-quarter of teams continuing to plan increases, mostly in critical infrastructure. The remaining 75% of enterprise teams are likely to remain flat or experience only a slight

decrease in their security investment. Such stability of budget reflects an increasing cyberthreat and a commensurate level of attention by executives and boards, balanced by market pressures to keep expenses low.

While enterprises continue to purchase technical solutions in the hope of mitigating various forms of risk, we continue to hear of companies suffering from ransomware attacks, corporate outages and sensitive information offered for sale on the darknet. The ever-changing threat landscape, along with the resource shortage and high turnover rates in security operations centers (SOC), coupled with the phenomena of alert overload is resulting in significant gaps in security tooling.

Additionally, many enterprises are well down the path of moving to the cloud, resulting in an explosion of virtual assets scattered across Amazon Web Services, Google Cloud Platform or Microsoft Azure. With the ephemeral nature of leveraging cloud solutions, most security teams are feeling the impact of the move to the cloud and the adoption of DevOps techniques, realizing that the significant churn of assets in the cloud is far more challenging than their legacy infrastructures. Couple this with the routine reuse of cloud identities and roles and the risks of cloud infrastructure surge by orders of magnitude.

All these factors leave an already struggling device and configuration management practice woefully unprepared to be the foundation of risk mitigation for the enterprise.

UNDERSTANDING ATTACK SURFACE MANAGEMENT CHALLENGES

To understand the challenges of today's attack surface, it's important to understand the legacy issues many enterprises deal with.

In a perfect world, whenever a new device or asset is put on the network, all the associated support teams would be notified accordingly. The server team would know to patch a new host; the IT team would know they need to manage access rights on it; the networking team would know what protocols are necessary for the applications running on it; and, not least, the security team would know to add it to their SOC monitoring and vulnerability management program.

Unfortunately, this process is far less successful for most large enterprises than one would imagine. Ask your average IT person in almost any enterprise how accurate their configuration management database is, and you'll likely get a chuckle or a half-hearted, "it's not bad." The hard truth is, asset management is an abysmal failure for many enterprises, and at least in part, responsible for the incredible spike in data breaches and ransomware events over the last several years.

While the challenges involved with tracking and maintaining legacy infrastructure are enough to make most technology teams give up, the addition of a rapidly growing list of cloud assets almost makes the effort pointless. In today's DevOps world, devices and hosts are instantiated or deleted almost continually, and any effort to track them manually would be not just futile, but also highly counter-productive.

RISKS OF NOT MANAGING YOUR ATTACK SURFACE

From **over \$34 billion in 2017 to almost \$58 billion in 2021**, worldwide spending on security technology has exploded. However, 2020 and 2021 were arguably the worst ever when it came to data breaches and ransomware incidents.

It goes without saying that there are many reasons for this, but the lack of a trustworthy record of devices throughout the enterprise is a key indicator that an organization's risk model is flawed.

Without a clear understanding of what devices are doing in your legacy and cloud environments, it is impossible to quantify the risk associated with configuration issues, missing patches or user access problems. Attack surface management (ASM) is far more than the legacy configuration management database—it requires understanding what applications are running on which devices in what networks and why that matters to the business.

This truly comes into play when we look at many of the recent major issues we have been dealing with as an industry. Without understanding your attack surface, it's impossible to know if you're exposed to threats such as [SolarWinds](#), [Log4Shell](#) or Spring4Shell. The failure of patching and configuration management is the primary casualty of poor device management.

Finally, a core functionality of any ASM platform is the ability to show the risks of a vulnerability in context to your environment. As most security teams understand, determining the risk to an organization based solely on CVSS score is not only inefficient, but leads to a false sense of security as well as significant "patch fatigue" resulting from the continual urgency to patch "critical" vulnerabilities. The ability to understand how the risk could be exploited within the confines of an enterprise's unique infrastructure is the true value of a modern-day vulnerability mitigation program.

The Impact of Cloud Deployments on ASM

As previously discussed, the legacy approach to device and asset management to mitigate risk has been a struggle for most organizations. When you consider the hybrid cloud infrastructure that exists at most enterprises, it's obvious that something needs to change.

When we consider the significant change the DevOps model has brought to the enterprise, it is more than a little naïve to believe that the legacy change management and device tracking process can be wedged into a DevOps sprint. Rather, in today's world, the development teams have the ability to stand up complete infrastructures, which historically relied on other IT infrastructure teams. Development teams can now instantiate a server, a database and the appropriate supporting applications with zero knowledge of the security teams highlighting the significant pre-delivery risks that can be introduced into any infrastructure.

The Challenges of Legacy Toolsets

As most security teams will attest, ensuring an accurate and up-to-date inventory is one of their biggest challenges. Successful vulnerability identification, endpoint protection solutions and SOC integrations all rely on knowing and understanding what is running in the environment. Unfortunately, legacy tool sets are ill-equipped to keep up with a modern ephemeral cloud environment. For example, if we rely on a legacy vulnerability scanner to identify new devices in our cloud environment, any vulnerabilities in workloads which are not actively running at the time of the scan would not be reflected, thereby skewing our results in a positive direction. Obviously, the fallacy with this approach is that such a solution only scans networks and devices it knows about and completely ignores those it doesn't. So, in the case of a new network being stood up, or more realistically, a new workload being published on AWS, if the security team is unaware of the new device's existence, it will never become part of the scanning practice.

Another struggle for many organizations is that even when they do manage to keep up with what is running in the infrastructure, fixing the issues presents its own unique challenges. Whether it is patching a critical vulnerability, or an unapproved system configuration change—Configuration Drift—correcting the issues identified by legacy scanning solutions often leaves teams completely overwhelmed. All

too frequently there are tens of thousands of vulnerabilities, if not hundreds of thousands for larger environments, that teams need to address. Trying to prioritize those patches or configuration updates is not only time-consuming but prone to mistakes due to the lack of understanding of the specific environment.

This issue continues to be exacerbated by the lack of correlation between the various tool sets used by many organizations. [A study in 2021](#) found that the average enterprise had 76 different security tools in use. This conglomeration of products and vendors all but guarantees misaligned priorities, mismanaged efforts and misrepresentation of the overall risk to the company.

A MODERN APPROACH TO ASM

When we consider the general failure of legacy asset management in most organizations, coupled with the significant change in the new development approach being adopted by those same enterprises, it becomes apparent that a new, modern approach to ASM is needed.

While many enterprises have undertaken consolidated reporting efforts to address the need to understand the environmental risks, often this is a unidirectional effort, i.e., data extracts are pulled from the various tools, consolidated into a data warehouse, models are run against the data and reports are generated. Rarely, if ever, is this data fed back into the originating tools to add valuable telemetry into the system. Additionally, due to the length of time it takes for report generation, feed ingestion, data correlation and reporting, the information provided by such efforts tends to be weeks old in the best of cases.

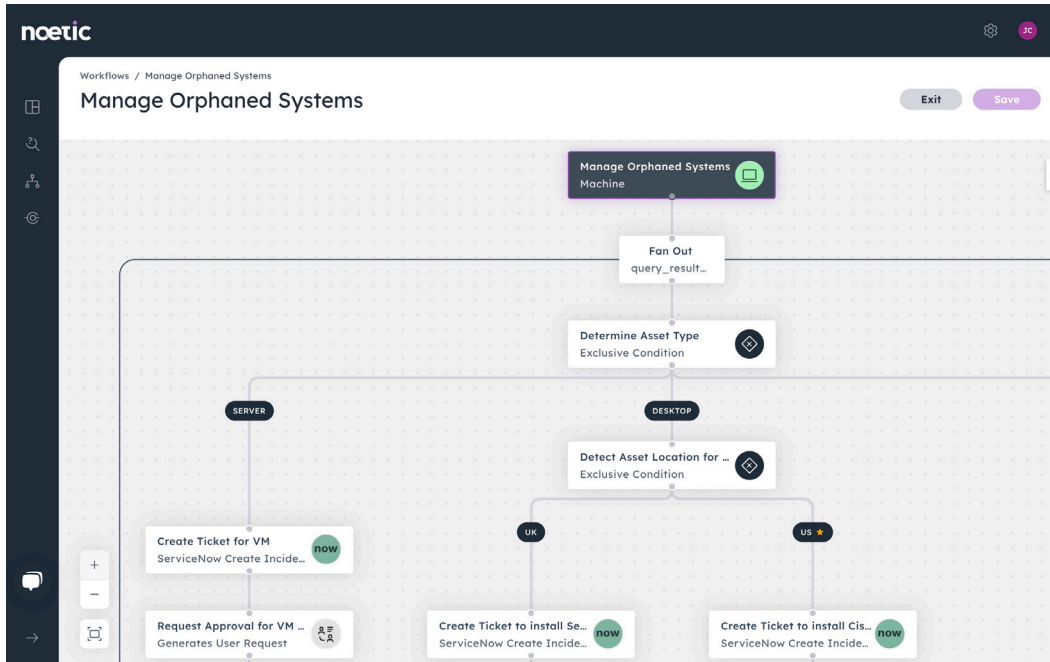
Today's dynamic enterprise environment needs a solution that can integrate with all the existing tool sets, from endpoint management and vulnerability scanners, to configuration management solutions and IT ticketing systems while integrating with the major cloud providers. The enterprise needs an *Attack Surface Warehouse*.

THE NOETIC PLATFORM OVERVIEW

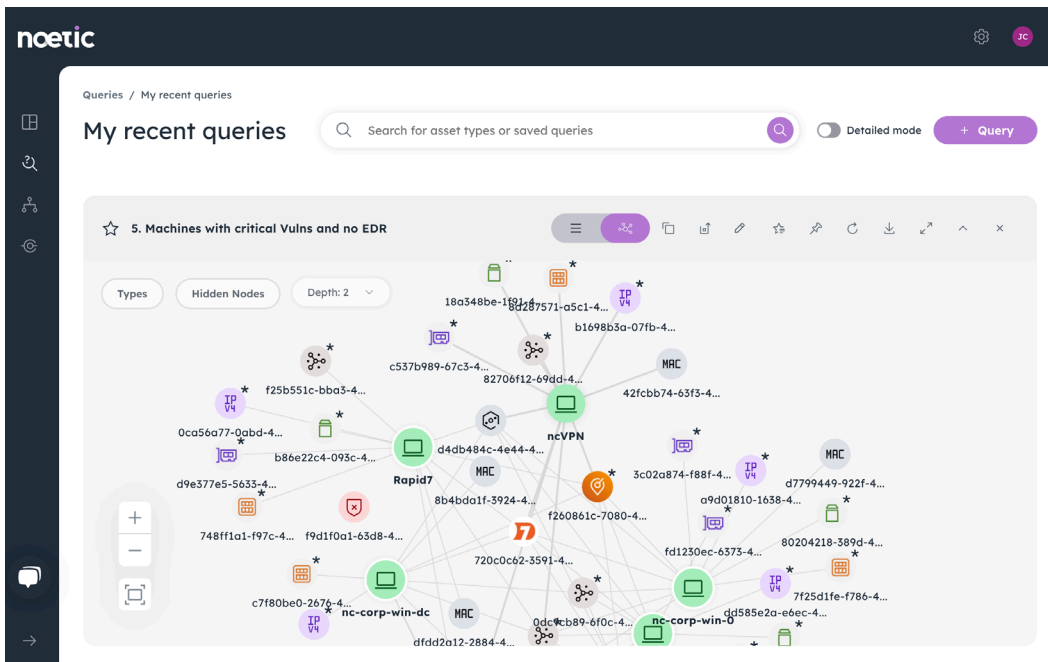
The Noetic platform addresses many of the significant asset management issues facing enterprises by addressing the many challenges of developing a risk-based asset information system.

Noetic can integrate with dozens of existing technology investments including endpoint solutions, vulnerability scanners, network monitors, IT ticketing systems and more to collect pertinent data already available within the enterprise and leverage it to create and enrich a continuously updated asset inventory. It is open, extensible and accessible via APIs to support custom integrations.

The platform uses a graph database that visualizes the cyber relationships between assets so users can easily understand the necessary security contexts and map the relationships between users, machines, vulnerabilities, networks, datasets and more.



The solution’s integrated automation and workflow capabilities also help the security team respond to the Configuration Drift that so often occurs in large enterprises. This can be end-to-end automation, driven from the Noetic platform, or simple notification and escalation to existing ticketing systems or SOAR tools as appropriate.



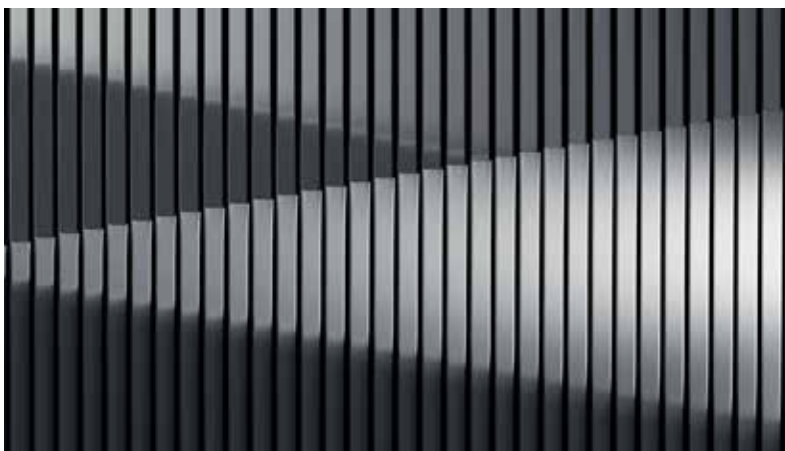
Noetic’s platform consolidates the multitude of existing security, DevOps and IT management tools into a unified risk-centric dashboard. It provides the security team with a clear view of risk and provides the IT team with context and insights into how to remediate pre-existing vulnerabilities or security coverage gaps. By leveraging the existing security infrastructure, Noetic continually assesses and evaluates the security posture of the environment, not only highlighting vulnerability-centric risks but also identifying new or missing devices as they appear, without adding to the overall complexity of the environment.

Finally, by providing a unified source of truth for assets across both on-premises infrastructure and cloud, the Noetic solution provides significant insight into asset and device configuration posture, vulnerability status and the actual risk of the identified issues mapped to the MITRE ATT&CK® matrix. These features, in combination with the integration of enterprise-specific business and technical data, provide a clear view of risk as it relates to your specific enterprise.

ACTION PLAN

Historically, security executives have had little influence over the legacy asset inventory function. While typically owned by IT, security teams considered themselves lucky just to be part of the provisioning/deprovisioning notification process. Today, however, security teams have powerful, self-contained options that will integrate and consolidate asset information across all verticals in the company, providing a risk-based ASM solution that will empower the security teams to focus on risk-quantified mitigation practices.

With the sheer number of vulnerabilities being identified annually, along with the countless number of nation-state adversaries and underground operators leveraging them, the modern enterprise must evolve from the “patch and scan” mentality and focus on moving from a basic vulnerability management program to a contemporary, multi-dimensional ASM approach. This effort will not only drive risk mitigation throughout the enterprise but will also align the security teams with a more business-centric approach, gaining wider acceptance throughout other IT teams along the way.





DELIVERING DIGITAL EXECUTIVE PROTECTION: AN INTRODUCTION TO BLACKCLOAK

DR. EDWARD AMOROSO

The need to provide concierge digital security support for corporate executives, high-access employees and prominent individuals has become well-established. Security start-up BlackCloak addresses this need through its Digital Executive Protection (DEP) solution that minimizes cybersecurity and privacy threats to these targeted individuals and groups.

INTRODUCTION

Enterprise teams have come to the recent understanding that an executive's personal digital presence has a significant impact on organizational cyber risk. When key personnel exercise sloppy security in their personal use of online accounts and services, or fail to remove personal data from online data brokers, exploitable risks emerge that can be targeted by bad actors. Risks also emerge from vulnerable home networks, unprotected personal devices and online accounts—not just of the executive, but also their families.

This report introduces and explains a new discipline known as *Digital Executive Protection (DEP)*, which is increasingly becoming a mandatory aspect of enterprise protection initiatives for corporate executives, board members and senior leaders with access. This approach also can be used to protect prominent, well-known individuals who must exercise prudence in their online presence to avoid targeted threats.

The commercial solution from **BlackCloak** provides effective DEP support for corporate enterprise buyers when it comes to protecting executives and other prominent individuals who are concerned with emerging digital risks to their business, personal finances, reputation or safety.

THE RISKS OF PERSONAL DIGITAL INFORMATION, DEVICES AND ONLINE PRESENCE

Digital risks to executives and prominent individuals span both cybersecurity and privacy. They emerge based on the so-called *personal digital lives* of these individuals, resulting in a concept often referred to as an attack surface. The most common risk elements associated with an executive's attack surface include the following threats, each of which are currently occurring on a regular basis:

- * **Targeted Attacks.** Executives and their families are commonly targeted for the purpose of financial attacks and online fraud, which can result in personal losses for the individual and their family, as well as be used to go after the assets of an enterprise. Online fraud is made easier by the mass availability of personal information— including cell-phone numbers, personal emails, home addresses, home IP addresses and other information—via online data brokers and social media.
- * **Identity Compromise.** There is a high potential for executives and other prominent individuals to lose their privacy and have their personal information stolen, which can then be used to open accounts, create tax fraud or purchase items. It can also be used to target enterprise resources if a company relies on personal information for authentication and authorization tasks, making identity theft a serious concern. Identity compromise can also lead to corporate data compromise and increase the likelihood for reputational attacks against an executive and the company.
- * **Modern Digital Threats.** In addition to fraud and identity compromise, executives must contend with additional risks originating in the home or on personal devices. These include: reputational attacks through deep fakes; phishing attacks to plant malware on personal devices and networks; and social engineering attacks aimed at a variety of different objectives. Prominent individuals and, by extension, their organizations must be on guard to avoid these risks, but they can also benefit from professional security assistance.

Organizations must pay close attention to these personal risks, because malicious actors now recognize that the path of least resistance to an enterprise's data, assets and resources exists through targeted executives. In other words, adversaries have learned that an executive's personal digital attack surface is a much softer means for gaining access to an enterprise, as opposed to trying to get through the layers of in-depth defense controls that protect a company's key assets.

An additional complication is that enterprise audits, assessments and reviews rarely consider the digital behavior and personas of their executives. The culture of enterprise security has maintained a focus on business assets, while the privacy of executives and their families has been considered a higher priority than the investigation of potential risk. This decision must be reconsidered, as the risk to executives continues to grow.

WHAT IS DIGITAL EXECUTIVE PROTECTION (DEP)?

A new form of cybersecurity protection has emerged known as *digital executive protection (DEP)*. The purpose of DEP is three-fold: namely, to reduce the personal digital risk of a targeted individual; diminish the risks associated with an individual's family and inner circle; and finally, lessen the risks associated with a targeted individual's enterprise or organization.

The manner in which DEP is offered varies between different commercial providers, but, in most cases, it includes a combination of technology, expert availability and supporting resources. This unique mix for

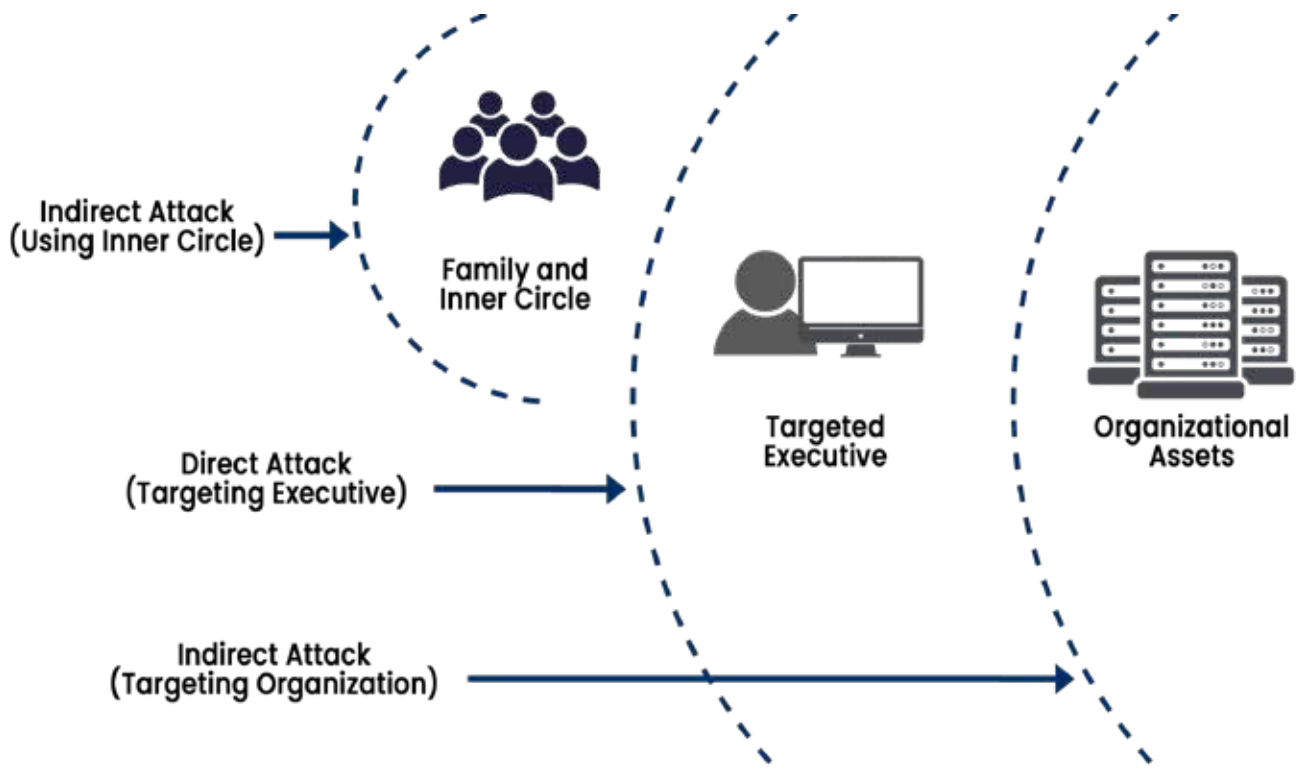


Figure 1. Indirect and Direct Targeted Attack Cases

executive protection requires that a DEP solution provider fully respects the many different requirements of its customers. Specifically, the following must be taken into consideration in any successful offer:

- **Privacy of Targeted Individuals.** Executives use personal online accounts for private, nonbusiness-related functions. These include community, family, church and other private activities, as well as sensitive communications with doctors, counselors or even competing enterprises. To this end, the DEP solution provider must ensure full privacy in all supporting activities.
- **Privacy of Executive Families.** Since most executives integrate their personal digital persona with that of their family through shared Wi-Fi, e-commerce accounts, streaming services, etc., it becomes important for DEP providers to recognize and protect the privacy of all involved. Family members often include minor children who require extra care when it comes to protecting their privacy.
- **Separation of Individual and Organization.** While executives recognize that protecting their personal information brings value to the organization, they may also be hesitant when it comes to exposing their private communications and accounts with the company. To that end, DEP providers must ensure there is a separation of attention between the executive and the company, much like the separation that exists with healthcare benefits.

In the next section, we introduce a new commercial solution that includes many aspects of required DEP functionality, while also paying attention to the basic privacy and separation considerations listed above. The offering from cybersecurity vendor BlackCloak combines technology, experts and resources in an arrangement that is well-suited to the needs of the modern executive.

OVERVIEW OF THE BLACKCLOAK PLATFORM

Founded in 2018 by Dr. Chris Pierson, BlackCloak provides concierge digital executive protection (DEP) services for executives, C-suite members, board directors, high-access employees and other prominent individuals. The objective of BlackCloak's DEP offering is to address the personal cybersecurity and privacy risks of these individuals, along with the additional goal of reducing transitive risks to their organizations.

The commercial BlackCloak Concierge Cybersecurity & Privacy Platform includes the following DEP capabilities for customers, families and their associated enterprise organizations:

- **Platform Features.** The BlackCloak platform offers a desktop and mobile experience for customers that addresses risks to endpoints, online accounts, personal networks and other relevant assets of interest to an executive and their inner circle. This platform also provides protection for their personal privacy by removing data-broker data and exposing any dark web risks.
- **Concierge Support.** BlackCloak experts are available on demand to provide real-time security recommendations for customers. Strategic actions are tailored to the executive's personal situation,



Figure 2. BlackCloak Desktop and Mobile Application

and a US-based security operation center (SOC) is available to offer guidance, support and full incident response to the executive, their family and the organization. This support covers all aspects of personal privacy and cybersecurity.

BlackCloak also includes an educational portal that helps customers make better decisions about their personal digital lives. The goal is to ensure that the executive is placed in a more secure personal ecosystem that combines technology platforms, expert support and guidance, and the ability to self-learn the most important basics of digital protection. Organizations obviously benefit when their executives enjoy this feature.



MAKING THE REGULATORY CASE FOR SOFTWARE BILL OF MATERIALS (SBOM) TO ENHANCE PRODUCT SECURITY

DR. EDWARD AMOROSO

This analyst report makes the regulatory case for using software bill of materials to enhance product security. We emphasize connected devices and embedded systems in the context of the software supply chain, and use the Finite State platform to demonstrate the existence of practical commercial support in this area.

INTRODUCTION

An enterprise's need to engage suitable cybersecurity solutions to enhance product security is generally recognized as having shifted from a discretionary decision to a requirement. This is especially true in industries such as automotive, medical and industrial control that rely on connected devices and embedded systems. Ultimately, the goal is to minimize the risk associated with commercial products to reduce the overall attack surface targeted by adversaries.

The good news is that many existing cybersecurity solutions translate well to this context. Strong authentication, identity and access controls, and log monitoring, for example, have been mainstays of modern enterprise protection for many years. Excellent commercial and open-source solutions exist that can be extended for use in product security. CISO-led teams often take advantage of these familiar approaches.

The unique risks, however, that are associated with connected device and embedded system security highlight the need for new types of protection. One major new area involves the use of software bill of materials (SBOM) to maximize visibility across the product supply chain. SBOMs offer transparency into the target device or system, usually through deep analysis of the product, all the way down to its firmware.

Since product security is a new discipline in most environments, establishing funding for this type of risk management solution often requires convincing finance teams and other approving authorities. This report offers some assistance in this regard by showing how the current regulatory direction is driving SBOMs and related visibility as requirements. Evidence of practical commercial solution availability is shown in the context of the [Finite State platform](#).

AUTOMATING PRODUCT SECURITY

Ultimately, the goal is to determine the composition of a target device or system to provide needed visibility for security. This requires establishing how binaries, libraries, embedded software, device drivers, and open-source or third-party components are organized into the product. As one might expect, users will typically demand this, and it will be offered through partnership and agreement between users and the device manufacturers.

As one would also expect, this type of device compositional insight can only be accomplished through automation to ingest product data and perform the analysis. The days of manual product reviews have long since passed, so the only practical approach is to use a platform to do the ingest, review, analysis, and reporting. [Emerging standards for SBOM, such as CycloneDX and SWID, presume the use of such automation](#).

The types of requirements that product security teams typically demand are driven by the desire for devices and systems to be secure by design. That is, rather than awkwardly retrofitting protections into products after they have been created, security teams prefer that security be engaged throughout the entire development lifecycle. SBOMs are particularly useful mechanisms to meet this goal with emphasis on the following areas:

- **Continuous Visibility**—The most basic and foundational objective for product security practitioners is to ensure high levels of visibility into the devices and systems being used in their environment. This includes functionality at all levels, including firmware images.
- **Supply Chain Risk**—Every security expert knows that supply chain risk has risen to a top concern for any environment, especially in critical infrastructure and industrial control systems. SBOMs are thus key controls to deal with this challenging objective.
- **Actionable Guidance**—Without the availability of actionable guidance on product vulnerabilities or other identified concerns, the SBOM process will not have meaningful impact on managing cyber risk. Such guidance is thus mandatory to minimize the attack surface.

These requirements should not come as a major surprise to any stakeholder or even observer of product security issues, but the reality is that too many environments have not reached the point of engaging such controls as a routine part of the product development, procurement and integration lifecycles. Such environments still view product security as discretionary and are hesitant to fully commit the time, effort and funding.

The next section provides an overview of how applicable regulations have begun to demand this type of protection for product security. As such, it is obvious to the analyst team at TAG Cyber that any product security team or executive funding authorities within an enterprise would be wise to act immediately. Organizations that ignore such obvious regulatory trends will find it more difficult and more expensive to make changes later, perhaps in response to more proactive competitors.

APPLICABLE REGULATIONS

Clear evidence exists that the regulatory environment for SBOMs and related product security visibility and action is becoming more intense. Product security teams must therefore pay close attention to such emerging regulations to ensure compliance and to optimize commercial success against competing products. Note that the applicable regulations examined here are mostly driven by US-based authorities, but product owners can easily extrapolate them to other countries.

The specific regulations are outlined below, with emphasis on sharing insights into their goals, objectives and direction. It is the view of the TAG Cyber analyst team that such regulations will continue to change frequently, so the specifics of requirements will continue to change frequently, so we outline here several applicable regulations as they exist now and offer references for product security teams to track progress as they continue to evolve.

The regulations selected are also just a sampling of applicable requirements for the same reason: new regulations are emerging all the time for product security owners. We, therefore, highlight three of the more prominent ones to illuminate what is being demanded and to provide a framework for product security teams to engage with funding sources to ensure that applicable solutions are put in place immediately.

NERC CIP Guidelines

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks, including for cybersecurity, to the **reliability and safety of the grid**. NERC's applicability covers many global regions including the United States, Canada and portions of Mexico. Product security teams recognize that customers demand compliance with NERC and it is thus mandatory to compete effectively.

The NERC Critical Infrastructure Protection (CIP) plan includes standards that regulate, enforce, guide and monitor the security of the electrical infrastructure (known as the bulk electric system) in the regions mentioned above. It includes requirements for critical infrastructure, asset classification, security policies, physical controls, security risk, incident response, system recovery, configuration management and many other areas.

The inclusion of SBOM is now well-established in NERC CIP. As part of its security guideline document for supply chain risk management in the electricity sector, NERC references SBOMs, and offers the following specific language:

One risk mitigation measure is to request that the vendor provide a software bill of materials (SBoM) for all components of their software and/or firmware that were developed by third parties – whether purchased or open source. An SBoM allows the entity to identify components known to present risks and hold the vendor accountable for providing patches for those components, when **available and applicable**.

Product security owners should view the inclusion of SBOM as key evidence that they must act immediately. The motivation is threefold: First, competition will demand SBOMs as users include this in their work proposals; second, costs will be high to integrate SBOMs later as they become even more complex and involved through practical application; and third, NERC CIP influences many other regulatory standards, so SBOMs will begin to appear more frequently across adjacent industries.

FDA Draft Guidelines for SBOM

The US Food and Drug Administration (FDA) recently released draft guidance called “[Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions](#).” This seemingly obscure document is in fact quite important to the industry, and it includes specific reference to the use of SBOMs to reduce cyber risk in products. The FDA recommends that device manufacturers use SBOMs to describe the software components they are using.

The guidance references off-the-shelf and any other software being used by the manufacturer as in-scope to the SBOM, and interestingly, the usage is described as applicable to both the product security teams as well as the FDA itself. This is a key reference that makes clear the obligation for manufacturers and users to pay full attention to this device design and quality system regulation—and this applies to both pre-market and post-market stages of the device lifecycle.

Biden Executive Order

The Biden Administration recently issued an [Executive Order on Cybersecurity](#) that includes best practices, encourages information sharing, and recommends many other security actions, primarily for the protection of .gov and other federal networks. Most industry observers agree that despite the government focus, the Executive Order is having much wider influence across commercial settings.

In addition to referencing foundational protection principles such as information sharing, the Executive Order includes innovative ideas such as the recommendation that agencies move toward a zero-trust model for their networks. The most innovative idea in the order, however, is certainly its reference to SBOMs, a construct that requires supply chain companies to list in a structured manner the components included in their product.

This is a major requirement for product security teams who expect their solutions to find their way into US government infrastructure. Without attention to SBOM in the pre-market and post-market stages of the product lifecycle, companies will struggle to successfully deploy connected devices and embedded systems to the government. As such, it becomes obvious that such regulatory pressure demands focus on this important new control.

COMMERCIALY AVAILABLE SOLUTION: FINITE STATE

The availability of practical commercial solutions for SBOM was originally a concept of device and system supply chain visibility. Luckily, the industry has responded with many excellent commercial options for product security teams to engage with an effective partner for implementing SBOMs. In this section, we offer a summary of the Finite State commercial solution.

The Finite State platform is a commercially available cybersecurity solution for connected devices. The platform is designed to improve the visibility of what specifically resides within a connected device or embedded system that is procured through a supply chain partner or even developed locally. Such enhanced visibility enables deeper analysis of cyber risk by exposing exploitable vulnerabilities that might be present.

The way the Finite State platform provides SBOM for a given connected device or embedded system helps illustrate how such a construct might be used in practice. Finite State analyzes the device and then offers a visual representation of problems that might stem from identified subcomponents. This is important because just reading a “parts listing” from an SBOM might not be useful to establish compliance with applicable regulations such as those described above.

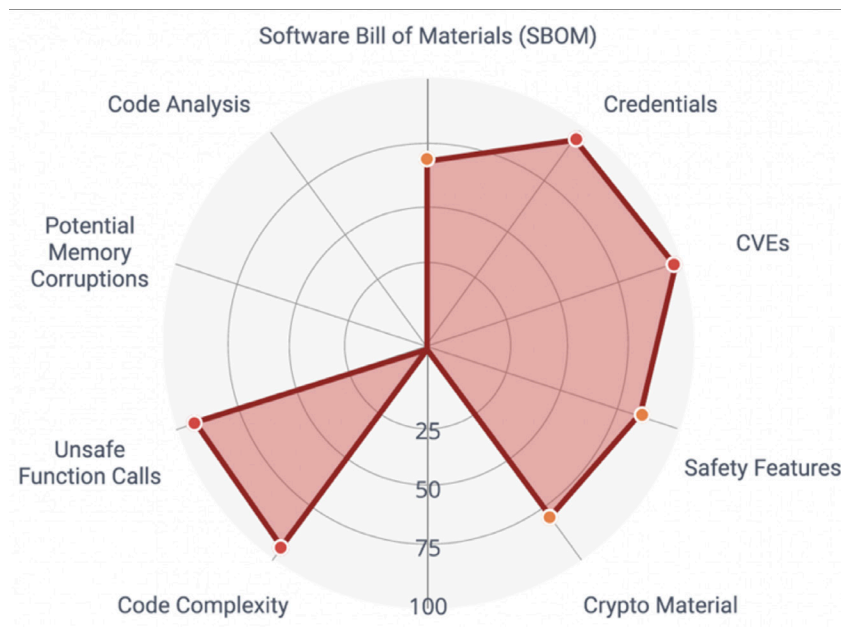


Figure 1. Example of How Finite State Visualizes SBOM-Derived Risks for a Device

To determine the effectiveness of a given platform in supporting a set of requirements, such as in the Executive Order, it is helpful to create a set of assertions that characterize the document. In essence, this replaces the unstructured document with a more structured set of statements that can support a mapping. The TAG Cyber team performed this task during a prior examination of the Finite State platform.

Specifically, assertions were culled directly from the Executive Order and used by TAG Cyber for investigative work. The team mapped these assertions against a similar set of assertions regarding the functionality included in the Finite State platform. This was done in conjunction with the Finite State team to ensure product completeness. The next step was to characterize each potential useful mapping into how the support method benefits the following characteristics:

- *Automated or Standard Method*: Determines the degree to which a function is supported by automation.
- *As Needed or Continuous Frequency*: Differentiates one-time support versus continuous coverage.
- *Technical or Administrative Type*: Shows the difference between a control based on technology versus an administrative process.
- *Detect or Identify NIST Focus*: Maps the function to the appropriate phase of the **NIST Cybersecurity Framework**.

The results of these determinations for the specific functions included in the Finite State platform showed a direct map to the Executive Order. This work can easily be extrapolated to other regulatory control requirements such as the ones referenced above. TAG Cyber analysts strongly recommend that product security teams thus act immediately to engage a commercial partner such as Finite State to begin a program of supply chain risk management commensurate with emerging regulations.

DISTINGUISHED VENDORS



DISTINGUISHED VENDORS

Q 1 2 0 2 3

Working with cybersecurity vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area—and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.



acsense is an easy-to-use IAM business continuity platform for Okta, allowing Okta customers to easily and quickly recover from cyberattacks in minutes and misconfigurations with a click of a button. With a complete set of enterprise features, acsense provides resilience and peace of mind so organizations know IAM systems are no longer a single point of failure.



Adaptive Shield is a leading SaaS Security Posture Management (SSPM) company, enabling security teams to maintain a secure SaaS app stack by continuously monitoring SaaS apps, users and their devices, while also identifying misconfigurations, assessing SaaS-to-SaaS risk and fixing any weakness. Adaptive Shield works with many Fortune 500 enterprises to help them secure their SaaS threat landscape.



Appdome is the one and only solution needed to protect, Certify Secure and monitor threats and attacks against Android & iOS mobile apps right inside the mobile DevOps CI/CD pipeline. Instantly defend mobile apps and customers from mobile app security breaches, mobile fraud, mobile malware, cheating and other attacks with ease.



Balbix enables businesses to reduce cyber risk by automating cybersecurity posture. Our SaaS platform ingests data from security and IT tools to create a unified view of cyber risk in dollars. With Balbix, you can automate asset inventory, vulnerability management and risk quantification, leading to lower cyber risk, improved team productivity and tool cost savings.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 3



concourse labs

Concourse Labs offers a cloud configuration management platform with centralized, automated, Security-as-Code enforcement of security controls and policy. They enable enterprises to deploy mission critical applications to cloud with security, resiliency and regulatory compliance. Clients move away from point-in-time security snapshots and human-dependent security checklists to persistently secure, auditable processes and environments.

CYBRARY

Cybrary is the industry-leading professional development platform designed to bridge the cybersecurity skills gap. With threat-informed training, advanced assessment capabilities, and certification preparation, Cybrary enables more than three million learners—from individuals, service providers and government agencies to Fortune 1000 organizations—to build the skills and knowledge needed to confidently mitigate the threats faced by their organization.



cyera

Cyera is reinventing data security. Companies choose Cyera to: improve their data security and cyber resilience; maintain privacy and regulatory compliance; and gain control over their most valuable asset—data. Cyera instantly provides companies with a holistic view of their sensitive data and security exposure, while delivering automated remediation to reduce the attack surface.



Elevate Security

Elevate Security provides an open and extensible insider risk management solution designed to identify a company's riskiest users and prevent incidents before they adversely impact business. Elevate Security's platform integrates with leading technology systems and products to predict user risk and stop incidents before they start.

FINITE STATE

Finite State helps product security teams and connected product end-user organizations (asset owners) leverage comprehensive, context-aware vulnerability intelligence to assess or generate SBOMs to ensure a continuous state of risk reduction and improved software transparency. Regardless of any given product's software, firmware or component composition, Finite State helps reduce third-party software supply chain risk.



Fletch delivers instant answers to the most pressing cyber risk questions. Their Trending Threats app is like having a whole threat intel team in your back pocket, while their People Risk app enables you to investigate anyone in seconds.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 3



HUMAN is a cybersecurity company that protects 450+ enterprises by disrupting bots, fraud and account abuse with modern defense. We verify the humanity of more than 20 trillion digital interactions per week, protecting against account takeover attacks, fake account creation, payment fraud, content manipulation, content scraping, PII harvesting and denial of inventory/stockout attacks.



Island is the browser designed for the enterprise that makes work fluid, yet fundamentally secure. With the core needs of the enterprise embedded in the browser itself, Island enables organizations to shape how anyone, anywhere works with their information, while delivering the Chromium-based browser experience users expect. Island, the Enterprise Browser.



OptimEyes.ai

OptimEyes offers a unique AI-powered, SaaS-based solutions platform with fully automated risk frameworks to assist organizations by creating a single source of truth to manage their cyber, data-privacy and compliance risk. Risk models are customizable and provide an enterprise-wide view with real-time decision-making.



Perimeter 81 is an enterprise-grade secure network platform that connects all users, in the office or remote, to all corporate resources: on premises, in public clouds, SaaS, or the open Internet. It is delivered as a cloud-native, simple-to-use service that is fully managed from a unified, single-pane-of-glass console.



RegScale frees organizations from manual, paper-based processes via its continuous compliance automation software. Our API-centric software integrates with security and compliance platforms to manage the security control state, shifting compliance left to deliver audit-ready documentation in the world's first real-time GRC platform. Heavily regulated organizations use RegScale to start and stay compliant.



Swimlane provides cloud-scale, low-code security automation for organizations of all industries and sizes. Our technology is rated as the #1 trusted low-code security automation platform. Our mission is to prevent breaches and enable continuous compliance via a low-code security automation platform that serves as the system of record for the entire security organization.

TAG CYBER DISTINGUISHED VENDORS

2 0 2 3



Sysdig is a software-as-a-service platform built on an open-source stack. Its Secure DevOps Platform provides security that lets clients confidently run containers, Kubernetes, and cloud services – allowing them to secure their build pipeline, detect and respond to runtime threats, continuously validate compliance, and monitor and troubleshoot cloud infrastructure and services.



VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control. As a trusted foundation to accelerate innovation, VMware software gives businesses the flexibility and choice they need to build the future.



Votiro Cloud helps companies apply Zero Trust Content Security through its API-First Content Disarm and Reconstruction SaaS. With Votiro Cloud, enterprises can remove malware and ransomware threats in incoming files and content without using detection. Completely scalable and open to existing apps, data and security platforms, Votiro maintains instant content flows with no interruptions to productivity.

