

Infosecurity[®] Magazine

Q1, 2023 / Volume 20 / Issue 1



The Rise of Wiper Malware

Understanding the explosion
of new disruptive attacks

**ISRAELI
STARTUPS**
Driving success

**ZERO
TRUST**
Biden's mandate

**EQUAL
OPPORTUNITIES**
Socio-economic diversity

There's one thing even
a billion-dollar company can't afford:

a security breach

**Safeguard your business
with ManageEngine.**



ManageEngine  **20**
YEARS

Our solutions

Identity and access management | Security information and event management
Endpoint security | Network security | Data security

www.manageengine.co.uk/cybersecurity

CONTENTS

COVER FEATURE

8 A New Tool in the Cyber-Criminal's Playbook

Wiper malware attacks spiked in 2022. Kevin Poireault investigates why this marks a shift in the cyber threat landscape.

NEWS FEATURES

12 MFA: The Next Frontline for Security Pros

MFA has long been recommended by governments and industry bodies, but cyber-criminals are searching for ways to turn this security strength into a weakness. James Coker investigates.

16 ChatGPT's Data Scraping Model Under Scrutiny

One use of ChatGPT, the superstar chatbot created by generative AI firm OpenAI, is drafting privacy notices. ChatGPT now finds itself under scrutiny from data protection experts. Kevin Poireault examines the issue.

FEATURES

20 The Story of Israel's Booming Cyber Startup Sector

Israel's cybersecurity industry has long punched above its weight, producing a world-leading sector relative to the nation's population. Gerrard Cowan explores the factors that are driving this and how the sector is adapting for future challenges.

26 How SSI Puts Identity Back in the Owners' Control

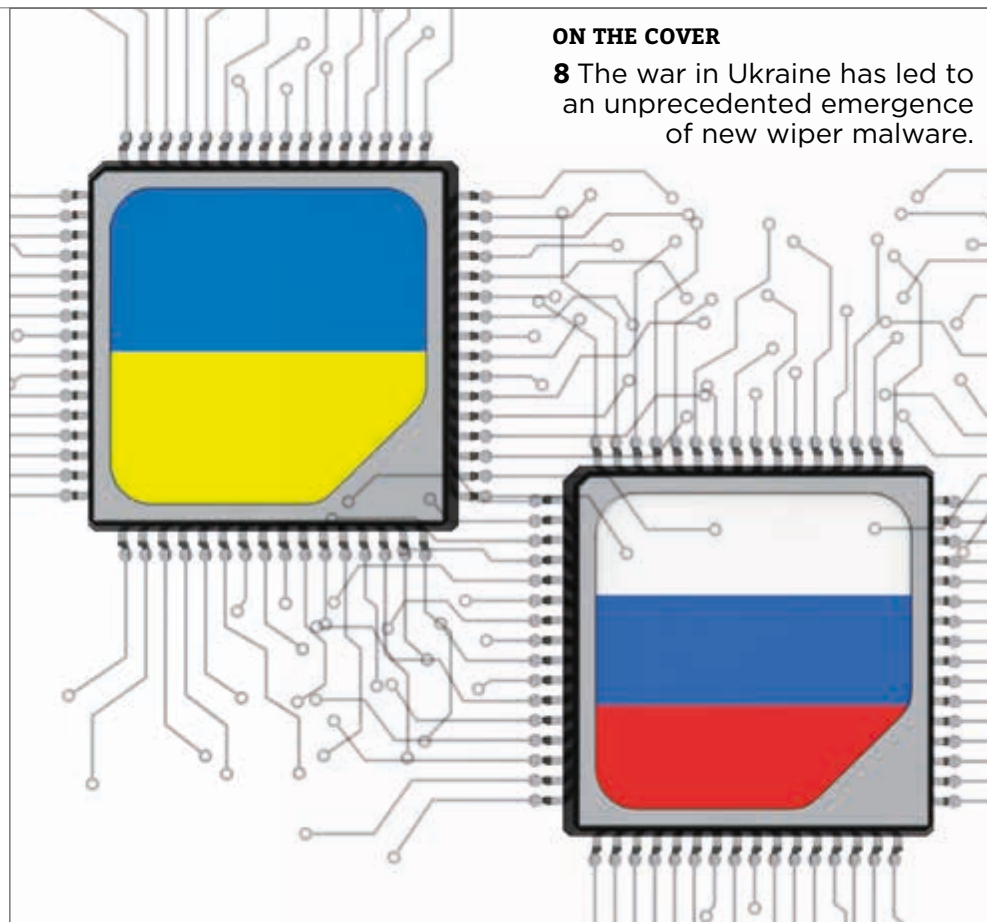
Danny Bradbury investigates whether SSI can solve a digital identity challenge that has perplexed tech and non-tech organizations alike for decades.

30 Biden's Zero Trust Mandate

Phil Muncaster examines the story of President Biden's Executive Order so far and the potential impact of zero trust on public and private sector security.

ON THE COVER

8 The war in Ukraine has led to an unprecedented emergence of new wiper malware.



38 Cyber Insurance: Understanding a Fast-Growing Market

Beth Maundrill speaks to experts to dispel some of the myths surrounding cybersecurity insurance and provide advice on how and why organizations should take out an insurance policy.

44 Lowering the Price of Admission: Making Cybersecurity an Equal Opportunities Industry

James Coker explores how socio-economic diversity can be of benefit to the industry and how the sector can open its doors to those with less economic means.

POINT-COUNTERPOINT

24 Is AI Essential to Cybersecurity?

Holly Grace Williams argues that there are cybersecurity problems AI is uniquely suited for, while Perry Carpenter believes humans remain more critical to security.

ONE TOPIC, THREE EXPERTS

42 How to Effectively Implement a Bug Bounty Program

Three experts advise on how to make bug bounty programs effective for your business.

INTERVIEW

34 Jerich Beason

James Coker meets Jerich to find out more about the values and experiences that underpin his career in cybersecurity.

REGULARS

7 Editor's Intro

48 Top Ten: Cyber-TV Shows

50 Slack Space

51 Parting Shots

The Contributors...



Beth Maundrill

Editor

Beth is the Editor at Infosecurity Magazine. She joined the team in August 2022 and has spent her career dedicated to business-to-business journalism and publishing.

@GunshipGirl



James Coker

Deputy Editor

With his MA in journalism, James has been with Infosecurity Magazine since 2020. He covers breaking news and the latest trends in information security, whilst also analyzing their potential long-term impact.

@ReporterCoker



Kevin Poireault

News Reporter

Kevin joined the team in August 2022 after several years covering cybersecurity and deep tech in France and the UK. He completed his master's degree in journalism from Sciences Po in Rennes.

@kpoireault



James Ingram

Digital Sales Manager

James helps clients achieve their goals by leveraging Infosecurity's marketing and advertising options. Outside of work James has a healthy passion for films, sport and cooking.

@infosecjames



Infosecurity Magazine



Infosecurity Magazine



@Infosecurity Mag

Infosecurity Magazine

Editor **Beth Maundrill**

Beth.Maundrill@rxglobal.com
+44 7436 050 850

Deputy editor **James Coker**

james.coker@rxglobal.com

News reporter **Kevin Poireault**

Kevin.Poireault@rxglobal.com

Online UK news editor **Phil Muncaster**

phil@pmmediauk.com

Online US news editor **Alessandro Mascellino**

alessandro.mascellino@protonmail.com

Print and online advertising

James Ingram

james.ingram@rxglobal.com
+44 (0)20 89107029

INFOSECURITY GROUP

Portfolio director **Saima Poorghobad**

saima.poorghobad@rxglobal.com

Event director **Nicole Mills**

nicole.mills@rxglobal.com

Sales manager **Abiola Agbalaya**

abiola.agbalaya@rxglobal.com
+44 (0)208 9107817

Group marketing manager **Julia Clarke**

julia.clarke@rxglobal.com

Production manager **Andy Milsom**

To amend or update your print subscription, please log in to your user account here:
<https://www.infosecurity-magazine.com/my-account/login/>

To cancel your subscription, simply return this magazine to sender to be removed from the mailing list or alternatively complete the short request form here:
<https://www.infosecurity-magazine.com/my-account/unsubscribe/>

For more information about how we process your data including your rights, please refer to our Privacy Policy:
[privacy.rxglobal.com](https://www.infosecurity-magazine.com/privacy.rxglobal.com)

ISSN 1754-4548

Copyright

Materials available in Reed Exhibitions Limited's Infosecurity magazine and websites are protected by copyright law. Copyright ©2023 Reed Exhibitions Limited. All rights reserved.

No part of the materials available in Reed Exhibitions Limited's Infosecurity magazine or websites may be copied, photocopied, reproduced, translated, reduced to any electronic medium or machine-readable form or stored in a retrieval system or transmitted in any form or by any means, in whole or in part, without the prior written consent of Reed Exhibitions Limited. Any reproduction in any form without the permission of Reed Exhibitions Limited

is prohibited. Distribution for commercial purposes is prohibited.

Written requests for reprint or other permission should be mailed or faxed to:
Permissions Coordinator
Legal Administration
Reed Exhibitions Limited
Gateway House
28 The Quadrant
Richmond
TW9 1DN
Fax: +44 (0)20 8334 0548
Phone: +44 (0)20 8910 7972

Please do not phone or fax the above numbers with any queries other than those relating to copyright. If you have any questions not relating to copyright please telephone: +44 (0)20 8271 2130.

Disclaimer of warranties and limitation of liability

Reed Exhibitions Limited uses reasonable care in publishing materials available in Reed Exhibitions Limited's Infosecurity magazine and websites. However, Reed Exhibitions Limited does not guarantee their accuracy or completeness. Materials available in Reed Exhibitions Limited's Infosecurity magazine and websites are provided "as is" with no warranty, express or implied, and all such warranties are hereby disclaimed. The opinions expressed by authors in Reed Exhibitions Limited's Infosecurity magazine and websites do not necessarily reflect those of the Editor, the Editorial Board or the Publisher. Reed Exhibitions Limited's Infosecurity magazine websites may contain links to other external

sites. Reed Exhibitions Limited is not responsible for and has no control over the content of such sites. Reed Exhibitions Limited assumes no liability for any loss, damage or expense from errors or omissions in the materials or from any use or operation of any materials, products, instructions or ideas contained in the materials available in Reed Exhibitions Limited's Infosecurity magazine and websites, whether arising in contract, tort or otherwise. Inclusion in Reed Exhibitions Limited's Infosecurity magazine and websites of advertising materials does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

Copyright ©2022 Reed Exhibitions Limited. All rights reserved

Infosecurity Europe

20 - 22 June 2023, ExCeL London

Join us

as we rethink
the power of
infosecurity

Keep up to date on the latest advances and innovations

Connect with the brightest minds

Get **hands-on** with the technology

Benchmark your **solutions** and strategies

Register at www.infosecurityeurope.com





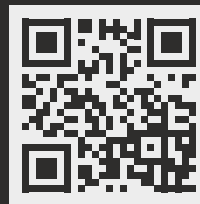
Ironclad security for all your devices.

Give your organisation the best defence against cyber criminals with Managed Endpoint Detection & Response (M-EDR) from Annodata.

We'll secure your organisation's devices with cutting-edge EDR software, reinforced by the oversight and expertise of our team of cybersecurity professionals. With 5 Managed EDR service packages to choose from, we can provide the right level of protection for your organisation's size and threat environment.

To find out more and register for a free 14 day trial of M-EDR*, visit our website today: www.kyocera-annodata.co.uk/m-edr

Discover more:



[annodata-ltd](#)



[@AnnodataLtd](#)



sales@duk.kyocera.com



+44 (0)333 151 856

annodata

A KYOCERA GROUP COMPANY

kyocera-annodata.co.uk

*Terms & conditions apply

From the Editor...



Welcome to the first edition of *Infosecurity Magazine* for 2023, we're delighted to bring you another information-packed issue to kick off the year.

As the team will be heading to the RSA Conference, San Francisco, in April, there is a US flavor to our content as we reflect on President Joe Biden's zero trust executive order 12 months on and consider how digital identity challenges can be solved by secure and sovereign identity (SSI) as an element of Web 3.0.

For myself, this will be my first time back in the US since 2019 and I am looking forward to connecting with new faces, colleagues and cybersecurity pros during the trip.

Password Problems

As mentioned, this is the first edition of 2023 and the year got off to quite the start. Think back 12 months and Log4j was the biggest talking point of the winter holiday period; fast forward to 2023 and the cybersecurity world was rocked by another LastPass data breach, putting the password manager firm under scrutiny.

The company suffered two major breaches in 2022, one in August and another in late December. The latter breach was the result of source code and technical information taken in August used to target another employee.

The whole episode put password managers at large in the spotlight, with many questioning how useful they are as a security tool given the vulnerabilities highlighted in the LastPass saga.

The consensus among security professionals is that you should continue to use a password manager, whether it be LastPass or another provider like Bitwarden, KeePass, Zoho Vault or 1Password.

Those I spoke with said that you should, however, do more due diligence than simply trusting a platform on face value, with one commenting that's what happened with LastPass, and it has gone "horribly wrong." Things to consider when selecting your password manager include ease of use, an understanding of where data is stored, cross-platform integration, shared vaults with admin controls, customizability, extra features and cost.

With everyone having multiple online accounts, which all require unique and complex passwords, there is still an important role for password managers to play. The LastPass scenario has highlighted how there must be a certain level of scrutiny when selecting the tools needed to secure your online presence.

MFA

Another security essential under scrutiny is multi-factor authentication (MFA). Widely accepted as a security necessity and now a feature for logins to most online banking and social media accounts, it is clear that cyber-criminals are now exploring ways to bypass this layer of security.

In this edition of the magazine, James Coker explores MFA bypass and how attackers are adapting to overcome this layer of security. He highlights a recent case study where a user alerted an organization to its own weaknesses in its MFA tool.

Coker also explores the growth in SIM swapping attacks and man-in-the-middle attacks, which are all evolving to exploit MFA and allow threat actors access to accounts and credentials.

Stay Informed

Other features in this edition of the magazine include a debate between two

experts on the value artificial intelligence (AI) in cybersecurity. Holly Grace Williams, managing director at Akimbo Core argues that AI techniques can be utilized to protect your systems and is uniquely placed to overcome certain problems in cybersecurity.

Meanwhile, Perry Carpenter, chief evangelist and security officer at KnowBe4 argues that there are limits to the role AI can play as long as humans remain the primary end user.

Other cybersecurity experts contribute to our "ask the experts" section, which in this edition explores the use of bug bounty programs as a tool to uncover vulnerabilities in your organization's security posture. Our experts explain how to get started, why they have implemented bug bounty programs and what to consider along the journey.

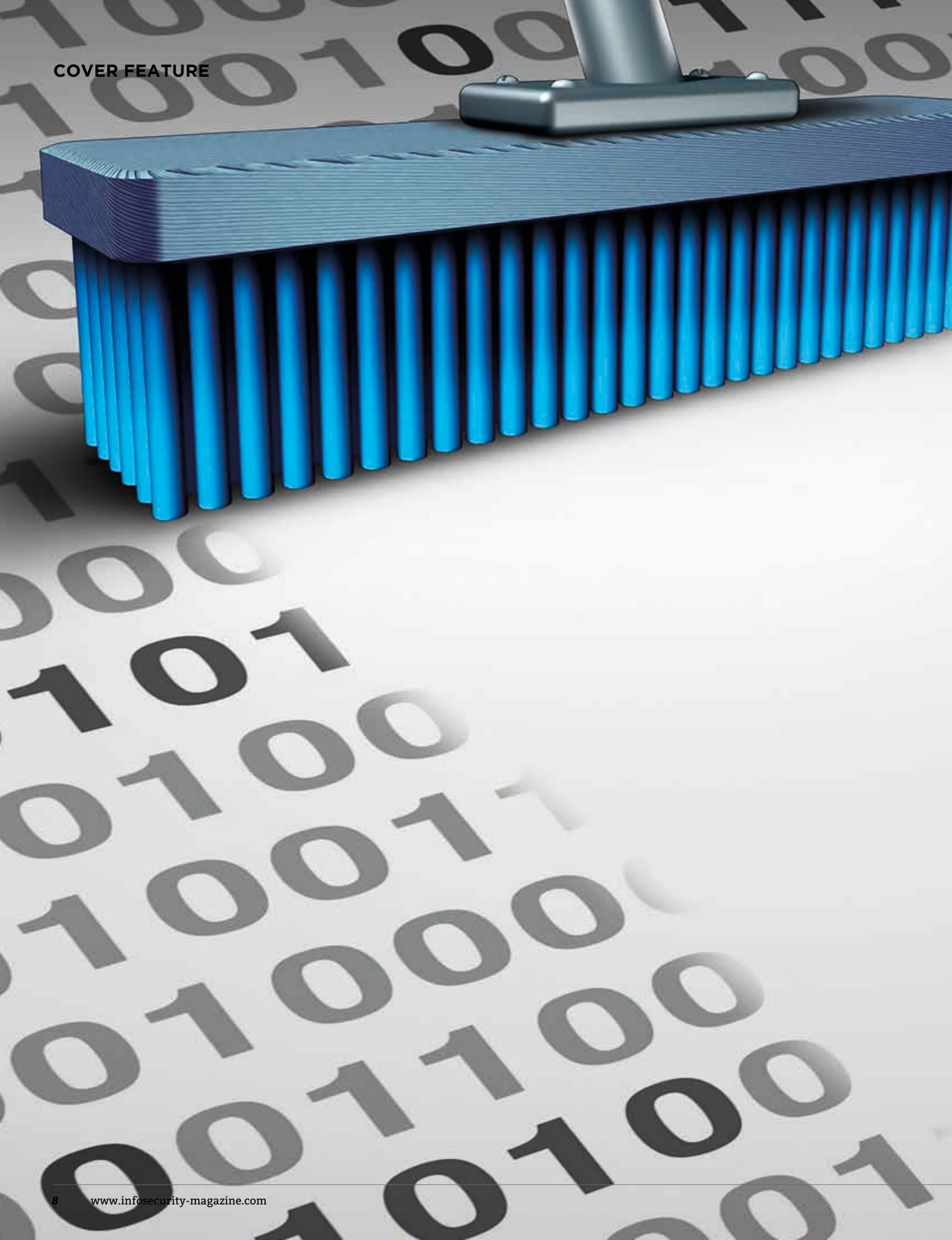
This edition of the magazine also includes an exploration of the boom in cybersecurity startups in Israel and what can be learned from their experience in investing in the sector; the state of the cybersecurity insurance market today; and how wiper attacks have emerged as an effective threat vector during the Ukraine-Russia conflict.

Finally, once you're done reading this edition of the magazine, do head to the *Infosecurity Magazine* website to sign up for our industry-leading Online Summit taking place on 21-22 March 2023. At this event, you can hear from the industry's biggest names about the most important issues to cybersecurity professionals today, earning CPE credits with every session you join.

We hope you enjoy reading and learning.

Beth Maundrill
Editor

COVER FEATURE





A NEW TOOL IN THE CYBER-CRIMINALS' PLAYBOOK

Against a backdrop of war in Ukraine, 2022 saw an unprecedented rise in wiper attacks. **Kevin Poireault** investigates why this marks a shift in the cyber threat landscape

The year 2022 saw an unprecedented emergence of new wiper malware. The first, WhisperGate, appeared in mid-January and targeted multiple organizations in Ukraine. From there, the kinetic invasion of the country by Russian troops on February 24 was accompanied in cyberspace by a significant wave of cyber-attacks, including HermeticWiper, which had begun infecting the Ukrainian government on February 23, and AcidRain, which shut down thousands of KA-SAT modems from satellite communications provider Viasat in Ukraine.

"The explosion in wiper activity continued throughout the whole first half of 2022, with the likes of Ukraine-focused CaddyWiper, IsaacWiper and DoubleZero, among others. During the second half, we saw these existing wipers being deployed in a number of attacks," Derek Manky, vice president of global threat intelligence at Fortinet, tells *Infosecurity*.

Jiri Vinopal, a threat researcher at CheckPoint, adds, "It shows that, at the beginning of the war, Russia-backed groups really wanted to make an impact."

From March onwards, however, Ukraine ceased to be the sole victim of wiper activity: Russia was the primary target of new wipers such as CryWiper and RURansom, and other wipers were active in the Middle East, such as Apostle and Fantasy, linked to the allegedly Iranian Agrius group.

Record Number of New Wiper Families in 2022

According to Fortinet's FortiGuard Labs, at least 16 new wiper families were

discovered throughout 2022. This is significantly more than ever before, with only a handful of wipers appearing in any of the previous years since 2012, when the first large-scale wiper, Shamoon, was developed.

Fernando Martinez, a security researcher at AT&T's Alien Labs, confirms there was a significant surge in wiper activity in 2022, even though he admits that "it is very hard to gather enough telemetry to substantiate it with any type of statistics because most wipers are deployed in very targeted, single campaigns."

Tom Hegel, a senior threat researcher at SentinelOne's SentinelLabs argues: "We're far from seeing the full picture. Wiping is quite a simple process, and there most likely are many more wipers we don't hear about."

Martinez agrees: "It doesn't require you to be particularly skilled to build a basic wiper."

While attackers can develop various techniques to deploy a wiper attack, these generally fall into two main categories:

- Wiping the files themselves by either deleting or overwriting them;
- Disabling, or even destroying, critical components of the operating system such as Windows' Master Boot Record (MBR) and Master File Table (MFT).

Since there are workarounds to each of these techniques, a more advanced threat actor would usually combine them or even use legitimate third-party drivers to bypass security controls' visibility and detection capabilities.

"The real sophistication, however, comes from what is developed around the wiper, like the initial access tooling or the privilege escalation process. For example, in 2022, we saw wipers using legitimate stolen digital certificates, such as those from a company called Hermetica Digital Ltd for the HermeticWiper, to delay detection. Later that year, we also saw wipers disguised as ransomware, like Azov and RURansom. But we haven't seen anything technically sophisticated," Martinez explains. ➔

Indeed, Hegel notes that many wipers that emerged in 2022 were “poorly developed and maintained.”

Overall, both Martinez and Hegel agree that nothing sticks out as unique, unlike what happened with NotPetya.

Lessons Learned From NotPetya

The NotPetya wiper first appeared in June 2017, just one month after the WannaCry ransomware started infecting thousands of computers worldwide. While it showed similarities with the Petya ransomware that targeted Ukrainian organizations in a series of attacks in 2017, security researchers quickly realized NotPetya was not only encrypting data but also wiping the master boot record (MBR), overwriting the Windows bootloader and triggering a restart – in effect, wiping data.

“The war in Ukraine has accelerated the rise of the advanced persistent cybercrime groups”

Like WannaCry, NotPetya used EternalBlue, an exploit developed in secret by the US National Security Agency (NSA) and leaked by the Shadow Brokers hacker group in April 2017. The exploit leveraged an unknown vulnerability in Microsoft’s implementation of the Server Message Block (SMB) protocol.

Additionally, NotPetya also had the capacity to self-propagate, “which means that we still see some NotPetya activity to this day,” claims Hegel.

“The wipers we saw in 2022 were very malware focused, did not exploit zero-day vulnerabilities nor have the ability to self-propagate,” notes Manky, who is also chief security strategist at Fortinet’s FortiGuard Labs.

According to Hegel, this comes as no surprise, as NotPetya’s global and long-lasting impact was probably

unsolicited by its perpetrators, whom several Western countries, including the UK and the US, have attributed to the Russian military.

“By exploiting a zero-day vulnerability, NotPetya and the WannaCry ransomware gained a lot of unwanted attention. Many groups with the same capabilities are not ready to take that step unless things take drastic turns – but, also, many of them simply don’t have the capabilities,” Manky argues.

Adam Meyers, CrowdStrike’s senior vice president of intelligence, agrees: “Immediately after NotPetya hit organizations in various countries across the world, there were discussions on whether the attack was triggering NATO’s Article 5.”

Article 5 of the NATO Treaty introduces the principle of collective defense, which states that each member state will consider an armed attack

against one member state to be an attack against them all.

Symbolic Impact Rather Than Destructive

Hegel, Manky and Meyers claim that all elements from their forensics work converged to conclude that the threat actors behind the 2022 wiper attacks targeting Ukraine most likely tried to avoid the same mistakes.

CheckPoint’s Vinopal notes: “The impact Russia-backed groups were aiming for was symbolic rather than destructive.”

Therefore, since the beginning of the war, a lot of the cyber efforts against Ukraine have been on access to information, an area where Russia-linked threat actors have a long-standing reputation.

The most notable examples were the repeated attacks against Ukrinform, the

country’s national news agency. “Russia has been trying to cut off Ukrainians from the information on the current situation and the course of the war since the early days of the full-scale invasion. They have shut off Ukrainian TV, the internet and mobile communications and have waged cyber-attacks against Ukrainian media,” Yuriy Shchychol, head of the State Special Communications Service of Ukraine (SSSCIP), said in a statement on January 18, 2023, after a failed attack on Ukrinform was discovered.

According to Gergely Révay, a security researcher at Fortinet, the apparent favored use of wipers to send a message rather than to destroy is common in times of kinetic war. “When you can bomb something, it’s probably easier to do so rather than spend months and resources in a destructive cyber-attack,” he argues.

However, the AcidRain attack on February 24 nearly escalated the conflict. While the attack was allegedly intended to disrupt Ukraine’s military means of communications, it spilled over, shutting down French satellite internet customers and German windmills’ communication systems, among other victims.

Talks of retaliation were triggered and such an attack has not been attempted again to this day.

It was not surprising, then, to hear the former head of France’s national cybersecurity agency (ANSSI), Guillaume Poupard, claim in June 2022 at the Forum international de la cybersécurité (FIC) in Lille that the war in Ukraine had not had any significant cyber-related impact in France, yet.

Hybrid Cyber Warfare

SentinelOne’s Hegel, however, argues that the rise of wiper attacks since the war in Ukraine started represents “a shift in cyber activity” towards what some call ‘hybrid cyber warfare.’

“We’ve seen such an interesting level of success from various actors in 2022, including hacktivists and cyber-criminal groups. The reuse of wipers like CaddyWiper, or even MeteorExpress in the Middle East, for example, is unprecedented in cyber history,” he adds.

An Unprecedented Surge

Emergence of major wiper families since 2010

2010
Stuxnet*

2012
SkyWiper/Flame/
Flamer; Shamoon

2013
DarkSeoul

2016
KillDisk;
Industroyer*

2017
StoneDrill;
NotPetya;
IsraBye; Odinypt/
German Wiper;
Triton/Trisis*

2018
Olympic Destroyer

2019
Dustman;
ZeroCleare

Russia has used cyber-criminals and hacktivists prior to 2022. Indeed, threat intelligence firm Recorded Future wrote in a 2021 report that “Russian intelligence agencies have used criminal commodity malware to obfuscate their activities and make attribution more difficult.”

What is new is the incorporation of wipers into this model. As a result, while some of the 2022 wiper attacks have been attributed to well-known advanced persistent threat (APT) groups linked to Russian military and intelligence agencies, like APT28 (aka Fancy Bear), APT29 (aka Cozy Bear), Sandworm (aka Voodoo Bear) and Ember Bear, the pro-Russia threat landscape has become so blurry that most threat analysts told *Infosecurity* they now refrain from attributing wiper attacks altogether.

This was also shown by a Mandiant case study published in September 2022, where the Google-owned cybersecurity firm highlighted close links between APT28 and the people behind the pseudo-hacktivist Telegram channels ‘XakNet Team,’ ‘Infocentr’ and ‘CyberArmyofRussia_Reborn,’

who claimed responsibility for various wiper attacks.

“While APTs, which are siloed groups with custom tooling, high skills and specific targets, are still operating, the war in Ukraine has accelerated the rise of the advanced persistent cybercrime (APC) groups, a new concept to name those cyber-criminals and pseudo-hacktivists working covertly for the interest of a nation-state and going for critical infrastructure, but also using their attacks for their own interests, which creates a spillover effect,” Fortinet’s Manky says.

“Through these groups, nation-states can enter the cybercrime-as-a-service (CaaS) market by purchasing ready-made tooling. And in 2022, those APC groups started adding wipers to their playbook, along with ransomware, distributed denial of service (DDoS) attacks and hack & leak attacks,” he adds.

Wipers-as-a-Service


On the other side, Ukraine also embraced a cyber approach with its ‘IT Army,’ where thousands of Ukrainian

citizens from Ukraine and abroad joined forces to defend the country’s digital infrastructure.

The next step, Manky says, could be the emergence of open-source wipers such as Endurance, a small wiper malware programmed in C# to which an attack against US federal government agencies in November 2022 is attributed.

“Now that APC groups are deploying wipers for cyber warfare purposes, they could also use them for financial gain by threatening to wipe a system one part at a time in exchange for a ransom,” he adds.

Hegel projects “more sophisticated, zero-day wipers and maybe the appearance of logic bombs, a piece of malware with a payload that is programmed to activate at a specific time.”

With the successive attacks of Sandworm-made SwiftSlicer, a wiper targeting Ukrainian organizations and NikoWiper, which was aimed at the Ukrainian energy sector, in January 2023, it seems likely that pro-Russian groups will be keeping up with their 2022 activities 

Industroyer2 Revived the ICS Threat

The year 2022 also saw the revival of Industroyer, a malware framework programmed to attack industrial infrastructure and considered to have been used in the cyber-attack led by the Sandworm APT group on Ukraine’s power grid in December 2016. In March 2022, a new version of Industroyer, named Industroyer2, attempted to infect Ukrainian energy providers again. Although the attack reportedly failed, it was an interesting case for threat intelligence analysts.

“For many of us, Industroyer2 was a mystery that popped up all of a sudden, but then we noticed that CaddyWiper was used as the initial access tool to determine how to deploy Industroyer2. It was fascinating to see that two different APT groups, Sandworm and APT28, could be supporting each other,” Tom Hegel, a senior threat researcher at SentinelOne’s Sentinel Labs, says.

What’s more, Industroyer2 was not only

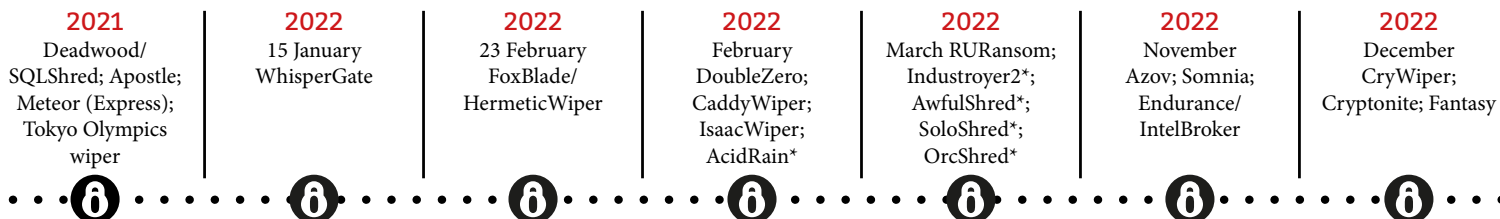
deployed with CaddyWiper to infect Windows-based machines but also with AwfulShred, SoloShred and OrcShred to attack Linux and Solaris systems, widely used in industrial networks.

“Industroyer2 may have failed, but there is a lot of mystery behind that attack. Was it successfully deployed but caught before it was used? We still don’t know. What’s sure is that, while I don’t think industrial control systems (ICS) attacks are the top priority from attackers, we

could see more of them in the future,” Hegel adds.

In April 2022, another toolkit for ICS attacks, very similar to the Industroyer one, was found by the US Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA) and FBI. Named ‘Pipedream’ by the industrial security firm Dragos and ‘Incontroller’ by Mandiant, it has been called the “Swiss Army knife for hacking industrial systems” by *Wired* journalist Andy Greenberg.

**Industrial control systems (ICS) malware targeting operational systems*





MFA BY

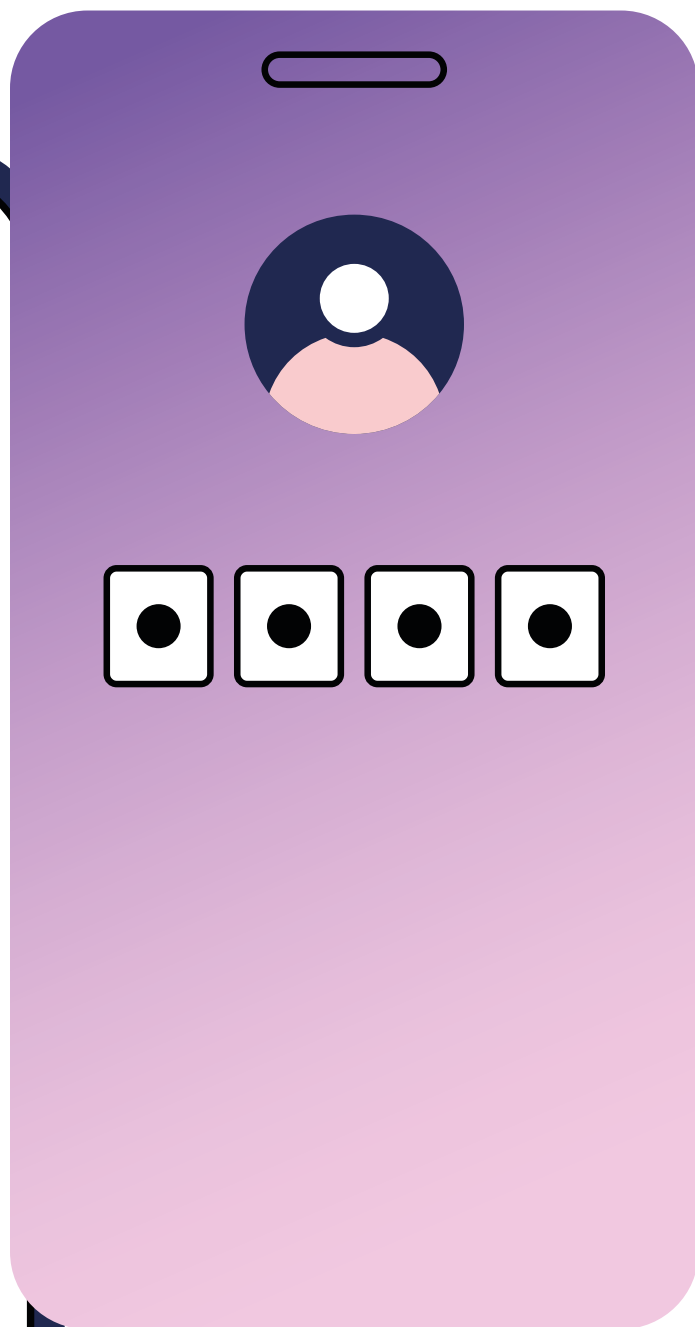
The Next Frontline f



PASS

or Security Pros

MFA has long been recommended by governments and industry bodies, but cyber-criminals are searching for ways to turn this security strength into a weakness. *James Coker* investigates



Multi-factor authentication (MFA) is becoming a crucial component of cybersecurity for organizations and individual users. The weaknesses of password-only authentication methods are increasingly recognized, with compromised login credentials the most common method used by cyber-criminals to breach organizations.

Verizon's 2022 *Data Breach Investigations Report* found that over half of cyber-attacks in 2021 resulted from stolen credentials.

MFA methods, ranging from codes delivered by SMS message to

passwords. They are often installed on a dedicated server owned by the threat actor or covertly installed on a compromised server owned by an unlucky individual.

These kits typically target human weaknesses to steal tokens. "Attackers often rely on notification fatigue, bombarding an employee with approval requests until they finally relent," says Cooke.

The use of social engineering tactics to steal MFA codes are also commonly observed by Dunn. This includes push notification attacks, whereby an attacker attempts to convince a user to hit 'yes'

the file allows the new 'owner' to log into Slack, Teams and other business critical systems without any additional authentication requirement," he explains.

A less common and particularly sophisticated technique sometimes used is the targeting of the cryptographic components behind the MFA process itself, allowing attackers to create a backdoor or mint their own authentication tokens.

"This is a rather sophisticated attack and requires a previous method of compromise, but it did rear its head during the SolarWinds incident," comments Dunn.

"Attackers often rely on notification fatigue, bombarding an employee with approval requests"

fingerprint scans, offer an invaluable layer of security in the event a user's credentials are compromised. Experts believe that widespread use of MFA will prevent a significant proportion of cyber-attacks from occurring.

However, in light of the growing use of MFA, cyber-criminals are finding new and innovative ways of bypassing these methods, aiming to turn this security strength into a weakness. In one example, in July 2022, Microsoft detailed a large scale phishing campaign that was able to bypass MFA.

Kevin Dunn, senior vice president, head of professional services at NCC Group, tells *Infosecurity*: "As with many things, as defenses increase, attackers adapt to overcome them. MFA bypass is becoming a common theme in attack chains to overcome initial authentication barriers and compromise a system or identity perimeter."

Common MFA Bypass Techniques

It is clear that threat actors have developed multiple techniques for bypassing MFA systems. Matt Cooke, director, cybersecurity strategy, EMEA at Proofpoint, notes that MFA phishing kits are being observed for sale on cybercrime websites, with many of these able to be purchased "for less than a cup of coffee."

These tools are often adapting similar approaches found in "traditional kits" that steal only usernames and

to a push notification access request through social engineering, or what he terms 'push notification fatigue.'

"This is where a user is so overwhelmed by either the frequency of requests or the hectic nature of their day-to-day lives that they simply hit yes without thinking. While this might seem unlikely, it happens a lot," he explains.

In addition, Cooke says he has observed an increase tools that use a transparent reverse proxy to present the actual website to the victim. This enables so-called man-in-the-middle (MitM) attacks – essentially the deployment of a proxy server between a target user and an impersonated website, allowing threat actors to capture the usernames, passwords and session cookie in real time.

The growth of SIM swapping attacks is another technique observed in this space, which specifically compromises MFA codes sent via SMS. This normally involves a fraudster socially engineering a mobile carrier operative to switch the victim's mobile number to a SIM card in their possession, leading to the victim's calls, texts and other data being diverted to the criminal's device.

Jason Steer, CISO at Recorded Future, also highlights the growing prevalence of infostealer malware to bypass MFA.

"These malware families, once installed on a victim's computer, look for credentials in browsers and for hard coded authentication tokens that store the zero trust information inside a file. Essentially the ownership of

Case Study: Discovering MFA Vulnerabilities

Sometimes, cyber-criminals find MFA bypass opportunities presented to them, by exploiting flaws and mistakes within organizations' systems. Therefore, it is increasingly important that security teams are consistently checking for vulnerabilities in their MFA systems that can potentially lead to a bypass.

In a recent example, a vulnerability was discovered on the member login portal of the website of cybersecurity certification body (ISC)² by security researcher Jacob Hill, CEO at GRC Academy. The vulnerability was found by accident when he tried logging into his member account.

After entering his username and password, Hill was prompted to select an MFA method, of which (ISC)² offers several options. As he wasn't able to access his choice of Google authenticator code, he clicked the option to 'try another method.'

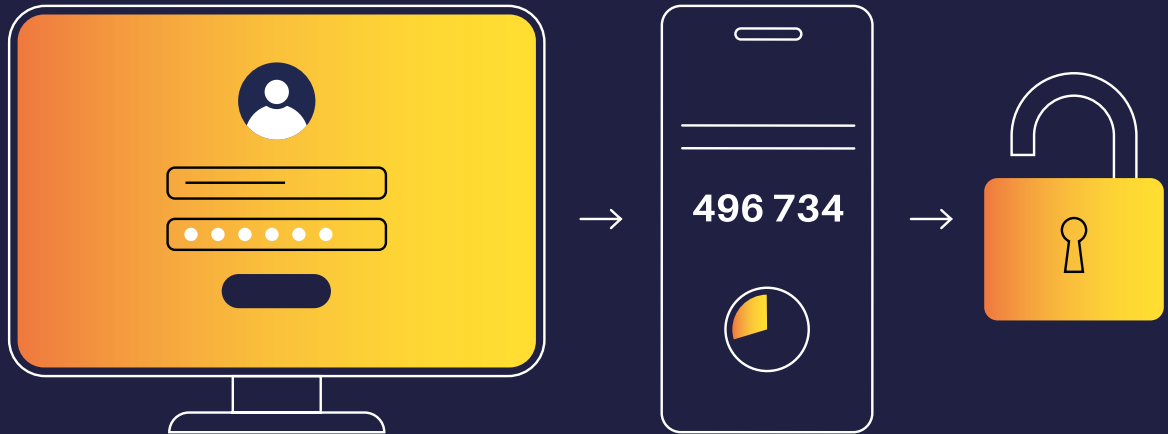
One of these methods was an SMS code, and this allowed Hill to register any phone number to enable the authentication method during the login flow. This code was sent to his phone and allowed him to access his account.

Therefore, he essentially bypassed his own MFA – although this can only occur if the users' password and username were already compromised and SMS wasn't already set up as their MFA method. Hill revealed that he reported the issue to (ISC)² on October 25, 2022, and three days later the certification body confirmed it had understood the report.

On December 13, 2022, (ISC)² informed Hill that the problem had been resolved, but the exact date of the fix has not been confirmed.

Speaking to *Infosecurity*, (ISC)²'s CEO Clar Rosso, says that the organization's security team shut the issue down by the end of October. Thankfully, "in the work we've done

One type of 2FA involves a code being sent via SMS to the user's mobile phone in order to complete authentication.



since there's no evidence of any kind of compromise that happened as a result."

In his blog detailing his findings, Hill suggested the flaw may have been caused by an SSO upgrade that (ISC)² made on its website on July 27, 2022. Rosso confirms to *Infosecurity* that the issue arose from a human implementation error, which provided learning opportunities for the body. "That allowed us to look at our security processes to see how we can avoid these kinds of problems on the front end in the first place," she says.

Rosso adds that this analysis needs to continue on an ongoing basis and that (ISC)² welcomes input from external security researchers.

In terms of advice for other organizations based on this recent experience, Rosso says security teams should always be aware of the wider impact and collateral damage a mistake can have on their IT system. "You need to test and retest your business processes to ensure they're working in the way they're supposed to," she notes.

Securing MFA

There are a number of steps that organizations should be taking to reduce the risk of MFA bypass. One of which is constantly testing their systems, as mentioned by Rosso.

NCC Group's Dunn also emphasizes that some forms of MFA are more secure than others. He argues that SMS, email, push notifications and even one-time codes are particularly susceptible to compromise and should

not be used by employees with high levels of privilege and access. Instead, for these staff, he urges the use of FIDO-compliant MFA methods, which are far harder to compromise. For example, FIDO USF security

activities before they become problems," says Dunn.

Continued Use of MFA

The experts *Infosecurity* spoke to all emphasize that MFA remains vital in

"If MFA is available to you, you should employ it"

keys ensure the user login is bound to the origin, meaning only a real site can authenticate with the key.

Dunn advises: "For the riskiest users (but ideally for everyone), FIDO U2F is the gold standard. Several sites and applications now support it, such as Okta, Duo, Google Workspace, AWS and Microsoft 365. Despite this, I see very few companies making the switch."

Recorded Future's Steer concurs, stating: "Look for alternate stronger MFA options such as Yubikey and other FIDO compliant tools to strengthen secondary MFA channels."

Finally, close monitoring and auditing of authentication events remain crucial to enable a rapid response when malicious actors have compromised a user's password and MFA, which can never be completely infallible.

"By understanding how the attacks work and how they manifest in terms of indicators of activity or indicators of compromise, an organization can set up a monitoring strategy that has a good chance of spotting suspicious

spite of the growing risk and should be employed in every possible circumstance.

"We as an organization take the posture that MFA is good practice – the same as government agencies across the world. If MFA is available to you, you should employ it," comments Rosso.

However, it is not infallible, and should be considered one aspect of a more rounded security strategy.

Proofpoint's Cooke says: "The days of the MFA 'silver bullet' for credential phishing are gone. A majority of leading organizations implemented MFA and have largely been able to discount credential phishing for several years. Those organizations need to now assess their ability to detect account compromise, not just prevent it."

Strong MFA should therefore be developed in conjunction with effective detection technologies and processes.

It may not be the golden bullet, but continues to be a crucial component of an organization's wider approach to authentication and protecting employees' accounts ●●●END

ChatGPT's



DATA-SCRAPING MODEL UNDER SCRUTINY FROM PRIVACY EXPERTS

One use of ChatGPT, the superstar chatbot created by generative AI firm OpenAI, is drafting privacy notices. ChatGPT now finds itself under scrutiny from data protection experts. *Kevin Poireault* examines the issue

While the various uses of ChatGPT – and other generative AI – can raise ethical and legal concerns regarding the violation of data privacy, some experts are questioning the very existence of OpenAI's chatbot for privacy reasons.

Addressing the Data-Scraping Method

First, the method used by OpenAI to collect the data ChatGPT is based on needs to be fully disclosed by the generative AI firm, claims Alexander Hanff, member of the European Data Protection Board's (EDPB) support pool of experts.

"If OpenAI obtained its training data through trawling the internet, it's unlawful," Hanff, host of That Privacy

from a legal point of view, there are many tensions between GDPR and foundational models; the large artificial intelligence models trained using self-supervised learning, such as ChatGPT.

"The way they work, by throwing a lot of unlabeled data and then defining the use cases, contradicts the EU GDPR's principle of data minimization, which says that an organization should use a minimal amount of information useful for a predefined purpose," Hillemann says.

Fair Use Not Likely Applicable

In many jurisdictions, using information without the owner's consent or copyright

considered fair. Satire wouldn't be valid either: although you can use ChatGPT for parody and satire, OpenAI has not created the model for these specific purposes," he says.

Also, although OpenAI states on its privacy policy page that it "[does] not and will not sell your Personal Information," Hanff considers ChatGPT a commercial product.

"There is a big debate on the definition of 'selling,' but ChatGPT is a commercial activity without a doubt – the company could be valued at \$29bn – so they can't get away with fair use. This AI model will create tremendous revenue and wealth for a small number of individuals off the back of everybody else's content and work," he says.

Hillemann is more nuanced: "I think, at this point, it's very hard to define whether ChatGPT is considered a commercial use of data. On the one hand, a lot of people are using it for free; on the other, the company is involved in a commercial business model."

However, the announcement of ChatGPT Plus a premium version of the chatbot that users will need to pay for, incites the lawyer to align closer to Hanff.

"Even if they don't sell personal data, they use it to perfect their product," Hillemann notes.

Interestingly, here is ChatGPT's own answer when asked, 'How does ChatGPT deal with personally identifiable information?': "As a language model, GPT-3 does not have the ability to collect or store any personal information. It can only process the information that is given to it as input and respond with generated text based on that input. When working with personal information, it is important to follow data protection laws and regulations such as the General Data Protection Regulation (GDPR) or California Consumer Privacy Act (CCPA) to ensure that the personal information is being handled appropriately."

Here, the chatbot focuses solely on the trained model and how it can be used without referring to the data-collecting process. "It shows that for OpenAI, the value is the model, not in the training," Hanff argues.

Dealing With Inaccurate Data

Another issue with ChatGPT and other generative AI models is that, by scraping vast quantities of unlabeled data, they are at risk of using inaccurate information.

"This inaccurate data – be it fake news, misinformation or simple

"We're not ready, as a society, to deal with these technologies"

Show on the streaming platform Twitch, tells *Infosecurity*.

"Just because something is online doesn't mean it's legal to take it. Scraping billions or trillions of data points from sites with terms and conditions which, in themselves, said that the data couldn't be scraped by a third party, is a breach of the contract. Then, you also need to consider the rights of individuals to have their data protected under the EU's GDPR, ePrivacy directive and Charter of Fundamental Rights," he adds.

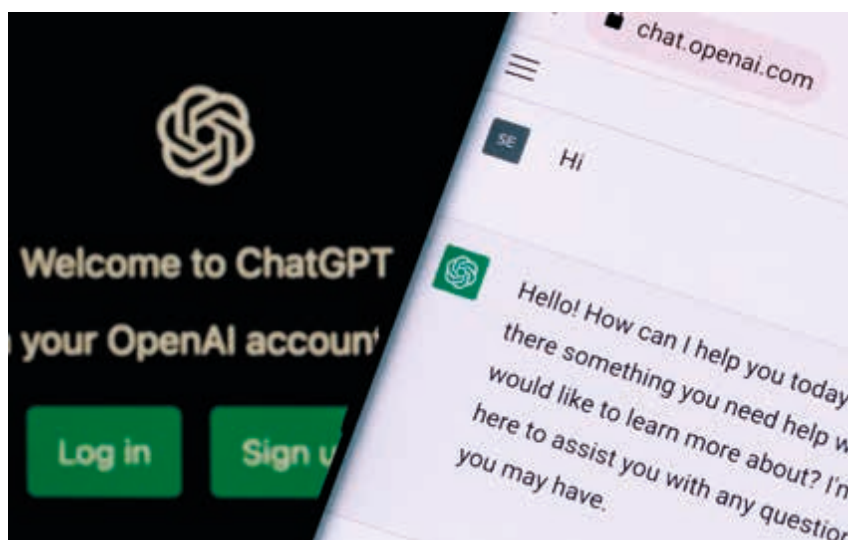
Dennis Hillemann, partner at the law firm Fieldfisher, explains that

is allowed under the fair use principle in certain circumstances, including research, quoting, news reporting, teaching, satire or criticism purposes.

Hillemann says it is likely OpenAI would lean on this defense regarding the data they used to build their ChatGPT model.

According to Hanff, however, none of the fair use conditions apply to their AI models. "Fair use only gives you access to limited information, such as an excerpt from an article. You can't simply grab information from a whole site under fair use; that wouldn't be





human errors – is not only used by people but also feeds the model itself. And, as I understand it, ChatGPT can judge whether a piece of information is correct. That means that, if the model initially has a lot of inaccurate data about someone or something, its judgment will be flawed. Then there's a breach of EU GDPR, which requires organizations to verify a piece of information before processing it," Hillemann explains.

Hanff agrees: "I've looked at a few privacy policies created by ChatGPT. Because the material it's been trained on comes from the internet and a great deal of material around privacy policies

and social media to create the global online database.

Kohei Kurihara, CEO of the Privacy by Design Lab, says there is a good chance that scraping the internet to build a generative AI model like ChatGPT's breaches contracts with platforms such as social media sites.

"Any massive scraping of data without the users' consent is a privacy concern," he tells *Infosecurity*.

However, Kurihara also argues that the case of Clearview AI is different because the firm was specifically scraping biometrics data, which is particularly sensitive, and was using it for law enforcement purposes.

"We don't allow cars to leave the factory without seatbelts, and the same should be true for AI models"

on the internet is wrong, organizations using the chatbot to create their privacy policies put end users at risk of being misinformed about the way their data is being processed."

Foundational Models in a Legal Vacuum

Hanff notes that this is not the first time a data-scraping model has come under scrutiny. He highlights how facial recognition company Clearview AI was fined by multiple supervisor authorities across Australia, the EU, UK and US.

In the UK for example, the company was fined over £7m for using images of people that were collected from the web

No legal action against OpenAI's internet data scraping model has been taken yet. However, Kurihara says, "time will tell if it is deemed unlawful as well."

Hillemann adds that another legal case that could set a precedent in judging foundational models is the Stable Diffusion lawsuit, in which artists have sued the UK-based firm Stability AI for using their work to train its image-generative AI model.

"What's at stake here is copyright infringement and not privacy violations, but both cases are asking the same question: 'Is it okay to scrape the internet, with its personal information and copyrighted work, and use it to

generate new content and build a business model on it?' We've never been in such a situation before, except perhaps with Google, where a company is scraping the whole internet and releasing it in the wild. Meta or Apple have used data in very concerning ways too, but for purposes that stayed within their own business."

Call for Ad-Hoc AI Regulators

The situation could become more concerning in the future, Hanff argues. "Microsoft, who announced it would invest \$10bn in OpenAI over the coming years, now has an AI that can completely copy your voice signal from three seconds of audio. Not only have they used data illegally to train their AI, data that was biased and are planning on using models that are breaking fundamental privacy rights, but they're also potentially creating an antitrust issue where it becomes impossible for people to compete with machines."

"We're not ready, as a society, to deal with these technologies," Hanff also claims.

"I would like to see specific AI regulators with technical knowledge capable of auditing OpenAI at a very deep level – ones that would be different from data protection and privacy regulators because the nuances of the technology are much more difficult to understand and regulate. If an AI technology is dangerous, it should be removed and retrained until we have a safe model for everyone to use. We don't allow cars to leave the factory without seatbelts, and the same should be true for AI models," he says.

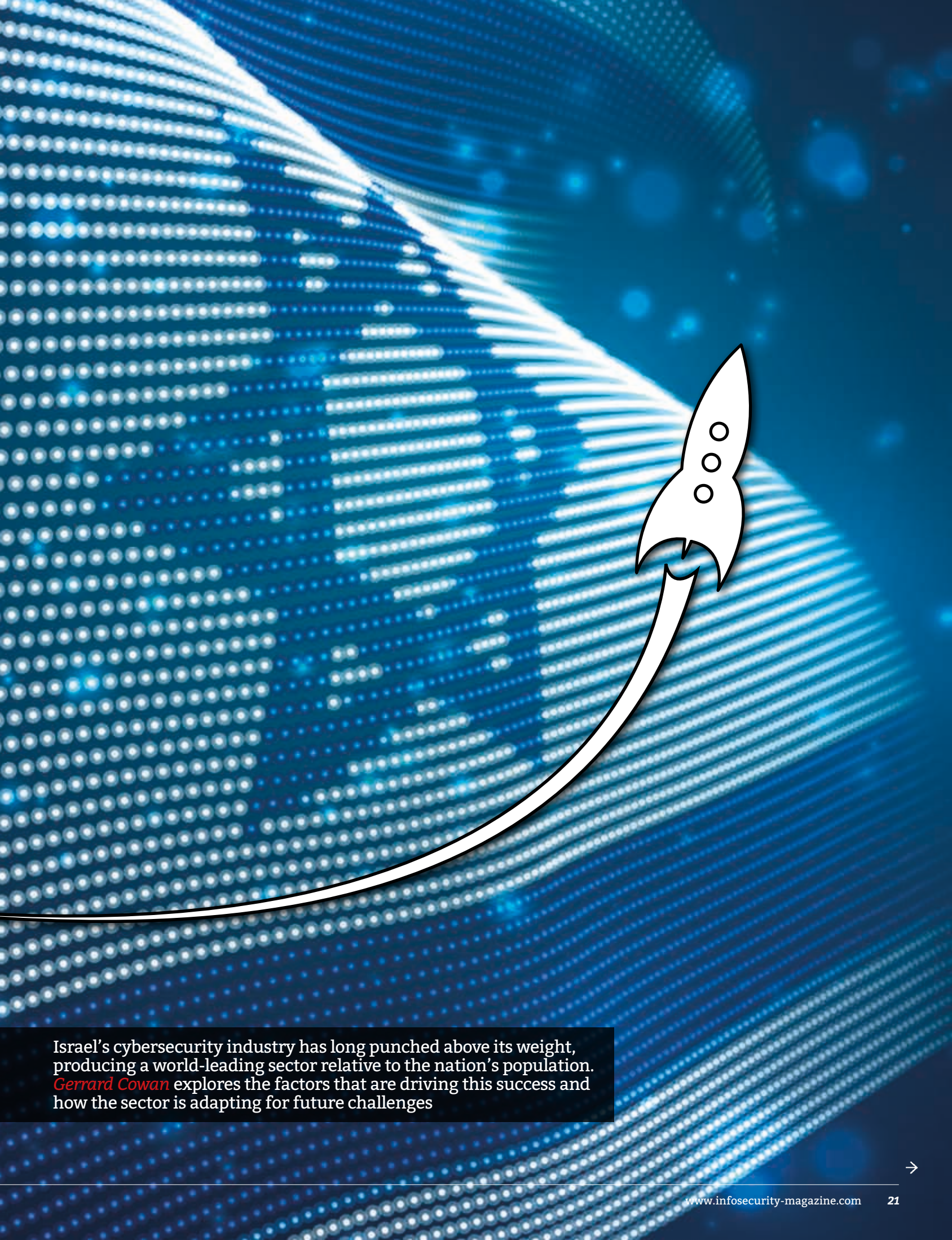
More optimistically, Hillemann argues, "While we have to look at the risks, we should not forget the benefits of these tools. And these are intrinsically linked to the business model generative AI firms have invented."

With the EU's Artificial Intelligence Act underway and similar initiatives being proposed in other countries, the impact of generative AI models on privacy will probably be on the regulators' agenda for years to come.

Meanwhile, OpenAI, Stability AI and similar technologies could be increasingly challenged by privacy advocates to disclose the safeguards they have put in place to protect their users against data violations ●●●

OpenAI was contacted by Infosecurity but did not respond to requests for comment on their training model. The company provided a fact sheet but none of the privacy concerns were directly addressed.

THE STORY OF ISRAEL'S **BOOMING** CYBER STARTUP SECTOR



Israel's cybersecurity industry has long punched above its weight, producing a world-leading sector relative to the nation's population. *Gerrard Cowan* explores the factors that are driving this success and how the sector is adapting for future challenges

Israel has offered cybersecurity startups a place to grow, find investment and leverage innovation-driven young talent in the country.

The Israeli cybersecurity industry has grown about five-fold over the past decade, says Dadi Gertler, executive director of innovation and technology partnerships at the Israel National Cyber Directorate (INCD), a government body that oversees Israeli cyber defense in the civilian sphere.

Gertler attributes this growth to three major factors. First, the cybersecurity market globally has grown dramatically due to rising cyberattacks from cybercrime groups and nation states. Second, the country's cybersecurity industry is part of a wider, successful high-tech industry which has successfully leveraged talent and investments. Third, Gertler points to the experience gained by young Israelis through service in the Israel Defense Forces (IDF), from which they retire

“bring together the pillars of the industry – companies big and small, Israeli and multinational, startups to those in the strongest commercial phase, academia, R&D institutes and the government.”

There have been two major trends in recent decades that have led to the boom in cybersecurity in Israel according to Cyber Together Chairman Ron Moritz, who is also a cybersecurity venture partner with venture capital firm OurCrowd and entrepreneur-in-residence with Australian cybersecurity accelerator CyRise.

First, Moritz explains, when Israel was building out its cybersecurity sector in the 1990s, its local industry was not sophisticated or mature enough to provide development partners for new companies. For an Israeli company to learn how its solution should operate when placed into an enterprise, it had to go to the US or Europe.

The problem was not to do with size, but with the capacity to solve problems, Moritz says. However, in the early 2000s,

The second factor was down to the military, with signals and intelligence units – such as Unit 8200 – becoming innovation hotbeds and incubators for new technological entrepreneurs.

“They’re facing very sophisticated attackers and they have to do things that are very creative, because there’s no toolkit they can simply find to deal with the problem,” Moritz tells *Infosecurity*.

According to a report from the Start-Up Nation Central NGO, which promotes Israeli innovation around the world and provides data on the Israeli innovation scene, there were 676 active cybersecurity companies in Israel in late 2022, which each had a presence in one or more subsectors, ranging from data protection to network and cloud security to risk and governance, risk and compliance (GRC) management.

Finding Funding

In terms of funding, however, the past two years have been something of a rollercoaster, according to Start-Up Nation Central data. There was a decline in capital raised of about 60% in the cyber sector between 2021 and 2022, falling from about \$6.6bn in 2021 to \$2.8bn in 2022. However, the number of funding rounds remained stable, which the report says “may actually be a more significant figure.”

Start-Up Nation Central CEO Avi Hasson notes in the report that 2021 was actually the exceptional year for the high-tech industry in the country, with an “unrealistic quantum leap in investments, market cap and transaction multiples.” This corrected itself in 2022; alongside global macroeconomic trends, there was a significant decline in investments, particularly in the second half of the year. “Nevertheless, the investments, exits and high levels of demand continue, but in a more prudent and measured manner. This in itself is a positive, long-term phenomenon. However, we do forecast some difficulty in VC funding that might have an impact on the available capital for investments in 2024 and 2025,” Hasson says in the report.

“Israeli companies that provide a focused narrow solution will need to find ways to integrate into wider platforms or expand their offering”

with “a strong sense of urgency and an innovative spirit.”

There are a number of organizations that work to promote Israel's cybersecurity industry, including Cyber Together. Alon Rafaeli, founder and partner in the organization, explains that Cyber Together is a national cybersecurity trade body that aims to

the industry in Israel matured, partly due to the nature of the attacks being experienced at that time.

“We found the companies didn't have to leave Israel to find an enterprise that they could partner with – or multiple enterprises they could partner with – to refine and develop their early prototypes and their early experimentation,” he says. “By the time they were ready to go overseas and actually begin serious commercialization efforts for their ideas, they already had a fairly mature product more and more ready for primetime.”

While 2022 has been challenging on a global scale, the ability to raise funds is still a key benefit of establishing a company in Israel, said Gil Don, CEO of Wib, an Israeli startup with a focus on API security. “If you have in place the right talented team, like we did, and you have the right product market fit, it will be easier for you to raise money in Israel, because of the success stories of cyber companies [from Israel],” he says.

Second is the ability to tap an experienced pool of talent, either from the IDF or other companies. “Don’t think it’s easy to bring in these guys, but they will want to join you if they understand you’re in the market in the right time, at the right place and space,” Don says.

Gil Shulman, head of product at Wib, is himself a veteran of Unit 8200. He says the experience provides potential employees with an “expedited maturity,” and not just when it comes to technology knowhow. “Technology is tools – what we learn are the use cases, and how we can create technology that is useful.”

Ilan Barda, CEO of Radiflow, an OT cybersecurity company offering solutions for industrial entities and critical infrastructure environment, also highlights the military experience, noting that many founders come from the IDF, which has confronted cyber challenges over the past several decades.

“This by itself made Israel a hub for cybersecurity firms and educational institutions focused on cybersecurity,” Barda says.

Widening Reach

Looking forward, Barda sees a need for a more holistic approach from the industry as it adapts to the challenges of the future. Barda notes that the cybersecurity realm is segmented into many different parts, including cloud, API, OT, IT, etc. However, as cyber challenges evolve, CISOs are looking for more multifunctional solutions, he argues. “Israeli companies that provide a focused narrow solution will need to find ways to integrate into wider platforms or expand their offering to [multiple functions].”

Additionally, Barda says that Israeli startups can be driven by technological innovations, but in the current economic environment, will also have to “optimize their product-market fit and better articulate their sales pitch.”

Aviv Cohen, chief marketing officer at Pentera, a company offering an automated security validation platform, also highlights the talent pool of IDF veterans, along with a natural movement of talent between cybersecurity firms, which is helping to develop second and third generations of skilled security

cybersecurity organizations will remain a prominent player in the marketplace.”

However, he thinks the economic climate could lead to more consolidation in the market and a shift to a focus on profitability, rather than pure growth rates. “This is a necessary adjustment that is happening across the industry, while simultaneously it continues to flourish and innovate.”

Cyber Together’s Moritz also highlights the increasing challenges in the marketplace when it comes to funding, which creates new pressures for

“They’re facing very sophisticated attackers and they have to do things that are very creative”

developers who can learn from more experienced leaders.

“Another benefit of launching a cybersecurity firm in Israel is the existing cybersecurity reputation, both professionally and among investors. While it is never easy to secure funds for a new start-up, the innovation that Israel has become known for has attracted a significant number of investors for cybersecurity to congregate and pay attention to our market,” Cohen says.

Changing Future

Cybersecurity has largely maintained its growth trajectory, despite the global economic downturn, Cohen says; indeed, hackers may be even more motivated to capitalize on companies that do not have the resources to boost their security.

“The potential for Israeli cybersecurity only continues to grow. As more digital technologies appear and the threats evolve, new challenges are introduced,” he adds. “The Israeli ecosystem is capable of addressing these issues and building solutions in a rapid manner. We believe this trend will continue and that Israeli-based

companies that had become used to much greater access to finance. “I don’t think all of the companies are going to find the money they need,” he says. “I think we’re starting to see some of that broader economic influence on cybersecurity.”

However, the INCD’s Gertler says that while there was a global decline in investments in 2022 when compared with 2021, “the cybersecurity challenges enterprises and governments are facing daily are still growing year over year and the cybercrime and cyberwar frontiers are becoming more and more brutal.”

Against this backdrop, the INCD projects continued growth and demand for advanced cybersecurity solutions and services.

“AI will take a wider role in this effort. The main sectors that will suffer more than others are healthcare, education and transportation as they are less protected and relatively easy targets for cybercrime groups,” Gertler warns. ●●●END

Point

Is AI Essential to Cybersecurity?

Yes



Holly Grace Williams

Managing Director, Akimbo Core
Holly Grace's early career was spent in the military working in roles such as site security officer. She is the founder and technical lead for Akimbo Core, leading both the development of the software platform as well as the security testing team capability.
@HollyGraceful

I often see advocates for the use of artificial intelligence (AI) in the cybersecurity space coming out with snappy soundbite reasons as to why you should be using these technologies to defend your organization. These include phrases like 'well the attackers are already using it, so why aren't you!' and pithy comments such as 'you should fight fire with fire!'

Instead of approaching this topic with worn out idioms, I want to present to you some simple ways that attackers leverage AI to cause great harm to organizations – and how you can utilize these technologies today to better protect your systems.

Blackboxes

Before I get to that, I want to try and address some of the reasons that organizations might feel restrained from investigating the use of AI to protect their systems. I think the primary reason is just plain bad marketing. There are two ways that AI is mentioned in the context of bad marketing for cyber defense products – the first is simply overpromising on capability, making AI systems sound infallible, and the second is false equivalencies, such as "our AI defense never sleeps!" (as if we haven't thought to address the issue of staff needing to sleep through the use of shift-patterns and "follow the sun" SOC implementation).

The second problem with bad AI marketing is companies that hold up an AI blackbox that promises to outperform your current capability without ever explaining how they achieve that. It's often just "we have AI, therefore we're better" or similar veiled statements.

I don't think blackboxes that offer protection through opaque means other than the promise that it uses AI are useful. The benefits that AI brings and the broad mechanisms through which it achieves those benefits should be described.

Vendors that don't share details on how their product works shouldn't be trusted with blind faith, yet equally, AI/machine learning (ML) shouldn't be ignored as a potentially useful capability simply because bad marketing exists.

Overcoming Hurdles

That said, I think there are three hurdles we must traverse to demonstrate that AI-based security is beneficial to organizations today. The first is: Are there problems in cybersecurity that AI/ML is not only well suited for, but potentially better at dealing with than both the existing manual or signature-based approaches? The second hurdle is: Are we able to develop these systems with the current level of AI/ML available on the market? The third is: Are these solutions required today or can we put off the investment until the future?

Regarding the first issue, of finding problems in cybersecurity that AI/ML is well suited for, there are several, but two good examples would be anomaly-detection and data-mapping. Anomaly-detection is the art of detecting unusual network traffic or user behavior. ML is generally well suited for these 'pattern matching' applications. As for data mapping, I'm referring to finding all of the places on an organization's network that confidential, sensitive or personal data is stored.

I've worked with several companies who have been worried about how they can find all of the different locations on their network that their busy, distracted and occasionally down-right disorganized staff have placed files that contain personal data. From birth certificates to financial paperwork, many companies have messy networks and files stored in places they shouldn't be. However, building a ML model that is able to detect common files that contain personal information is fairly trivial these days. There are off-the-shelf

solutions that can find personal data, but even building something in-house is not too difficult.

Add to this the fact that the risk of a significant data breach gives an attacker a huge amount of leverage over a target organization. We've seen threat groups utilize the threat of said breach as a means of coercing companies into paying ransoms as part of a ransomware attack.

We might start seeing cyber-attackers utilizing tooling like this in the future to more quickly and effectively find sensitive data on company networks to ensure that their attacks cause maximum potential impact – and to do that faster than defensive teams can react. We're always looking for more efficient ways to hunt out sensitive data during penetration tests to demonstrate the potential impact of a data breach, so there's no reason to think that the bad guys aren't looking for more efficient ways to do this too.

In summary, are there cybersecurity problems that AI/ML is well suited for? Yes, there are many cybersecurity tasks that fall into either 'anomaly detection' or 'pattern matching' and ML is uniquely well suited to those. These include finding files that contain PII across disorganized network shares.

Is the current state-of-the-art for AI/ML capable of solving these problems? Yes, and not only that, but solutions for these tasks are no longer considered novel, with off-the-shelf capabilities for detecting PII well established now.

Finally, are companies required to investigate these capabilities today or is this something that we can put off for a while? Well threat groups are already targeting personal data during both data breaches and ransomware attacks. Therefore, cleaning up network storage and monitoring for unusual access patterns should be something companies are working on right now ■

Counter-Point

No

No, not as long as humans remain the primary end user.

AI definitely does have a place in training users on best cyber practices. But ultimately, it's the adaptive mind of a user or somebody who's receiving an email or text phone call who determines whether an attack is successful or not. That doesn't mean that some of the training can't happen via AI, but it doesn't mean that it has to happen that way.

AI-based training can be useful when AI is trying to understand what a user might need to learn or where they're going to be most susceptible. AI can also certainly be a force multiplier.

But if you're asking the question, 'is AI essential for security?' then I'd argue that AI can actually be used to prove that the human is essential for security. This is because when we use AI as part of training, learning attack types and running phishing simulations, it is limited in scope. At the end of the day, the human is always essential and technology can never be the ultimate protector. If you don't believe me then explain how (at least for now) AI will prevent a human from being socially engineered in a bar, writing sensitive information on a whiteboard, or not properly disposing of sensitive paper-based documents? And that's just naming a few potential issues.

The truth is that the human is the critical security layer. We can use AI to bolster training for a human, but ultimately, it's a piece of the puzzle. At the end of that chain is somebody that's using a human mind to make a decision that results in an action.

The question isn't 'do we use AI or do we not use AI?' The question is really 'is AI necessary for security?'

The answer to this is No. You don't necessarily need AI in order to improve your security. But can it be useful? The answer is absolutely it can.

We can nod our heads to some of the critical security areas and use cases where AI plays a big role. As I mentioned before, AI is a great force multiplier and its usefulness is growing. But when it comes to things like social engineering or this last mile where things are transitioning from digital to physical, AI's usefulness starts to peter out. This is because at that stage you are dealing

designers never anticipated, allowing threat actors to bypass it.

What we've seen for decades now is that despite the faith we put in technology and all the great advances being made in AI and machine learning, the human (the chaos factor) way that we approach things tends to find ways to bypass all of that and create unexpected responses, which leads to data breaches.

With ChatGPT, we're seeing AI advance to become better at simulating human thinking. An argument could be made that if AI, through things like ChatGPT, is

"The truth is that the human is the critical security layer"

with a human and that person's mindset, biases and habits.

At least for now, you can't depend on technology in those cases, and you haven't been able to for decades despite the bold promises being shouted from booth barkers on the vendor floors of the world's largest security conferences each year. You can't depend on technology to create a protective bubble around a user or totally protect a system from a user's mistakes, negligence or malfeasance. Technology and AI will not necessarily have the same anticipatory function as a human (although maybe advocates of ChatGPT would disagree with that).

The reason why attackers are able to bypass technology is because they're using or exploiting technology in ways that have not been foreseen by the designer of that technology. Or because the end user deploys a piece of technology negligently or unintentionally in a way that the

showing that it can simulate some of that erratic and unpredictable nature of humans, couldn't it be true that in five to 10 years we will reach a point where AI can create that protective bubble?

When you get down to the weeds of it, some aspects of AI still operate very much like predictable decision trees. So, when you have a single human on the other side of that, you still have a mind which can pivot very quickly. That means, at least for now, the human mind wins out.

That being said, this is a space that we need to pay close attention to. We are seeing amazing advances in AI at an accelerated pace. Heck, threat actors are even already using ChatCPT to produce malicious code and create convincing social engineering scams and phishes. But, for now at least, I see the human mind, human behavior and the power we have as a collective as being more critical to security 🍌



Perry Carpenter

Chief Evangelist and Security Officer, KnowBe4
Perry Carpenter is co-author of the recently published, *The Security Culture Playbook: An Executive Guide To Reducing Risk and Developing Your Human Defense Layer*. This is his second Wiley book publication on the subject. He is chief evangelist and security officer for KnowBe4.
@PerryCarpenter

HOW SSI PUTS IDENTITY BACK IN THE OWNERS' CONTROL

Danny Bradbury investigates whether SSI can solve a digital identity challenge that has perplexed tech and non-tech organizations alike for decades



The Web 3 concept promises to solve many of the problems present in the internet's current form and it will put users in greater control of their data online including how they share information about themselves.

A crucial component of Web 3 and the notion of a next-generation decentralized web is centered on the idea of secure sovereign identity (SSI).

In this model, instead of large centralized big tech platforms running most of the apps and services, technology users get to run their own apps and own their data, whether on a blockchain or via a federated protocol.

It is a concept that could go some way to providing a better approach to verifying a person's identification without relinquishing control of sensitive data.

A recent anecdote recounted by Drummond Reed, chief digital trust officer at Gen (formerly Symantec), highlights why we need to consider the Web 3 approach as a better way of verifying credentials.

Reed was trying to get into a bar in Boston. "The bouncer said, 'Yeah, just give us your ID' and they popped it into a copier machine," he recalls. He grabbed his ID back, spun on his heels and told his colleague that they were going to another bar.

"I expect to have my ID checked, but there is very sensitive information on there. And there's no way they should be keeping a copy of it," he complains. What's the worst that could happen? Identity theft, for one. He also points out that a woman might be even more cautious about letting a strange man copy something with her name and address on it.

This kind of problem is rampant. Anyone forced to upload an image of their government ID to a recruitment site, or worse still asked to email one to their bank, surrenders control of sensitive data and puts themselves at risk.

Digital Wallets to the Rescue

SSI, or decentralized identity, may be able to provide a better means of verifying identity. In this model, the person who owns the data (the holder and in our case Reed) keeps those credentials in a digital wallet. They show only the credentials they want to whomever they choose. The person verifying that credential doesn't get to keep it. They cannot sell it. No rogue employee can use it to stalk you or sell it to data thieves.

SSI can transform traditional interactions around identity. Holders present their credentials in the same

way that they might pull an ID card or a membership card from a physical wallet. The difference is that they can do it digitally and be more selective in their disclosure. That changes the scenario in the bar with the copier, says Reed.

"The ideal scenario is that there's an iPad sitting there with a QR code on it," he says. "I grab my phone, scan the QR code, and a message pops up saying they want to prove that I'm over whatever the legal drinking age is in that bar."

The patron would press a button on their digital wallet granting access to the credential, and "in about a second, that screen goes either bright green or bright red. Done."

These wallets will also simplify more complex workflows, explains Phil Windley, co-founder of the Internet Identity Workshop conference and author of a new O'Reilly book, *Learning Digital Identity*. He recalls signing up to popular recruitment site Guru.com just to answer a question that he'd been told someone had posted there. That involved a grueling 12-step process, including uploading ID information, solving captchas, verifying emails and creating passwords.

A wallet with a decentralized credential would have made things so much easier.

"You'd go from this 12-step process that has me typing lots of stuff into forums, to a three-step process that is just incredibly easy for me to navigate."

We have digital wallets on our phones already, Reed points out (Apple Pay is an example). "But they aren't using open standards and can't accept and share our credentials with anyone that we choose," he explains. "SSI is about solving that problem."

Verifiable Credentials

The World Wide Web Consortium's (W3C) Verifiable Credential (VC) data model seems to have the most traction today when it comes to open standards. A VC comprises a set of claims about the holder made by an institution known as an issuer.

A government could issue a claim that the holder has a specific name, address and age. An employer might claim that the holder works at the company in a particular role. A local tennis club might claim that the holder has a membership there.

The third party in the transaction is the verifier. This is the organization that needs to verify something about the holder. A recruitment site could verify that they are who they say. A loan company could verify that they really are employed. A tennis league could verify membership, allowing a player to participate.

When it comes to a verifier being able to trust that the holder didn't falsify those credentials the key is cryptography. The issuer digitally signs the claim with their own signature, which it stores in a public repository. That could be a database, but it could also be a blockchain. The verifier can check the digital signature against the signed claim to ensure that it came from the verifier and that it hasn't been altered.

"Ultimately, I hope we have lots of credentials," says Windley. "I've got several thousand entries in my password file, and I would expect that I might have credentials relating to a lot of those."

Decentralized Identifiers

We must also be able to uniquely identify a particular entity, whether that's an issuer, an individual or a verifier. This would overcome issues of confusion when a claim came from an individual with the same name as another, for instance a claim that John Smith earned a

"You'd go from this 12-step process that has me typing lots of stuff into forums, to a three-step process that is just incredibly easy for me to navigate"

degree at Oxford relates to him and not to another John Smith. Or that it was issued by the University of Oxford, as opposed to nearby Oxford Brookes University, formerly Oxford Polytechnic.

In June 2022, the W3C made the concept of decentralized identifiers (DIDs) a standard (Reed was a co-editor). These are unique alphanumeric strings that their owner creates and digitally signs themselves.

"You can create your own IDs and give them to issuers that they will embed in your credential," explains Mary Lacity, distinguished professor and executive director of the Blockchain Center of Excellence at the University of Arkansas' Walton College of Business.

Ad hoc creation also makes it possible to create multiple DIDs. That stops

someone tracking the same ID across different organizations, allowing you to have separate personas for different activities and memberships. “For every credential, I want my own DiD so that I have more privacy-enhancing things than a national identity number or social security number,” Lacity explains.

Other Standards

While VCs and DiDs have gained significant traction in the SSI space, there are multiple standards, either existing or in development, supporting some aspects of SSI. For example, ISO’s Mobile Driving License (MDL) standard supports the storage and exchange of electronic driving license information.

Some candidates have emerged from the blockchain community. Ethereum co-founder Vitalik Buterin has proposed Soulbound NFTs, a form of non-transferrable non-fungible token that would contain claims about a holder.

AnonCreds is another standard that uses zero-knowledge proofs when presenting credentials. This is a privacy-preserving concept meaning that users don’t have to use identifiers at all to prove things about themselves. In November 2022, long-time AnonCreds user The HyperLedger Foundation officially adopted the project.

Yet another is the Digital Travel Credential (DTC) from the International Aviation Travel Authority (IATA), which is positing it as a way to digitize passport information.

One Stack to Rule Them All

How will companies unite these and other SSI technologies? The Trust Over IP Foundation (TOIF), which falls under the umbrella of giant open-source non-profit the Linux Foundation, has opted for a first-principles approach where it proposes

many of the necessary interoperability protocols from scratch.

In January 2023, the TOIF launched a working group to develop the Trusted Spanning Protocol (TSP). Reed, who is on TOIF’s steering committee, likens this to the IP protocol’s linchpin role in the TCP/IP stack.

TSP will form part of a four-layer technology stack that TOIF is developing to communicate trust between parties over the IP protocol. At the bottom layer, it will help unite different documented methods for implementing DiDs (there are currently over 80). At the top (application) layer it will support use cases in verticals ranging from payments

customers pushed back against dictating interoperability standards.

“We give you the smallest set of technologies that are necessary to have the conversation and then it’s up to you,” he says.

SSI in Action

Despite the jostling over stacks and standards, the SSI/decentralized concept overall is gaining significant traction. Microsoft relied on VCs and DiDs when developing Entra, its implementation of SSI that integrates with Azure. “Now, anybody who’s using Azure AD can start to issue credentials,” muses Windley. The appearance of

“You can create your own IDs and give them to issuers that they will embed in your credential”

to healthcare. It also includes a related ‘governance stack’ outlining the rules and relationships for the different players in these trust networks.

The TOIF submits what it develops to standards organizations like the W3C, IETF and ISO rather than trying to ratify the standards itself. Reed’s vision is that organizations including its extensive list of steering members and contributors will integrate with elements of the tech stack as these bodies standardize them.

However, there are some notable absentees from that member list, including Apple, Google and Microsoft. Ankur Patel, partner product manager at Microsoft, says that the company didn’t want to join TOIF because its

SSI capabilities in these platforms will hopefully accelerate adoption.

The UK NHS used VCs as the basis for an SSI-based digital health passport system for health workers, enabling them to transfer more easily between health facilities. Microsoft provided the Azure-based back-end, while Evernym (at which Reed worked, and is now part of Avast, which in turn is part of Gen) provided the wallet tech.

In Canada, the province of British Columbia is using VCs for various applications including verifying organizations and people based on the TOIF’s trust model and a Hyperledger-based back-end wallet.

The EU has also proposed using VCs as the basis for a European Digital Identity (EUID) wallet. This would allow anyone who can get a national ID card to carry their own digital credentials for international use within the bloc.

There is some overlap between SSI and Web 3, as SSI is a decentralized tech that puts ownership back in the individual’s hands. However, this needn’t be a Web 3 play, and it has nothing inherently to do with Web 3-linked concepts like the metaverse and NFTs.

Instead, SSI applies decentralization to identity credentials in multiple scenarios. In doing so, it attempts to solve a digital identity challenge that has perplexed tech and non-tech organizations alike for decades. Perhaps finally, overreach by bouncers and bureaucrats with scant appreciation of privacy will be a thing of the past ●●●





BIDEN'S ZERO TRUST MANDATE

Phil Muncaster examines the story of President Biden's Executive Order so far and the potential impact of zero trust on public and private sector security

Over the past decade, US Presidents on both sides of the political divide have issued Executive Orders (EOs) designed to enhance the US' cybersecurity. Yet few could have predicted that the missive sent down from on high by octogenarian President Joe Biden would be the biggest and boldest to date. In the end, though, Biden's EO 14028, *Improving the Nation's Cybersecurity*, was widely praised by industry experts on its publication, just a few months after the Democrat took office.

Key among its requirements was a mandate for federal agencies to develop plans to implement a zero trust architecture. This promises a new framework via which to make federal government security fit-for-purpose in an age of cloud-first, application-centric working, and pervasive state-backed and financially motivated cyber-threats.

"Incremental improvements will not give us the security we need," Biden says in his EO. "Instead, the federal government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

The question is what's happened since May 2021, and how successfully might the mandate not only transform federal government security, but also spur businesses to follow suit?

Why the World Needs Zero Trust

Government and private sector organizations across the globe operate in a world of cyber risk very different from that of 10 or even five years ago. It is one increasingly dominated post-pandemic by cloud infrastructure and applications, remote working endpoints and digital transformation. This in turn has created a more complex and distributed IT environment, with an attack surface far greater than anything previously seen.

Threat actors bypass perimeter security at will, with phished, stolen or brute-forced credentials available in their billions on underground sites. They exploit vulnerabilities being published each year in numbers so great that many organizations' patching programs are overwhelmed. Cyber-criminals then move laterally once inside networks

using under-the-radar legitimate tooling that fails to set off any alarms. The proliferation of mobile devices in use by employees further increases cyber risk. One 2022 Verizon report estimates that 45% of global organizations were compromised over the previous year via a mobile device. The supply chain adds yet another vector for attack. A Trend Micro study claims that over two-fifths of organizations believe their attack surface is "spiralling out of control."

These trends have given financially motivated cybercrime groups and state-backed actors an overwhelming advantage against network defenders. It has led to a record number of publicly disclosed data breaches and ransomware volumes in 2021, and major government incidents such as the SolarWinds campaign, which compromised at least nine federal agencies.

Although conceived of over a decade ago, zero trust is the perfect approach for managing risk in today's volatile digital world. It mandates that users are only allowed access to enterprise resources according to a policy of "least privilege:" both they and their devices



will be implicitly untrusted and verified/authenticated regularly. Networks are segmented to contain the blast radius of any potential breach, and continuously monitored for suspicious activity.

Actions Following Biden's EO

The first major step forward since the EO was issued came in January 2022 with an Office of Management and Budget (OMB) memorandum titled *Moving the US Government Towards Zero Trust Principles*. It listed several key timelines for agencies. First, it gave agencies 30 days to “designate and identify a zero trust strategy implementation lead for their

key areas: identities, devices, networks, apps/workloads and data.

Forrester senior analyst, Heath Mullins, explains that progress so far has been mixed.

“The EO and memo have spurred action within US federal government from a planning perspective, as well as creating a framework outlining specific requirements,” he tells *Infosecurity*.

“With that being said, the answer varies widely, dependent upon the agency in question. Overall, my federal clients are moving forward with purpose, but there is still quite a bit of confusion about how to actually implement the overarching strategy.”

Part of that confusion may be related to the fact that government practitioners

“The bad actors will not sit on their laurels just because an organization has implemented an advanced state of zero trust. Malicious attacks will forever evolve, and, through continuous monitoring and assessment, organizations’ zero trust posture must change with the times.”

The Bigger Picture

The federal government has an opportunity to lead by example, and in so doing improve baseline security across verticals and nations, according to Hendra Hendrawan, security technical councillor at the Info-Tech Research Group.

“First, the mandate would showcase the commitment by the government to protect its people’s personal information, which is a valuable asset. Second, it would prove that implementing a zero trust architecture in a complex IT environment is challenging but achievable. Finally, it would reiterate the data protection imperative for federal agencies and other sectors or industries,” he tells *Infosecurity*.

Forrester’s Mullins agrees, arguing that organizations in highly regulated industries and federal contractors will be the first to follow suit, as a cost of doing business with the government.

“For example, a manufacturing organization may create a single piece of hardware which, in turn, is installed into a top secret device. This manufacturer should have a robust zero trust solution implemented, even if the part itself is not highly classified,” he explains. “Another great example is the financial industry. It is not just good practice; it may become an absolute requirement to engage in government contracts or reporting.”

Mike Aiello, CTO of threat defense vendor Secureworks, also sees huge

“Zero trust, as a concept, is a continuous assessment of an organization’s security posture”

organization.” These will be responsible for coordination, engagement with the OMB, and planning and implementation efforts.

Next, it demanded agencies submit to the OMB and the Cybersecurity and Infrastructure Security Agency (CISA) an implementation plan for fiscal year (FY) 2022-24 and a “budget estimate” for FY 2024. The OMB said it wants agencies to “achieve specific zero trust security goals by the end of FY 2024” – goals which should be organized using CISA’s *Zero Trust Maturity Model* (see box out). These cover capabilities in five

might be viewing zero trust through the wrong lens. As the memo makes clear, it is just “a starting point” rather than a “comprehensive guide to a fully mature zero trust architecture.” Different agencies may find different ways to plan and implement its requirements, and they are encouraged to work with the OMB and CISA to share best practices and lessons learned. However, there is no definitive end point when they will achieve zero trust, according to Mullins.

“Zero trust, as a concept, is a continuous assessment of an organization’s security posture,” he adds.



promise in a new wave of zero trust projects radiating out from government.

“We see the zero trust mandate as a great step in creating standard sets of controls that work together to build an extended ‘kill chain’ that attackers must defeat to be successful,” he tells *Infosecurity*. “That means that in the zero trust model, the attacker needs to defeat multiple components of an integrated security stack, rather than single security solutions. Bringing more context to security decisions results in better security outcomes.”

Where to Start

Yet delivering on the promise of zero trust will not be easy for organizations, given the complexity of modern IT environments. Info-Tech’s Hendrawan argues that CISOs must build out any framework on the principles of “assume breach, continuous verification and least privilege” in order to deliver success.

For Mullins, visibility into the existing enterprise security architecture is a vital starting point.

“Perform an assessment. Understand what you have in place

prior to buying security solutions carte blanche. Clients are sometimes surprised at how far down the path towards zero trust maturity they may be,” he says.

“A perhaps larger hurdle is organizational buy in. Be mindful of the fact that zero trust knocks down traditional security silos. To be effective, CISOs must clearly communicate to the organizational stakeholders why zero trust is important, and how they can help.” ●●● **END**

CISA’s Five Pillars of Zero Trust

CISA’s technical expertise and resources are helping federal agencies to design their zero trust goals. Key among these is its Zero Trust Maturity Model document cited by the OMB.

The “five pillars” outlined in that document are:

1 Identity:

“Enterprise-managed identities” are used by staff to access workplace applications, with MFA protecting those individuals from phishing and other online attacks.

2 Devices:

The federal government manages a complete inventory of every used for official business, and can prevent, detect, and respond to incidents targeting those devices.

3 Networks:

Agencies encrypt all DNS requests and HTTP traffic inside their environment and begin the process of network segmentation.

4 Applications and Workloads:

All applications are treated as internet-connected and therefore at risk and are regularly subject to “rigorous empirical testing.” Agencies also welcome external vulnerability reports.

5 Data:

Agencies begin categorizing data based on protection requirements and deploying relevant protections – leveraging cloud-based monitoring of user access to do so. They also implement enterprise-wide logging and information sharing.





Jerich Beason is renowned for sharing his expertise in leadership and his experience navigating a career in cybersecurity, *James Coker* speaks to Jerich to find out more about the values that underpin these ideas and his desire to educate his peers

JERICH BEASON

Every day I try to help at least one person and add value to their life,” says Jerich during our video interview. The notion of ‘giving back’ is prevalent throughout our conversation, and is indicative of Jerich’s attitude to cybersecurity, and indeed life.

Many aspiring and current industry professionals across the world are benefitting from Jerich’s wisdom following many years in a range of security leadership roles, leading to his current position as CISO of the Commercial Bank and Capital One Software at Capital One bank. He uses just about every medium possible to engage with the cyber community, including but not limited to regular in-person talks and panels at conferences, writing whitepapers and articles, hosting a cybersecurity podcast, and fronting a security show on YouTube.

Jerich also is also an instructor for LinkedIn Learning and the SANS Institute, taking time out of his

busy schedule to teach cyber professionals as they navigate their careers.

Across these various platforms, he is keen to highlight the importance of soft skills in an industry renowned for its technical side. Jerich is especially passionate about managing people in the right way and is determined to inspire a new generation of cyber leaders.

However, he admits that for a long time he was too “chicken” to take on the mantle of thought leader in the field, waiting “until I had a title that I thought people would respect.” This is a mindset he now regrets.

“When I joined the security industry I didn’t really have any role models I could look up to, and we didn’t have social media platforms like we do today,” he explains.

This void in his early years in the sector inspires Jerich to spend so

much time sharing his experiences and knowledge with the wider cybersecurity community, something he finds extremely fulfilling.

“I wanted to help other people see in plain sight some of those things I learned in hindsight,” he notes.

“My professional mission is democratizing leadership and cyber strategies”

With the power of digital communication methods and social media, Jerich is able to share his insights to people anywhere in the globe. Jerich comments: “People are messaging me and commenting from all over the world. It’s surreal, absolutely surreal.”

Democratizing Cybersecurity Leadership

Transparency and sharing information are fundamental to Jerich’s leadership philosophy, which is to empower individuals to succeed and not see glass ceilings. “My professional mission is democratizing leadership and cyber strategies,” he confirms.

Jerich adds that he wants to “squash perceptions of age being a qualifier for any role,” noting that his first leadership position was at the tender age of 24, managing people twice his age.

Part of this approach involves giving his team authority and a voice in the decision-making process, as long as the right guardrails and support mechanisms are in place. If authority is not delegated, he warns that “you’re actually going to stifle their growth and as a result, your own.”

After all, more junior employees “know more about the details than I

ever will and their input on strategy and tactics are immeasurable.”

Jerich now knows that feedback is just as vital for security leaders to receive as it is for them to give out to their team.

“If my goal is to grow and develop leaders, I need the people who report to

me to feel like I’m achieving that goal,” he explains. “I always thought it was a top-down thing – it took me a while to learn it’s more of a 360°.”

Another way Jerich is attempting to change the nature of security leadership is ensuring teams work with the business, rather than be perceived as a barrier to growth. He notes that at the start of his career, cybersecurity leaders were typically chosen for their technical expertise rather than leadership qualities.

They also rarely had a voice at the boardroom level and were seen as “the people who tell you when you can’t do something” across the wider business.

Jerich is committed to ensuring his security teams are aligned with the wider business and helping them achieve its goals in a secure way. In fact, the word ‘no’ is banned on his team. Instead, the answer should always be “yes, if” to any requests from the business. In other words, if the right controls and processes are put in place to make it secure, then any new tool or idea can be implemented securely.

Jerich’s perspectives on empowerment and collaboration have naturally been shaped by real-world experiences, but also underpinned by strong religious and family values around community. →

"It is a lot of what has grounded me and made me who I am as a person," he states.

To understand his perspective better, it is essential to visit Jerich's earlier life and career experiences.

Destined for a Career in Cybersecurity

Raised in Los Angeles, California, in the 1980s and 1990s, Jerich describes himself as a typical kid who "wanted to play outside, make a mess and

Jerich views his time at ITT Tech as "integral to the success of my career" for several reasons. Unlike many colleges at the time, the institution focused on teaching technical skills, such as configuring routers, programming firewalls and building a domain. These skills put Jerich in a position to take a job in the field immediately.

He also highlights these years as crucial to making connections with teachers and other students – skills that would later open doors as he forged his career in cyber. "I unintentionally

This work taught Jerich to take a more holistic view of security and was the first time he was introduced to the notion of governance, risk and compliance. This included approaching security from the NIST 800-53 risk management framework standpoint, the regulatory standard that defines the minimum baseline of security controls for all US federal information systems.

"Prior to that, I specialized in whatever I was focused on – I never really saw the big picture," says Jerich.

While the government was among the first institutions to take cybersecurity seriously, compared to today Jerich says its approach was archaic. He terms this "paper security," where his team operated without many of the tools and technologies that are available today. This meant "a lot of what we did was tedious and manual."

"I wanted to help other people see in plain sight some of those things I learned in hindsight"

drive my parents crazy." In those formative years he also developed a keen interest in computers, as desktops gradually became a mainstay in the average household.

Jerich recalls the first computer he used – one his dad brought home from work that was going to be thrown away by the company. It quickly became apparent that Jerich was something of a natural when it came to IT.

"My dad told me that I taught him how to use MS Paint when I was five, and that was the moment he realized 'maybe this kid knows something,'" he says, grinning. Although Jerich modestly points out that nowadays "a kid knowing Paint at five is actually behind schedule!"

The family then obtained another computer, and certain games were added to it that Jerich was not allowed to play unless his father was in the room. However, desperate to play the likes of *Duke Nukem* and *Doom* more regularly, Jerich figured out how to connect to the computer upstairs from the one downstairs.

He says: "A lightbulb went off, and I started wondering what else I could connect. That started my interest in cybersecurity."

It was a fascination that didn't wain with time. Fast-forward to 2004 and post high school, Jerich enrolled at an ITT Technical Institute (ITT Tech) campus to study for an Associate (AS) Degree in Computer Networking Systems. After graduating in 2007, he went on to take a Bachelor of Science (BS) in Information Systems Security at the same institution, which has since closed, from 2007-2009, while juggling his early jobs.

stumbled upon the power of networking and, more so than education, that really shaped my progress," Jerich reflects.

Variety the Spice of Life

Taking his first job as a systems analyst at Kraft Foods in 2006, Jerich says he "bounced around a lot" in those early years in the sector. "The majority of my early jobs were short-lived because of contracts, outsourcing and layoffs due to the recession in 2008," he notes.

Jerich admits this was a difficult period for him, but in retrospect, appreciates it taught him invaluable lessons that have served him well for his later career and life. The first is developing resilience; making him realise that whatever challenges he experiences, he will survive and come through the other side.

Jerich uses song lyrics from the late singer Aaliyah to illustrate this point – 'dust yourself off and try again.'

Working in a variety sectors and businesses also exposed him to wide range of experiences, which broadened his understanding of cybersecurity. "Each place I landed in was different from the others, and that diversity of experience really helped develop my skillsets," he highlights.

From 2010-2012, after receiving his BS degree, Jerich worked in security for a crucial US federal government agency – the National Nuclear Security Administration (NNSA). This was initially as an information system security officer, then as CISO and cyber security program manager for two NNSA contractors. In essence, he was charged with helping protect the nation's nuclear secrets.

Having a Consultation

By 2012 Jerich was ready to throw himself into a new challenge, entering the consultancy space for the first time. This was a move facilitated by his network, with a former colleague who worked at RSA suggesting that Jerich would be well suited to the security firm's professional services arm – advising and consulting organizations on their approaches to cybersecurity.

Jerich worked in this role for around three years before joining professional services giant Deloitte in 2015 as an advisory risk services manager, staying there until 2018.

He describes his move to the world of consultancy as "by far the single best decision that I made in my career." This was due to the opportunity to work on projects with a wide variety of organizations and people, exposing him to "the best of the best, the worst of the worst, and some even worse than that!"

He says his capabilities as a practitioner and a leader grew "10X" in those six years. "I worked on projects that still blow my mind, and the relationships I developed are why I am where I am today."

The highly professionalized environments that Jerich was exposed to in these roles was also a major learning curve. "There's a different level of professionalism and quality that quite frankly I never experienced, when working as a consultant," he comments. "As a bonus I learned the impact of a well put together slide deck and the power of story-telling."

While working at RSA, Jerich studied for his master's degree in Information Technology – Information Security and Assurance at Kaplan University, from 2012-2014. He says an advanced

degree was necessary to “open certain doors,” but in terms of the course material, it “was full of content that I was experiencing in my day-to-day life.”

The biggest lesson he took from this course was time management, as he had to juggle his studies between a full-time job and supporting his family. Jerich says: “What I learned in terms of juggling all of that has really carried me through to today.”

After leaving Deloitte, Jerich joined engineering company AECOM in 2018, initially as global director of information security strategy and governance, before becoming the firm’s deputy CISO.

For this role, Jerich again drew on his contact book, with the company’s CISO at the time a former client of Deloitte he worked with. “Another time my network led to a role,” he notes.

He credits this CISO as providing valuable guidance in how to be a security leader, most importantly not to be a “chicken little CISO” – in essence, not excessively communicating the risk around cyber-threats to the board and C-suite.

This is a trap that CISOs often fall into, says Jerich, due to the scale of cyber-threats being faced. However,

Epiq. Working for a large commercial bank in the highly regulated financial sector, his focus is “more narrow,” with the firm more “ahead of the curve” in cybersecurity compared to other sectors he’s worked in.

Nevertheless, the regulatory pressures and challenge of protecting a much larger organization brings with it different challenges, and Jerich says he’s “loving all of it.”

Using every new experience, including setbacks, as a learning opportunity, is a hallmark of Jerich’s approach to life. He credits the importance of working in a variety of roles and industries with providing him with the toolkit necessary to become a CISO at a large organization.

A Source of Inspiration

He advises cybersecurity professionals who aspire to become leaders to take a similar approach in their careers. In particular, working as a consultant develops the ‘soft skills’ that are so crucial to management.

This includes experience in handling budgets and developing influence among business leaders. “All of that happens when you’re a consultant

notes this wasn’t the case when he was growing up, where being an engineer, doctor, lawyer, athlete and actor were viewed as the only paths to financial stability.

“In cybersecurity, you can make as much money as many of these careers, and it involves a whole lot less school. But I don’t know that people understand that,” he comments.

Reflecting on whether he himself has experienced discrimination during his career because of his ethnicity, Jerich believes some employers have doubted his ability to handle certain roles, however, he cannot pinpoint whether this was due to his young age or race. In numerous cases, he was given the job he interviewed for but placed on a reduced wage and told to prove himself.

“I took multiple jobs where the people next to me were making significantly more money,” he says. “But I learned, grew and eventually could demand the same rate. I still don’t know if it was because of age or race – it’s one of them.”

Away from Cybersecurity

Given the demands of his work and activities in cybersecurity, Jerich has a number of hobbies and interests to help him unwind. He is a big sports fan, following all the LA teams. He also enjoys “unconventional” cooking, where “I find stuff to put together and see if it works. I’d say 70% of the time it doesn’t,” something that doesn’t always go down well with his wife, he admits jokingly.

Church and family are a hugely important part of Jerich’s life, keeping him grounded and reminding him of what’s really important. “Above all, I love hanging out with my family – I have a big one and can’t get away from them even if I wanted to,” he laughs.

The importance of family is further highlighted when Jerich describes the proudest moment of his life, which was telling his grandparents he had graduated from college – the first time someone in his family had done so. Jerich adds: “I can’t think of a prouder moment for everybody in my family.”

Jerich retains his sense of humility and perspective when looking to the future, explaining he learned “a long time ago not to be goal orientated but be growth orientated.” His ambition for the next 10 years sounds understated, yet nevertheless feels very powerful:

“I don’t have a specific goal for myself 10 years from now, other than to be 10 years better, 10 years wiser and have relationships that are 10 years stronger. I’m excited to see where that lands me.”

It is an approach to life that would serve us all well ●●●

“I unintentionally stumbled upon the power of networking and, more so than education, that really shaped my progress”

highlighting the threats too often and too dramatically will ultimately lead to the messages falling on deaf ears. “Therefore, I’m far more pragmatic with how I articulate risk as a result, which has helped my ability to build trust and influence to this day,” he notes.

Jerich was now ready to become a CISO at a large company, and he threw himself into the deep end at legal and business services firm Epiq in 2020. He became the organization’s first CISO and was appointed in the aftermath of a damaging ransomware attack. It was a daunting task, but nevertheless a rewarding and educational experience.

He recalls: “I had to teach the organization what the CISO is and how we can help the bottom line. I also had to rebuild the trust of customers.”

Jerich took his current post as CISO at Capital One in March 2022, describing the role as “very different” to that at

because you don’t know what type of project you’re getting thrown into,” he explains. “You develop an ability to work on your toes, learn quickly and sell yourself and your program.”

As a person of color working in a sector not renowned for its representation of minority groups, Jerich’s engagement with the cyber community has an extra sense of relevance. His story can hopefully inspire others from underrepresented communities to pursue a career in cybersecurity, and promoting diversity in all forms is a big passion of Jerich’s.

“Everything I do is in some way is meant to demonstrate representation – whether I bring in a diverse panel for a show or I interview a diverse set of people for a podcast,” he says.

Jerich is also keen to help “position cybersecurity as a viable career in underrepresented neighborhoods.” He

CYBERSECURITY INSURANCE: UNDERSTANDING A FAST-GROWING MARKET



Beth Maundrill speaks to experts to dispel some of the myths surrounding cybersecurity insurance and provide advice on how and why organizations should take out an insurance policy

As the cyber risk landscape evolves, so does the cybersecurity insurance market, and statistics suggest that the global market for cyber-insurance will more than double in size over the next few years, from \$9.2bn in 2021 to more than \$22bn in 2025.

However, this new insurance market is not without its challenges and has come under scrutiny from cybersecurity professionals. Taking a snapshot of the market today, insurance premiums are unstable, often increasing, and there are challenges relating to risk posture assessments. Additionally, the increase

in 2019 and 2020, which reached deep red levels far above 100%.”

Speaking to *Infosecurity* about the rise in premiums, Andreas Wuchner, field CISO, at Panaseer, says, “There is a growing need for organizations to find a more accurate way of assessing their security posture to make insurance more achievable and affordable; the narrow, often subjective questionnaires used by insurers today simply won’t cut it anymore.”

Rather than these tick-box questionnaires for security controls like multifactor authentication (MFA), Lawrence Perret-Hall, director,

The exclusions mentioned must cover losses arising from a war (where there is no separate war exclusion); exclude losses arising from cyber-attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state; be clear as to whether cover excludes computer systems that are located outside any state that is affected; set out a robust basis by which the parties agree on how any state backed cyber-attack will be attributed to one or more states; and ensure all key terms are clearly defined.

These exclusions once again highlighted the evolving nature of cyber insurance. While some were concerned about attribution of a cyber-attack, some experts highlighted how it continues to provide clarity over what policies should and should not include.

When asked if organizations should be worried about these types of clauses, Andrew Correll, Security Scorecard’s insurance solutions director says, “In short, no.”

He explains, “Insurance policies are merely contracts between two parties. Within that contract will lay out the provisions and circumstances under which each party is responsible for acting. It’s true that certain types of incidents, causes, etc., may be excluded under the policy. This is why it’s imperative for a business to work with a knowledgeable and reputable broker to obtain coverage that best suits their operations. That broker is responsible for reading and understanding the type of cyber insurance policy recommended to a buyer. I would also be remiss if I didn’t point out that the buyer should also read and understand their insurance policies, no different than any contract they enter into.”

Security Scorecard currently works closely with AXA insurance on cyber-related issues.

Meanwhile, Jason Rebholz, CISO at Corvus Insurance, explains to *Infosecurity*: “All types of insurance policies, including cyber policies, have exclusions to clarify where coverage does not exist. Cyber insurance is young, compared to most other types of insurance, and the market is evolving along with the threat landscape. Cyber policy coverage, including exclusions, is naturally changing as well. Recent policy language changes on attribution are designed to reflect modern day threats. The purpose of the new clauses is to give clarity to policyholders by updating legacy language that doesn’t reflect the reality of today’s cyber threats.”

Risk Management Strategies

Against a backdrop of an uncertain markets with fluctuating rates and

“Responding to a major cyber incident is not a solo sport”

in ransomware attacks globally is resulting in a high number of claims.

These challenges were laid out by a recent Panaseer report, the *2022 Cyber Insurance Market Trends Report*, which surveyed 400 global insurers, as well as CISOs and risk experts, to understand the state of the market today.

Panaseer found that 82% of cyber insurers expect premiums to grow over the next two years.

Risk advisor and insurance broker Marsh highlighted in its Q4 2022 research on the insurance landscape that there was “continued moderation” in cyber pricing, with the huge spikes of previous years levelling off somewhat. However, it still grew by 28% globally, compared to property insurance which grew just 7% and casualty insurance which grew just 3%.

Panaseer notes in its report that this is leading to a growing trend in “self-insuring,” where organizations are setting aside money to cover themselves should they suffer a breach. Indeed, some businesses are making the assumption that having the cash in the bank to respond to a cyber incident may be cheaper than skyrocketing insurance premiums.

Considering the pricing fluctuations, a recent report by Alta Signa said that the pricing extremes over the past two years can be put down to changes in the underlying risk assumptions as well as cyber insurance being an immature market.

Of cyber insurance in Europe, Alta Signa’s report says, “We hope that cyber penetration rates will continue to increase as the market matures, fueling demand for additional capacity, resulting in a sustainable equilibrium over the mid and long-term, and avoiding the kind of drastic rate softening which ultimately leads to the kinds of combined ratios seen in

CYFOR Secure, says insurers should look in more depth at the defense an organization has in place, alongside the results of regular vulnerability scans to get real-time and reliable data on their customer’s security posture.

“These scans will also enable organizations to understand where their weaknesses lie and look to remediate the most critical, likely uninsurable risks,” he notes.

The Lloyd’s of London Problem

One of the biggest issues to be discussed in cyber insurance today is the complexity of attribution. In 2022 the cyber insurance industry hit mainstream news when insurance behemoth Lloyds of London announced that as of March 31, 2023, it will exclude catastrophic state-backed attacks from its cyber insurance policies. This did not go down well against the heightened cyber-threat from Russian-backed actors since the start of the war in Ukraine. In a recent report, Google noted that Russia-backed cyber-attacks targeting Ukraine rose 250% compared to 2020 and those targeting NATO countries rose 300%.

The news was met with backlash and concerns that insurers could now be the party that decides what is and is not a nation-state backed attack, with catastrophic implications. It has also been noted by many that the line between nation-backed attacks and criminal gangs operating for financial gain only is particularly fine.

The market bulletin from Lloyds, titled *state backed cyber-attack exclusions*, is said to set out Lloyd’s requirements for state backed cyber-attack exclusions in standalone cyber-attack policies.

ongoing challenges relating to security assessments it is no surprise that many question whether cyber insurance is the right choice for their business. Despite this, many experts *Infosecurity* spoke to note that cybersecurity insurance is vital to a business' risk management strategy and offers much more than just a pay-out to cover expenses.

Rebholz comments, "Responding to a major cyber incident is not a solo sport. When a ransomware attack or business email compromise occurs, you need security experts and financial support to respond in the most effective manner possible.

"While the financial benefits of offsetting the impact of a cyber incident are obvious, cyber insurance provides much more than just recouping costs."

He notes that cyber insurance will cover the majority of security threats that every organization faces, including business email compromise and ransomware.

"For those organizations that do not have cyber insurance, many of these hacks can be an existential event due to the damage from the attack or financial losses," Rebholz says.

Guaranteeing all risks are insured is no mean feat and requires cooperation between business functions within the organization as well as between the organization and the insurer.

That includes avoiding certain risks, mitigating other risks with internal controls, and finally, transferring the remaining risks via instruments like insurance. However, it's important to note that "not all risk can be covered by insurance; some must remain with the company," Correll says.

"The goal of cyber insurance, from the perspective of the buyer, is to be there to pay a claim in a timely and efficient manner so you can get back to running

your business. That only happens with specialized providers," he notes.

Incentivizing Cybersecurity

There is also a case for cyber insurance having a positive impact on organizations' cybersecurity postures as the requirements by insurers for coverage mean that many customers have been required to step-up their efforts.

Of course, this does depend on the organization, according to Correll. He notes that organizations with relaxed security postures already will view insurance as a substitute for adequate cybersecurity measures. He suggests that some may assume insurance is there to pay if the company suffers an attack, and the extra expense on cyber hygiene, for instance, becomes unnecessary.

"This is clearly a negative impact cyber insurance can have," Correll tells *Infosecurity*. "Other organizations that already have a positive view of cyber hygiene will see insurance as a tool to better protect the organization's downside if a catastrophic event occurs. It's painfully clear that any and all defenses are not fool-proof. But they do have merit in slowing down attacks, mitigating

Rebholz adds that cyber insurance offerings from "insurtech" players are positively positioned to support an organization's security posture and have access to an "unmatched amount of data about cyber incidents." Ultimately this data can be analyzed to help better pinpoint effective security controls.

Who's in Charge?

CISOs and senior cybersecurity experts have been bombarded with information about cybersecurity insurance in recent years, but whose job is it to take out the policy and manage the risk?

Typically, the CFO or risk manager are the most common buyers of cyber insurance, but in SMEs it could be the business owner taking on the responsibility.

Wuchner notes that having the basics of cyber hygiene in place and understanding where your biggest risks lie are the start of your journey in taking out a cyber insurance policy.

This needs input from the CISO or security leader within your organization.

Panaseer's research shows that insurers want to see more evidence of a multi-layered defense posture to get the best understanding of their customers'

"Cyber insurance acts as a backstop for when the best laid plans and defense are compromised"

severity, and preparing an organization to face big attacks. Cyber insurance acts as a backstop for when the best laid plans and defense are compromised."

security postures and effectively assess cyber risk. This includes everything from security in the cloud and application security, to security awareness and patch management. Insurers expect enterprises to demonstrate cyber hygiene across the whole spectrum of cybersecurity controls.

With all these security requirements, CISOs will be able to accurately discuss with the insurance provider the current status of the organization's security posture and have the technical insights to help fill out the application as accurately as possible.

Rebholz notes, "They should work closely with the organization's broker to ensure all of the right technical information and risk mitigation strategies are transposed into the application."

The cyber insurance market is evolving rapidly, and we can expect more changes, like the Lloyd's decision, to occur in the future. Ultimately, we cannot shy away from the fact it will soon become a necessity for all businesses in the near future



How to Effectively Implement a Bug Bounty Program



Andre Bastert

Global Product Manager, Axis Communications

Andre Bastert is responsible for cybersecurity in the AXIS OS platform, the Linux-based operating system that powers Axis network products. His main tasks include vulnerability and lifecycle management and driving the security-related functionality roadmap of the AXIS OS. His career at Axis began in 2014 as a technical support engineer.

At Axis Communications, we believe cybersecurity should be a consideration throughout the entire software development lifecycle. That is why we recently partnered with crowdsourced cybersecurity specialists, Bugcrowd, to initiate a private bug bounty program as part of our continued efforts to effectively address cybersecurity in our products. This program forms part of the Axis Security Development Model (ASDM), which describes the security activities that should be considered during a product lifecycle's phases.

As an approved CVE Numbering Authority (CNA), we have been working with external security researchers and ethical hackers for a number of years. The bug bounty program represents the latest activity within ASDM, helping to provide peace of mind to partners and customers by guaranteeing the highest levels of cybersecurity for our products and solutions.

The Axis bug bounty program forms part of our wider cybersecurity focus as we are committed to being a responsible and trusted vendor. Through expert research, Axis will be able to take positive action to proactively identify, patch and disclose vulnerabilities in AXIS OS, the Linux-based operating system that drives Axis products. Regular meetings and coaching sessions

with Bugcrowd are hugely important in providing a wealth of knowledge and expertise, while at the same time allowing us access to a pool of dedicated security researchers.

Initiating the Bug Bounty Program

Researchers that were assigned to the bug bounty program were hand-picked through Bugcrowd's AI-based *CrowdMatch*™, based on interest areas, skills and experience which we have seen has resulted in strong levels of engagement.

One critically important element of the program is that Axis can steadily and methodically increase activities, following a crawl, walk, run model which has allowed the program to take shape and the partnership with Bugcrowd to grow at a manageable pace. This is something I'd strongly recommend to others considering where to start with such a program. We've been able to give the program a defined structure through implementation of Bugcrowd's triage system whereby the most important bugs can be focused on and immediately addressed. Researchers are guided using workflows and rewarded for their efforts, providing a clear pathway to success.

We have a transparent vulnerability management strategy at Axis and

the bug bounty program has become a key part of our layered approach to cybersecurity. Through working closely with Bugcrowd and its *Security Knowledge Platform*™, Axis is benefitting from cybersecurity expertise, engineered software-as-a-service (SaaS) and a global network of ethical hackers.

Other important elements that we have access to through the Bugcrowd platform include advanced penetration tests, vulnerability disclosure programs, attack surface management and other fully scalable options to uncover in-depth intelligence about potential areas of risk while providing comprehensive protection through an integrated, coordinated program of activity.

Bug bounty programs are relatively common in IT, but rare in the physical security industry where many businesses may not yet have fully made the leap into the world of device interoperability and data sharing over a network. Yet this world is growing and the plethora of new devices that come online each day presents a larger attack surface and greater potential for vulnerabilities.

We recommend the wider use of these kinds of programs across all industries. It enables key relationships to be built with external security researchers and ethical hackers, providing learnings that can help create a smarter, safer and more cyber-secure world 🌐

Crystal Hazen

Principal Program Manager at HackerOne

Crystal Hazen has worked for HackerOne for seven years. Crystal also works part time as a Community Event Lead for Security BSides San Francisco - a non-profit organization that hosts annual events that provide an open space for discussion and debate with InfoSec professionals.

A clear process to accept third-party reports about software vulnerabilities must be an integral part of an organization's cybersecurity strategy. A bug bounty program goes a step further by financially incentivizing third-party researchers and hackers to hunt for vulnerabilities that, if exploited, could have a significant impact on a business.

Before getting started, organizations must decide whether to self-manage the bug bounty program or work with a vendor. The benefits of working with a vendor are that they manage the payment processing element, as well as providing expert guidance and support for under-resourced security teams.

For organizations that are new to the concept, it is a good idea to start a private bug bounty with a small group of hackers to get initial processes in place before expanding. Setting up effective internal processes at this stage will allow businesses to optimize results down the road. During the first few months after the program launch, collect feedback from hackers and make any necessary adjustments before expanding hacker invitations.

Historically, while most organizations begin with a small

scope, with a few web-facing assets for instance, and expand as they become more experienced, it's a best practice to engage hackers upfront. There's an element of marketing to running a bug bounty program

"The average price for a critical bug is around \$4,186"

and the best time to capture hacker attention is during the first few interactions. What's most effective is to map out a view of assets prior to launching. The most mature organizations include their entire brand in scope because without visibility into what the attack surface is, how can organizations protect it?

Establishing a collaborative relationship with hackers is essential for a successful bug bounty program. HackerOne's 2022 *Hacker-Powered Security Report* found that nearly half (49%) of hackers would choose not to work on a program with poor communication. Get to know the hackers and treat them as an extension of the security team.

Remember that most hackers are naturally curious, so a great way to build trust is to include context in communications. Set expectations so hackers clearly understand the process and fix timelines.

Industry data can inform the baseline of what rewards businesses should set for vulnerabilities. The HackerOne report shows that the average price for a critical bug is around \$4,186. Organizations need to strike a balance that is high enough to get engagement, but not too high to the point of overspending. Don't start too low as this can be a missed opportunity to capture a hacker's attention.

One of a bug bounty program's scariest and most elegant features is its ability to adapt as the threat landscape evolves. When a company adopts a blameless security culture, bug bounty programs can help foster learning and collaboration within security teams.

Sean Poris

Senior Director, Cyber Resilience, Yahoo

Sean Poris leads Yahoo's Cyber Resilience unit for the Paranoids, providing security solutions to ensure the protection of Yahoo's critical consumer and company data and its one billion users. The team's mission is to deliver resilient products and infrastructure by envisioning, developing, and maintaining the processes, software, infrastructure, and tools needed to protect the enterprise and its brands.

Over the years, Bug Bounty has evolved from being on the fringe to becoming a mainstream element of many information security programs. The researcher community is stronger than ever, with seasoned testers investing more of their time and talents to teach new researchers how to conduct reconnaissance, understand the attack surface and identify areas of interest in a Bug Bounty program's scope.

This means there are more researchers now than ever before who can engage with a program. It also means the arrival on the scene of ever more Bug Bounty programs, ripe with enticing, untouched scope. How does a Bug Bounty program keep the community engaged, maintain high quality standards and continually elevate and adapt to the overall business strategy?

First and foremost, a Bug Bounty program needs to establish and maintain a sound delivery foundation and recognize the full breadth of the community with which it works. Vulnerability management, product security and infrastructure security baseline practices must remain healthy, and the Bug Bounty team must have a sound process model with up-to-date documentation. It is critical to invest in, measure and monitor the mechanics

of ingesting, triaging, routing and systematically resolving vulnerabilities that researchers provide to the organization via Bug Bounty. Second, the program must build robust engagement and communication plans with the three tiers of any Bug Bounty ecosystem:

- 1) The hacker community
- 2) The security community
- 3) The product and engineering community

Bug reports can get complicated, and back and forth comments on tickets sometimes can only go so far. It is crucial to invest in real time interactions to work through challenges and continue to feed the community with new content through blogs, newsletters or other updates. Keeping peers in security functions around the organization up-to-date on the Bug Bounty program will earn immense goodwill, and insights from it can feed tool and process updates for the security team.

Finally, ensuring the program engages key stakeholders outside of security such as legal, finance, public relations, marketing and engineering in governance/oversight and communications plans is crucial to maintain support. This oversight also allows for the voice of the business to

remain represented front and center of the Bug Bounty program, which can then evolve according to the direction of the business.

An effective Bug Bounty program is able to incorporate the findings from researchers into an ever-strengthening security posture. As products and infrastructure harden, the program needs to adapt to continue to be interesting for researchers while also aligning with the business. Key dials to turn include increasing scope, experimenting with new ideas to keep the program fresh and actively remaining on top of company product launches or key initiatives that it can plug into.

Budget permitting, live hacking events are a great way to bolster the Bug Bounty community, while providing a platform for research and opportunities for endless creativity. If budgets are tight, monthly or quarterly promotions can provide a way to focus research or try out new tactics that complement the company's overall security strategy.

Bug Bounty programs provide meaningful vulnerability insights from a global research community, but it is imperative to keep driving the program forward and aligning it with rapidly changing business climates and the stakeholder community to ensure continued success.



FEATURE

LOWERING THE PRICE OF ADMISSION



MAKING CYBERSECURITY AN EQUAL OPPORTUNITIES INDUSTRY

James Coker explores how socio-economic diversity can be of benefit to the cybersecurity industry and how the sector can open its doors to those with less economic means

Tales of rags to riches have long resonated with the public's imagination, tugging at emotional heartstrings and offering inspiration. Overcoming difficult life circumstances through a mix of perseverance, ingenuity and good fortune is a theme that has played a central role in the world of fiction, from Charles Dickens' literary classic *Oliver Twist* to the hit movie *Slumdog Millionaire*.

Lack of social mobility for socio-economically disadvantaged groups remains a major problem globally. For example, a staff survey published in December 2022 by KPMG found that social class is the biggest barrier to career progress in its organization, ahead of race and gender.

In cybersecurity, like many sectors, ethnicity and gender have – understandably – been the primary focus of diversity efforts in recent years. However, it is important that the age old issue of social class and socioeconomic circumstances are not neglected as efforts to improve diversity in the industry increase.

Barriers to the Economically Disadvantaged

In cybersecurity, a technical field renowned for expensive qualifications, the opportunities for disadvantaged socio-economic people are especially limited. The UK National Cyber Security Centre's (NCSC) 2021 *Decrypting Diversity* report highlighted this issue, finding that the high cost of gaining

So, how is a person from a poorer socio-economic background going to pay for the certifications to get into the industry?" asked Whiteside.

Phillimon Zongo, CEO at the Cyber Leadership Institute, is an inspiring story of someone who grew up in abject poverty in Zimbabwe and was able to reach the position of CISO at the age of 36 in Australia. Describing his journey to *Infosecurity*, Zongo reveals: "It took me more than six months of developing websites after work and during weekends to save money to pay for my CISA exam."

While Zongo's story shows that anyone can, in theory, thrive in cybersecurity regardless of circumstance, the barriers faced are undoubtedly still holding back many capable individuals.

Virginia Spitzer is executive director of One in Tech, an ISACA Foundation that works to remove barriers to equitable access to beginning and advancing careers within the cybersecurity and IT audit professions. She notes that in the US, many youngsters grow up in environments that makes entering the technology industry unrealistic.

"There's schools with very few STEM classes, sometimes they don't even get computers," she comments.

A 2021 study by BroadbandNow found that 42 million Americans do not have the ability to purchase broadband internet.

Spitzer also points out that many socio-economically disadvantaged teenagers are often forced to drop out of education at the earliest opportunity for economic reasons, such as working to

Review found that US workers from lower social-class origins are 32% less likely to become managers than people from higher origins, showing this is an issue across all sectors.

There are a variety of factors that explain this, according to Spitzer. These range from difficulties of studying for further qualifications to enable progression, to being overlooked by superiors because of the way they speak.

Benefits of Socio-Economic Diversity

Yet, great challenges also offer great opportunities. Improving access to the field to those from poorer backgrounds will undoubtedly benefit the cybersecurity industry. Most obviously, it would expand the talent pipeline to help fill the cyber skills gap, which (ISC)² estimated at 3.4 million workers in its 2022 *Cybersecurity Workforce Study*.

In addition, a more socio-economically diverse workforce can enhance cybersecurity teams' ability to tackle the growing volume and sophistication of cyber-threats. Clar Rosso, CEO of (ISC)² points out: "Multiple forms of diversity help us think differently about problems, like the attackers are doing."

Rosso also notes that addressing socio-economic barriers will naturally improve diversity in other areas too, with strong overlaps between poorer backgrounds and minority groups.

"I do believe that if you tackle socioeconomic diversity, you will also be tackling other kinds of diversity, such as ethnic and neurodiversity," she says.

Another consideration is that people who are socio-economically disadvantaged have particular characteristics that make them valuable to cybersecurity teams, where traits like resourcefulness and problem-solving are so critical.

"I've been in the field of youth and job development for 30 years now and one thing I always notice about socio-economically challenged people is that they are very resourceful," outlines Spitzer. "They are challenged every single day, whether it's how they are going to eat or how they are going to get to school. This means they are always solving their own problems and that's different from people who are well resourced."

Improving Accessibility to Qualifications

The case for more socioeconomic diversity in cybersecurity is powerful. However, one of the biggest challenges the industry faces when increasing opportunities for people from these

"All of us can rise past any obstacle as long as we believe and keep pushing"

cyber technical qualifications, including for entry-level roles, frequently acts as a barrier to socio-economic and ethnic diversity within the industry.

The frequent emphasis on expensive qualifications, even for junior roles, is an issue that Larry Whiteside Jr., CISO at RegScale and president of Cyversity, highlighted during the December 2022 episode of the IntoSecurity podcast. He pointed out that many organizations require a CISSP for an entry-level cybersecurity job, a qualification that requires a minimum of five years' experience.

This makes it difficult for anyone to get their foot on the ladder, but especially those from deprived socio-economic backgrounds. "There's so many certifications and they cost money.

support their family.

She argues that this reality acts as a barrier to many capable people starting a career in cybersecurity. "They may have, with training, excellent skillsets, but they've not got the opportunity so they're already excluded." Even when such individuals do get a foothold in the industry, there can be major barriers to progressing into senior positions. The NCSC's *Decrypting Diversity* report found that over a quarter (27%) of cyber professionals with a free school meals-eligible background felt inhibited at work.

"If they manage to enter the field, very rarely do they grow into management positions," says Spitzer.

Academic research published in 2021 by Paul Ingram on the Harvard Business

backgrounds, is the scale of technical skills that are required.

Encouragingly, the barrier of the cost of qualifications is being increasingly recognized by relevant industry bodies.

At (ISC)², a number of initiatives are taking place to make certifications more accessible to those from economically disadvantaged backgrounds. For example, Rosso says the body is focused on providing more opportunities for candidates in emerging economies in Africa and Asia. She notes that the body's tiered pricing scheme has led to "spikes in historically underrepresented nations" where a high proportion of people would otherwise struggle to pay the necessary fees.

"We try to price our products in a way that chimes with the capacity to pay," notes Rosso, adding that "if you can break down the economic barrier to entry into the profession then there is some serious interest out there."

In 2022, ISACA foundation One in Tech launched a scholarship program, which Spitzer says is "designed to provide tuition and support with fees for socio-economically challenged students."

Importantly, this is undertaken in collaboration with the cybersecurity industry, allowing the program to focus on developing skills that companies are looking for to fill their workforce. This increases the likelihood of disadvantaged people quickly finding jobs once they have completed training.

"It is building a model of how the industry can start building its pipelines earlier – not waiting until people are looking for jobs," explains Spitzer.

Pipelines also need to be developed for progression into management roles for these individuals, once they have entered the industry. These programs should focus on leadership and other softer skills that are "both inspirational and tactical," she adds.

Zongo is co-founder of the Cyber Leadership Institute, whose flagship course, the Cyber Leadership Program, provides equal access to professionals

from lower income backgrounds. This program equips professionals with "executive communication, confidence, strategy design, leadership and stakeholder management skills to land top roles and thrive in the c-suite," he says.

Making training and qualifications more specific to jobs is an important element of the remit of the UK Cyber Security Council, an independent body responsible for boosting professional standards and career prospects for those working in cybersecurity. It has begun work mapping out the different specialisms within cybersecurity, and the skills and qualifications required to reach them.

The Council's CEO, Professor Simon Hepburn, notes: "A key barrier for individuals attaining qualifications is the vast number of cyber qualifications out there, meaning individuals can spend a lot of time and money on courses that may not be relevant to the particular specialism they are looking to work in."

A New Approach to Recruitment

Another important approach to improving socioeconomic diversity is reducing the current emphasis on certifications in the industry, particularly at entry level. According to Whiteside, this requires organizations to revamp their hiring practices.

Speaking during *Infosecurity Magazine's* podcast, he argued that the original purpose of certifications has been lost. Rather than being a necessity for entry-level roles as is often currently the case, "they were meant to show that a person had an aptitude to be able to accomplish something. Now, there's so many certifications and they cost money. So, how is a person from a poorer socio-economic background going to pay for the certifications to get into the industry?"

Instead, he believes organizations should focus on hiring on the basis of soft skills and willingness to learn, particularly for entry-level roles. After all, cybersecurity is a fluid profession that requires continuous re-training and adaptation as technologies and attack techniques evolve in any case.

"It comes down to looking at the job descriptions and understanding what's important for the role – do you really need someone who has trained in every single toolset that you have in that team? Or, are you looking for someone with a curious mindset who you can put through some cognitive testing as part of the hiring process to show that they have an aptitude for what it is you can do, and then be willing to train them?" said Whiteside.

Hepburn also emphasizes the importance of promoting on-the-

job training, ensuring expensive qualifications like university degrees are not a pre-requisite to entering the sector.

"Traditional education routes such as university degrees are also not necessary to access the cyber industry and those unable to fund university should not miss out on the opportunity to enter the field. Soft skills and aptitude are highly valuable at entry level and apprenticeships and placements are effective, accessible ways to start out in cyber," he outlines.

Positive Role Models

The need for positive role models – highlighting people from similar backgrounds who achieve great things in sector – is also vital for improving socio-economic diversity in cybersecurity.

Zongo cites a lack of relatable role models as a "formidable" barrier to reaching the position he is in today.

"When I stepped into cybersecurity, there was no one who looked like me who was doing things I aspired to become across all Australia," he explains.

Therefore, after reaching the role of CISO at just 36, Zongo took it upon himself "to become the role model I never had." This included writing his memoir, *The Gift of Obstacles*, to share his journey and "encourage people from all walks of life to rise above their predetermined narratives."

Zongo is perhaps the ultimate example of overcoming difficult life circumstances to succeed, and his overarching message is one of hope. "My point is very simple – all of us can rise past any obstacle as long as we believe and keep pushing, even in the absence of distant rewards," he says.

Spitzer is similarly keen to push the message that despite the barriers, it is possible for people from disadvantaged socio-economic backgrounds to enjoy a successful career in cybersecurity. She emphasizes that more diversity in all forms is a *need*, not a luxury. "They should realise they're what other people are missing – they're a solution, not just begging to get into an industry that might help them."

Socio-economic diversity is an area that cybersecurity is struggling with. But it is an aspect of diversity that should not be neglected, especially as poverty heavily overlaps with other disadvantaged groups. Creating more opportunities to these individuals to enter and grow in the sector will ultimately both help reduce the cyber skills gap and enrich cybersecurity teams' ability to respond to an increasingly dangerous cyber-threat landscape.

It's true that anyone can succeed in cybersecurity regardless of background, but reducing socioeconomic barriers will make this prospect far more realistic for many people ●●● **END**



TOP TEN

Cybersecurity TV Shows



01

Mr Robot (2015-2019)

Coming in first place is the US drama series, *Mr Robot*, which follows a cybersecurity engineer and hacker called Elliot Alderson, played by Rami Malik. Elliot, a complex character who suffers with social anxiety, is recruited to a group of hackers by a by an insurrectionary anarchist known as 'Mr Robot'. The show spanned seven seasons and included 45 episodes.

IMDb rating: 8.6

03

Silicon Valley (2014-2019)

Parodying the Silicon Valley technology sector, this comedy series follows the fortunes of a startup company called Pied Piper as it attempts to make its mark. While not focused on cybersecurity per se, the series contains several themes around the issue, including a '51% attack' on the firm's app. The show ran a total of 53 episodes over six seasons.

IMDb rating: 8.5

02

Person of Interest (2011-2016)

In joint second is American sci-fi drama *Person of Interest*, which ran for five seasons and 103 episodes. The show focuses on billionaire programmer Harold Finch and his computer program 'the Machine'. The program is used by the federal government to predict terrorist attacks and their perpetrators before they happen by collating vast sources of data. Inevitably, moral questions are raised throughout the episodes.

IMDb rating: 8.5

04

The IT Crowd (2006-2013)

Another lighter take on the world of IT, the UK sitcom *The IT Crowd* ran for four seasons and 24 episodes with a special 'farewell' episode in December 2013. It focuses on an IT support team working in a dingy basement away from the rest of the organization. The program regularly featured themes around hacking and accessing personal data, emphasizing the vulnerability of sensitive data.

IMDb rating: 8.5



JAMES COKER

Top Ten: Cybersecurity TV Shows



The growing relevance of cyber-threats in society means this issue is becoming increasingly prominent in popular fiction. This includes cyber playing a central role in numerous

television series over recent years – to varying degrees of success, and indeed accuracy.

Cyber has proved to versatile across genres of TV – from tense action and drama to light-hearted comedies. Below, *Infosecurity* has listed its top 10 cybersecurity-related TV shows to date, with the rankings determined according to IMDb ratings at the time of writing.

Only those series where information security themes are prominent throughout the show have been selected.

05

Halt and Catch Fire (2014-2017)

This drama series provides a fictional insight into the personal computer revolution of 1980s and early days of the internet in the 1990s. *Halt and Catch Fire* refers to a machine code instruction that would cause the computer's central processing unit to stop working. The show often portrayed the early days of hacking and computer security fears, including the development of antivirus software. It ran for four series with 40 episodes.

IMDb rating: 8.4

06

Scorpion (2014-2018)

The US action-drama series *Scorpion* centers on a team of computer experts who tackle highly complex technology threats around the world. Throughout the show, the group are employed by the Department of Homeland Security and various private individuals and organizations to solve major tech problems. The show ran for four seasons featuring 93 episodes.

IMDb rating: 7.0

07

Unit 42 (2017-)

This Belgian TV series ran for two seasons, encompassing 20 episodes. The show focuses on a federal police unit that works to combat various cyber-threats linked to major crimes like murder and terrorism. A new inspector at the unit, Sam Leroy, collaborates with a former hacker called Billie Vebber to track down cyber-criminals who are terrorizing Belgium.

IMDb rating: 6.9

08

The Undeclared War (2022)

This thriller series from 2022 follows a team of analysts working at the UK's intelligence and security agency, GCHQ. In the six-episode series featuring actor Simon Pegg, the team of analysts work in secret to ward off a sophisticated cyber-attack against the UK's electoral system in the run up to the 2024 general election.

IMDb rating: 6.8

09

Intelligence (2014)

This American cyber-themed adventure series ran for just one season, containing 13 episodes. The plot centers around Gabriel Vaughn, a US government intelligence operative who has a super-computer microchip implanted in his brain in order to access any data centers and intelligence files in the globalized information grid. Many of the episodes are set around preventing disasters caused by hackers.

IMDb rating: 6.8

10

Intelligence (2020-2021)

Another cyber-related series named *Intelligence*, this UK comedy show revolves around a US National Security Agency (NSA) agent called Jerry Bernstein working with a UK government cybercrime unit. Bernstein, played by David Schwimmer, turns out to be a maverick operator which doesn't go down well with the unit's chief. The show has run for two seasons of six episodes.

IMDb rating: 6.2

01 All Ears When It Comes to Surveillance

Spyware and surveillance tech has been grabbing the headlines over the past few years. However, mobile security has improved significantly, making it much more difficult for malware to obtain the required permissions. Also, the latest Android and iOS versions are now imposing restrictions on third-party apps for recording calls using microphones.

What if there was no need to implant malware or a recording app in your phone to eavesdrop on your private conversations? A team of researchers from seven US universities have developed a method to spy on your phone calls using only two zero-permission features: your device's ear speaker and accelerometer.

The technique, called EarSpy, was described in an academic pre-print paper published on ArXiv in December 2022. It consists of analyzing tiny vibrations of smartphones' ear speakers – they used the OnePlus 7 and 9T models for their powerful ear speakers – to get information on the person's identity on the other end of the line and on the content of the conversation.

The researchers employed a set of tools, including Mobile Ear Speaker Earphone, a third-party Android app that redirects all the output audio through ear speakers with default volume, and Physics Toolbox Sensor Suite, another app that collects accelerometer data while audio is played. Then, they used a MATLAB program to extract relevant data from the phones' accelerometers – primarily time and frequency data. They also designed a convolutional neural network (CNN), a category of deep learning algorithms to analyze the data.

The EarSpy technique had a 98% accuracy in recognizing whether the target is male or female and a 56% accuracy for capturing numbers spoken in a phone call.

"[This] accuracy still exhibits five-times greater accuracy than a random guess, which implies that vibration due to the ear speaker induced a reasonable amount of distinguishable impact on accelerometer data," the researchers said.

SLACK SPACE

Grumbles / Groans / Gossip

02 Keeping Kids Data Safe

Educational data is a goldmine for organizations looking to have a competitive advantage and use it to customize the products they sell to schools.

In the latter case, however, legislation worldwide is increasingly restricting how schools should use their students' and staff data. For instance, in May 2022, the US Federal Trade Commission (FTC) banned education technology companies from using the personal information of children under 13 for any commercial purpose.

A staggering 96% of US schools from kindergarten to 12th grade share pupils' personal information with third parties, including advertisers, often without the knowledge or consent of users or schools, according to a report published by the non-profit Internet Safety Labs (ISL) in 2022.

Researchers looked at 13 schools in every US state, leading to 663 schools representing nearly half a million students. They found that most schools had more than 150 approved technologies for classrooms.

Also, 28% of services approved by schools for student use were not explicitly designed for educational purposes or with children in mind. Such apps included *The New York Times* app, Duolingo and Apple, Amazon, Meta and Google apps.

"We all know how much personal data is already flowing to companies that excel in monetizing it, but this research provides an accurate look at the reality of where student data is going. We hope [it] will highlight how urgent the problem is and further our efforts to create strong software product safety standards that lead to positive change and make internet-connected technology safe for everyone," Lisa LeVasseur, executive director of ISL, said in a statement.

03 The Spies Who Trolled Me

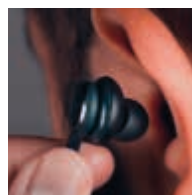
Here is a story that should convince you to stop using the same password twice. On December 19, 2022, two young men were charged by a US federal grand jury in Los Angeles with hacking into the Ring home security cameras of a dozen random people across the country in November 2020 and then "swatting" them.

According to the US Attorney's office in the Central District of California, James Thomas Andrew 'Aspertaine' McCarty and Kya Christian 'ChumLul' Nelson, respectively 20 and 21-years-old, first hacked Yahoo email accounts and then checked whether they were linked to Ring accounts. For those that were, the two men tried the passwords used for the Yahoo accounts and thus gained access to Ring home security door cameras.

The duo then "allegedly placed false emergency reports or telephone calls to local law enforcement in the areas where the victims lived [...] to elicit an emergency police response to the victim's residence [and] transmitted the audio and video from [the hacked Ring devices] on social media during the police response. They also allegedly verbally taunted responding police officers and victims through the Ring devices during several of the incidents," the indictment reads.

The US Attorney's Office also claims that McCarty continued his swatting spree in 2021 from his hometown of Kayenta, Arizona, where he called in bomb threats and hostage situations on more than 20 occasions. In addition, the Telegram and Discord aliases allegedly used by McCarty, including 'Aspertaine' and 'Couch,' correspond to an active identity in specific channels dedicated to SIM-swapping.

"If they were to be convicted of the conspiracy charge in the indictment, [McCarthy and Nelson] would face a statutory maximum penalty of five years in federal prison. The charge of intentionally accessing without authorization a computer carries a maximum possible sentence of five years, and the charge of aggravated identity theft carries a mandatory two-year consecutive sentence," concluded the indictment.



1. The phone
whisperer



2. Tinker, Tailor,
Advertiser, Spy



3. With Ring,
you're always
home... so are
the hackers

To share your thoughts with us please contact us at infosecurity.press@reedexpo.co.uk



Parting Shots...

James Coker, Deputy Editor

Each year brings with it new and previously unforeseen cybersecurity challenges. In 2020, the shift to hybrid working suddenly expanded the cyber-attack surface for organizations, who generally did not have the security infrastructure to defend their networks beyond the perimeter of the corporate offices.

The following year, 2021, was the year of ransomware, where attacks and extortion payments exploded in volume, often hitting critical services like hospitals and energy supplies.

The big theme of 2022 was the ongoing Russia-Ukraine conflict, in which cyber has been used to support military campaigns, a phenomenon referred to as 'hybrid warfare.'

Throughout these years one-off incidents occurred that rocked the world of cybersecurity to its core, and placed hundreds, and sometimes thousands, of organizations in a perilous position. These included the SolarWinds and Kaseya supply chain attacks in 2020 and 2021, respectively, the Log4j vulnerability that was uncovered towards the end of 2021, and the multiple LastPass breaches in 2022.

The challenge facing the cybersecurity industry is clearly enormous and cannot be solved by quick fixes. Encouragingly though, we are seeing a number of exciting initiatives across governments and industries that are designed to build a more secure world.

Join Our Online Summit

It is against this backdrop that we will be hosting the upcoming *Infosecurity Magazine* Online Summit, which is taking place on March 21 and 22, 2023.

New for this year, we will be tackling how to address the cyber skills gap with our 'Rookie Road' panel – here, industry newbies will join with senior professionals to discuss how to start and navigate a career in the industry,

and advise security leaders on how to encourage young people to enter the cyber job market.

The opening day will also see a session exploring the rise of cybercrime-as-a-service and highlight how the industry can work effectively with law enforcement to disrupt this model and bring perpetrators to justice.

The second day of the summit will have a strong emphasis on prevention, with a panel looking at how developers and security teams can work together better to build in security into technologies from the ground up.

We will also be hosting a lively head-to-head debate on the effectiveness of Software Bill of Materials (SBOM).

Recruitment and retention within the cybersecurity industry will also be addressed, with a panel discussion analyzing how organizations can evolve their hiring and management strategies to ensure security vacancies are not going unfilled and individuals are not leaving the cyber workforce.

Register for the event on the *Infosecurity Magazine* website to hear from leading experts on these topics and more, and earn CPE credits.

The Year Ahead

Given the erratic nature of the past few years, I am reluctant to make any bold predictions for 2023. However, there are several areas of cybersecurity that I expect to come increasingly into prominence as the year unfolds.

One of these is the debate about the future of open source security. While there are enormous benefits to open source software, from ease and cost to the ability to innovate, the growing discovery and exploitation of open source vulnerabilities is raising big questions about its security. We are now seeing governments and industry recognize the need to approach security differently in this area, while

maintaining the advantages of open source software.

I'm also hoping to see law enforcement continue to disrupt cybercrime and bring perpetrators to justice. Investigations into these types of crimes are notoriously difficult.

Nevertheless, the past year has seen the operations of numerous high profile cyber-criminal gangs curtailed thanks to coordinated law enforcement actions. This included the take down of the notorious 'Hive' ransomware group, enabling the capture of decryption keys, which were distributed to global victims of the group.

Another important area to monitor this year is how organizations adapt their approach to cybersecurity in the face of severe economic headwinds. The ongoing financially uncertain conditions are likely to place the budget available for security teams under scrutiny, particularly among SMEs.

It will be vital for organizations to prioritize basic cyber hygiene above procuring sophisticated tooling. Such an approach will necessitate ensuring all employees take more responsibility for their organizations' security, from good password practices to recognizing and reporting potential phishing emails. This brings staff awareness training even further into the spotlight, and organizations must work harder at making these sessions more engaging and impactful.

I am excited by the growing collaboration within the industry and also with governments to tackle the multitude of challenges at play.

As always, it has been a pleasure working on this edition, and I hope you enjoyed reading it.

Best wishes,

James Coker

Infosecurity Magazine **ONLINE SUMMIT**

21 - 22 MARCH 2023 / ON-DEMAND

8

Learn from the experts about the latest cybersecurity trends and topics, including:

- How to Maintain Strong Cybersecurity Against Economic Headwinds
- Rookie Road: How to Get into Cyber from Those at the Start of Their Careers
- The Evolution of Social Engineering
- Spotlight on How to Shape a Cybersecurity Aware Culture
- Debate: Can SBOM Deliver Practical Value or is it a Pipe Dream?



REGISTER NOW TO ACCESS INDUSTRY-LEADING EDUCATION SESSIONS, HEAR FROM INFORMATION SECURITY EXPERTS AND JOIN THE DISCUSSION ON THE LATEST CYBERSECURITY TRENDS.

**JOIN TODAY AND
EARN CPE CREDITS**

WWW.INFOSECURITY-MAGAZINE.COM/ONLINE-SUMMITS

