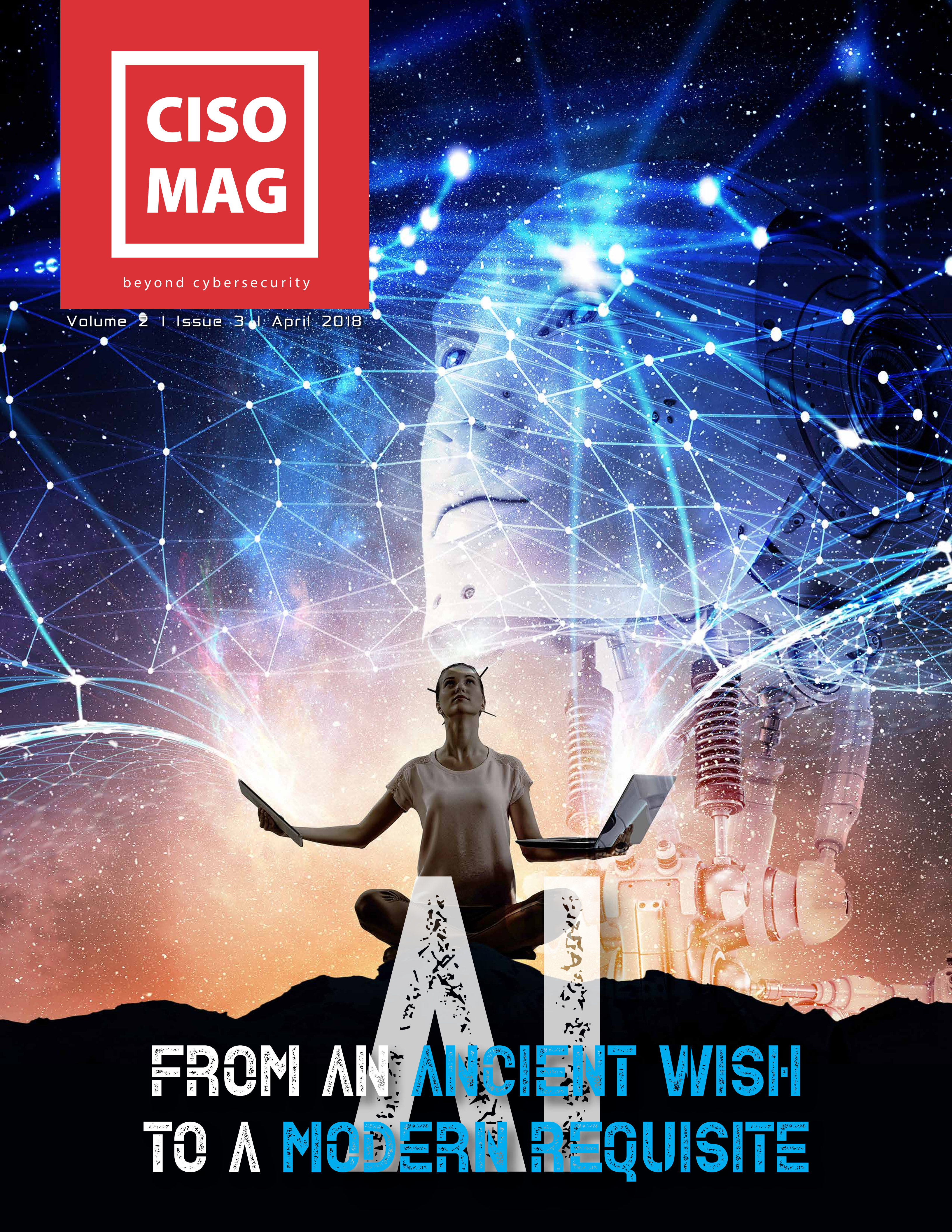
CISO MAG
beyond cybersecurity

Volume 2 | Issue 3 | April 2018



AI FROM AN ANCIENT WISH TO A MODERN REQUISITE

DTS SOLUTION
CYBER SECURITY REDEFINED

C Y B E R

S S O R R

CYBER STRATEGY · CYBER SECURE · CYBER OPERATIONS · CYBER RESPONSE · CYBER RESILIENCE

CYBER STRATEGY

CYBER RISK MANAGEMENT - SECURITY REGULATORY AND COMPLIANCE -
CYBER TRANSFORMATION - CYBER SECURITY STRATEGY - CYBER RISK MATURITY ASSESSMENT -
EXECUTIVE CYBER DASHBOARD - CYBER SECURITY METRICS -
EDUCATION, TRAINING & AWARENESS

CYBER SECURE

RED TEAM - OFFENSIVE - BLUE TEAM - DEFENSIVE - WHITE TEAM - ADVISORY
VULNERABILITY ASSESSMENT - PENETRATION TESTING - INFRASTRUCTURE PROTECTION -
NETWORK SECURITY PROTECTION - IDENTITY AND ACCESS MANAGEMENT -
DATA PROTECTION PROGRAM - CYBER SECURITY POLICIES IN OT/ ICS-
CYBER SECURITY OPERATIONS IN OT/ ICS - BLOCKCHAIN & FINTECH

CYBER OPERATIONS

CYBER SECURITY OPERATIONS CENTER - SECURITY OPERATIONS GOVERNANCE - OPERATING MANUALS-
SIEM 2.0 CONSULTING AND ENHANCEMENT - PURPLE TEAMING - THREAT MODELING METHODOLOGY -
MITRE ATT&CK MATRIX DETECT - THREAT ADVERSARY SIMULATION - HUNT - USE CASE DEVELOPMENT
CYBER THREAT INTELLIGENCE

CYBER RESPONSE

INCIDENT RESPONSE (IR) PROGRAM - IR GOVERNANCE & FRAMEWORK
POLICIES, PROCESSES AND PROCEDURES - TOOLS / TACTICS, TECHNIQUES AND PROCEDURES
INCIDENT RESPONSE PLAYBOOKS - MITRE ATT&CK MATRIX RESPONSE
THREAT ADVERSARY SIMULATION - HUNT - THREAT HUNTING METHODOLOGY
POST-COMPROMISE ASSESSMENT - DIGITAL FORENSICS

CYBER RESILIENCE

CYBER RESILIENCE ASSESSMENT - RED TEAMING - OFFENSIVE -
SIMULATED TARGETED CYBER ATTACK - PURPLE TEAMING — RESPONSE -
SIMULATED TARGETED CYBER RESPONSE - CYBER WAR-GAMING - TABLE TOP EXERCISES -
EXECUTIVE WORKSHOPS - MANAGEMENT WORKSHOPS - TECHNICAL WORKSHOPS

Is your business under threat from a Cyber Attack?

☎ 800 HACKED
+971 43383365
sales@dts-solution.com
www.dts-solution.com

DTS SOLUTION
CYBER SECURITY REDEFINED

Is your business under threat from a Cyber Attack?

☎ 800 HACKED
+971 43383365
sales@dts-solution.com
www.dts-solution.com

INDEX

EDITOR'S NOTE

Artificial Intelligence is writing the story of tomorrow. It is the future and it is here. As the world is embracing this paradigm change, we are exploring in our cover story how AI is transforming our world, while tracing its roots back to Ancient Greece, where the creation of an intelligent robot echos how AI is currently used in cybersecurity to safeguard enterprises.

In our Under the Spotlight section, we interview Jeff Carpenter, Vertical Market Director – Authentication of Crossmatch, who tells us how biometrics is playing a crucial role in cybersecurity in the future. He also talks about the renewed interest in biometrics and how behavioral and continuous authentication is the future of the space. In our Buzz section, we review how information security professionals are ill-equipped to handle the emerging threat landscape. Many companies are still using security paradigms from decades ago—paradigms that technology has made obsolete.

We also interview Jason Lim, Vice President, Cyber Security, Wiki Labs, who talks about challenges in privileged access management risk and identity access management. Move to our Insight, where we discuss DevOps becoming a standard approach for businesses, while highlighting the pros and cons of the customer-driven approach.

Tell us what you think of this issue. If you have any suggestions, comments, or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

CISO MAG
beyond cybersecurity

Volume 2 | Issue 3
April 2018

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Nishtha Pathak
nishtha.p@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Design Head and Visualizer
MSH Rabbani
rabbani@eccouncil.org

Designer
Jeevana Rao Jinaga
jeevana.j@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

Marketing Manager
Pooja Saga
pooja.saga@eccouncil.org

Sales Manager - India
Basant Das
basant.das@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora.

Volume 2 | Issue 3

Volume 2 | Issue 3

Bringing **knife** to a **gun fight**

Augustin Kurian

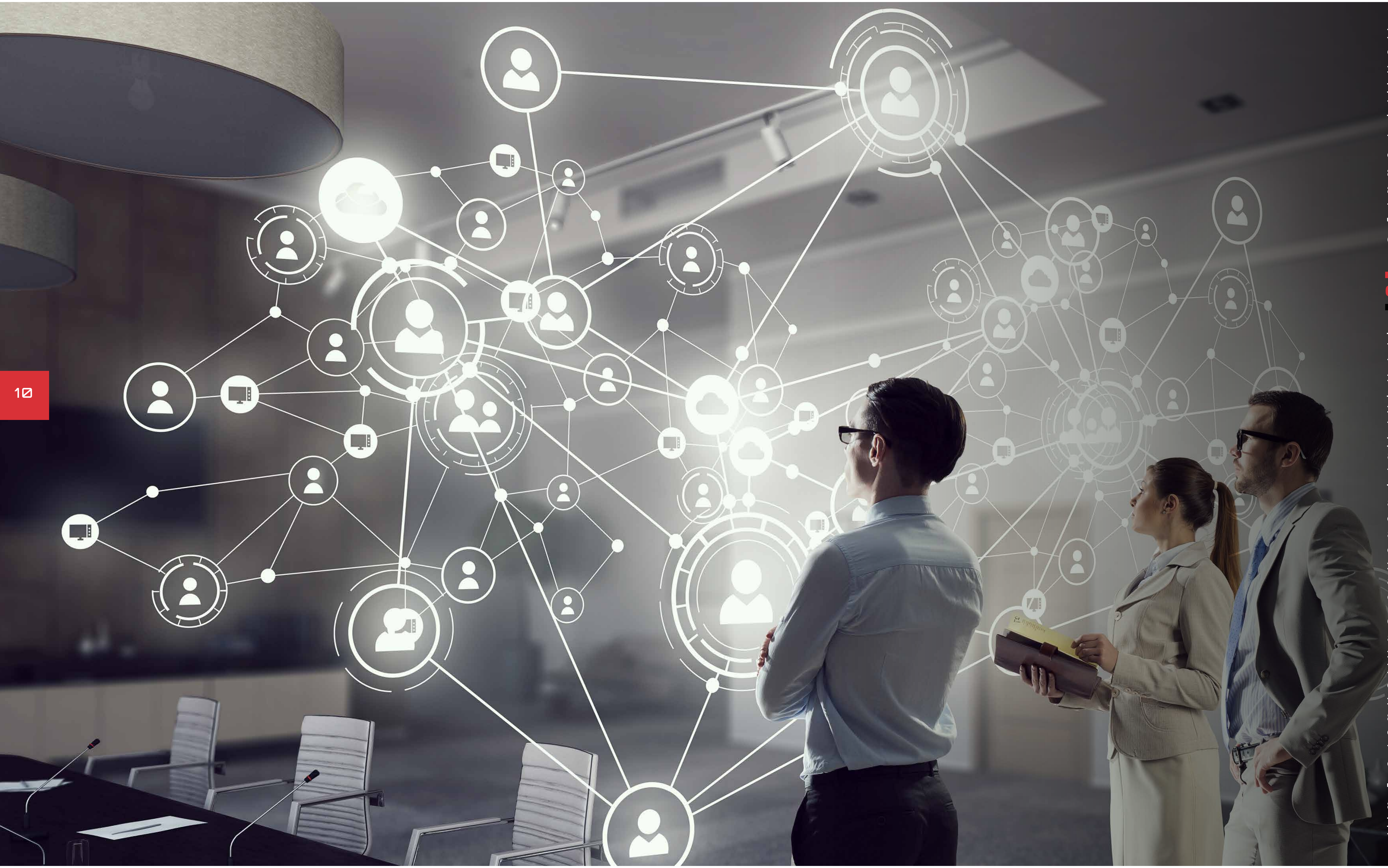
Relying entirely on knives, shovels, picks, and other melee weapons in the age of modern warfare obviously wouldn't make any sense. Now, that might seem like a rather cinematic metaphor for cybersecurity, but the plight of cybersecurity solutions and preparedness among so many of the world's largest enterprises isn't much different. It is still commonplace for organizations to resort to using prehistoric security tools to safeguard their companies—tools that are outdated and dangerously vulnerable. "I still see businesses using security approaches, technologies, and processes from decades ago," said Troy Hunt, Australian web security expert and creator of 'Have I Been Pwned', in a recent interview with *Computer Weekly*. "Many companies are still using security paradigms from decades ago, but the technology landscape is quite different now, with different risks, and so these paradigms no longer make sense."

A report commissioned by Cyber adAPT suggested that nearly one-third of security teams depend solely on outdated tools such as basic search and monitoring for their cybersecurity needs. The survey collated insights from over 6,000 senior IT professional including CISOs from around the world. "New generation technologies offer an exciting future for the cybersecurity industry. Many CISOs are struggling to persuade their boards to invest in new solutions, having failed to demonstrate the returns delivered by outdated tools – in fact, almost 60% of respondents thought they received poor value from their existing investments," Kirsten Bay, President and CEO of Cyber adAPT, stated in a release. "A platform approach, bolstered by AI and machine learning is set to offer real returns for cybersecurity customers. Technology will no longer rely on human input to detect threats and will prioritize alerts to streamline the CISOs workload, reducing the amount of time a threat is active inside a network."

Outdated software

The buck begins at the user end where software are not regularly updated becoming the biggest vulnerability vector. A 2017 research from Avast's PC Trends revealed that "over 52% of the most popular, critical and security-related applications, like Firefox, Flash or Java aren't being updated by users around the world." The research cited reasons like ignoring updates or updates not working properly, enabling attackers easy access as well as denying users the latest features, security patches, bug fixes, and compatibility. It stated that almost 56 million users across the world run an outdated version of Java Runtime Environment (6-8) which has earlier been linked to several critical security vulnerabilities.

"In the online world, your security habits, such as keeping your software updated, play a big role in the level of your protection on the internet. Running outdated programs leaves PC users susceptible to attacks from savvy hackers exploiting easy-to-find or



known vulnerabilities. The cause of people using outdated software may be that updates don't install properly or they postpone or forget to update even when prompted. We recommend people get into the habit of doing a regular status check on their PC, use an automatic software updater tool and make sure their AV is always kept up-to-date," said Ondrej Vlcek, Chief Technology Officer, GM, and EVP Consumer Business at Avast.

Outdated reporting structure

Another elephant in the boardroom that needs to be the addressed is the outdated reporting structure followed by several organizations. A survey by K logix revealed that more than half of CISOs report to the CIO or COO while only 15 percent report to the CEO. This is an archaic organization structure that exposes organizations to a whole host of potential problems and conflicts of interest. It is crucial that organizations have an experienced security expert on board who is given ministerial independence, which can be assured by reporting to the CEO directly – not the CIO.

CIOs have responsibilities aplenty—keeping up with innovations, managing the entire IT infrastructure, troubleshooting existing technology while planning for the next, etc. Management of security needs extra attention and care, and deploying an expert for the job is what will matter at the end of the day.

The CISO reporting to the CIO sets the company up for security problems because the agendas of the two positions can sometimes

be at odds with each other. A CIO may be pushing to innovate and stay ahead of the competition (in a technology company, for example) while the CISO may see major security concerns. With the CIO as the boss, there is no guarantee that the security concerns will be given proper priority. When egos clash, bad decisions are made.

Outdated data security policies

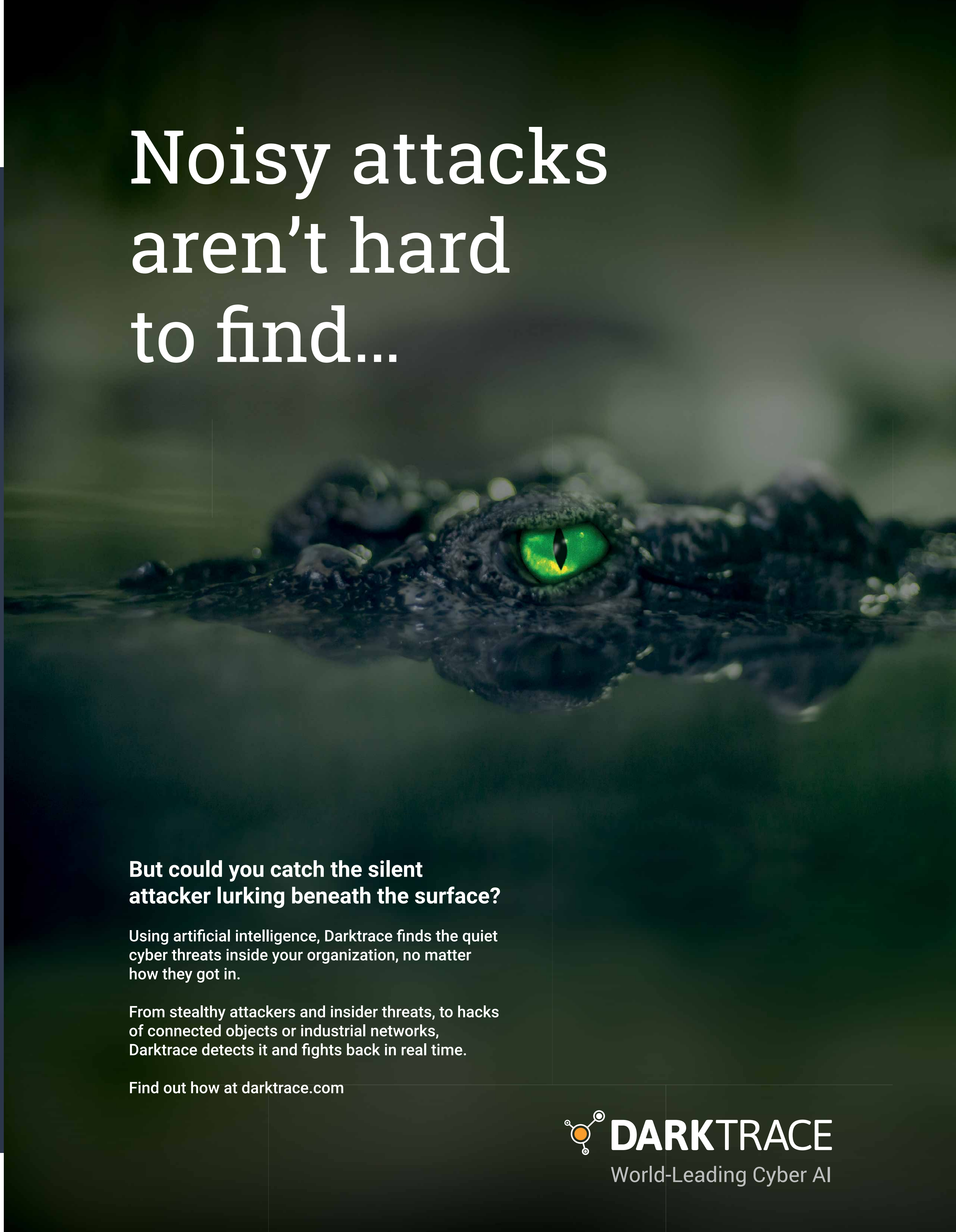
For many organizations, security isn't a routine part of business. It needn't be the foremost priority in order to be effective, but it certainly shouldn't be an afterthought. Making sure end users see security as part of the daily routine can go a long way toward assuring that the organization won't be cited for noncompliance. Part of daily security is identity management, as a lack of controls around identity may lead to unnecessary data access. Companies must also keep constant vigilance on the devices brought in by employees, as employee devices can lead to shadow IT.

Updating policies also means having constant threat assessment and penetration testing as part of the security program. As the old saying goes, a chain is only as strong as its weakest link. And lastly, make sure your organization is compliant with the cybersecurity standards in the nation the organization is based out of. Many of the companies involved in high-profile breaches in recent years were not compliant with even basic laws and regulations.

All is not lost

The Cyber adAPT report suggests that spending on cybersecurity has been increasing at a rate of nine to 12 percent each year. This testifies to the fact that awareness of the importance of security is showing signs of improvement. The report also suggested that nearly 69 percent of security teams are switching to a more evolved, analytical approach to defense like advanced security information and event management (SIEM), next-generation artificial intelligence (AI), machine learning, and network analytics. Andrew Kellett, Principal Analyst, Infrastructure Solutions at Ovum, comments: "With an evolving threat landscape, CISOs are battling to equip organizations to improve security and data protection. The lack of available resources within internal teams creates a vulnerability that technology must address. Prioritizing risk must be the focus to ensure effective returns on cybersecurity investment and safeguard network infrastructures."

Even though the threat landscape is evolving by the minute, defense continues to take a backseat in many organizations. The number of organizations that still consider VPN and legacy firewalls as the tent poles of cybersecurity is truly shocking, but there are signs of improvement.



4th Edition

CISO SUMMIT

EC-Council

07th - 08th June 2018
Mumbai | India

C|CISO Certified Chief Information Security Officer

TRAINING DATES
04th - 07th June 2018
Mumbai | India

PARTNERS / SPONSORS

Supporting State Partners

FINTECH VALLEY VIZAG

An Initiative by the Government of Andhra Pradesh

GOVERNMENT OF TELANGANA

Gold Partners

DARKTRACE

GROUP IB

Supporting Associations

ELECTRONIC SECURITY ASSOCIATION OF INDIA

CYBER SOCIETY OF INDIA

Mobility Partner

OLA

Education Partner

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Outdoor Partner

BRIGHT OUTDOOR MEDIA PVT. LTD.

Exclusive Media Partner

CISO MAG

KEY HIGHLIGHTS

Two Days	350+	50+	30+	25+	8+	4+
Power Packed Summit	C-Level Attendees	Expert Speakers	Solution Providers	Technical Addresses	Country Representations	State Pavilions

CONTACT

Alliances & Delegate Registrations
Meghana Vyas
meghana.vyas@eccouncil.org
+91-84240-61022

Speaking Opportunities
Jyoti Punjabi
jyoti.punjabi@eccouncil.org
+91-99636-54422

Sponsorship & Trainings
Renaldo Howell
renaldo.h@eccouncil.org
+91-79955-64887

AI : FROM AN ANCIENT WISH TO A MODERN REQUISITE

Augustin Kurian

“Myths, stories, and the Greek antiquities. Hephaestus, the Greek god of blacksmiths, metalworking, carpenters, artisans, sculptors, and metallurgy (the technology of day), was believed to have created Talos, a giant bronze warrior programmed to guard the island of Crete. From a modern perspective, Talos sounds like a futuristic cyborg with the ability to think and feel. According to the myth, Talos was Hephaestus's project that combined neurological-computer interfaces and living and nonliving components into one giant being. Was this mythology the first example of humans imaging the potential of intelligent robots and artificial intelligence (AI)?

Cut to the present and AI is all around us, and data and algorithms have become more important to our lives than we can fathom. And this is just the beginning.

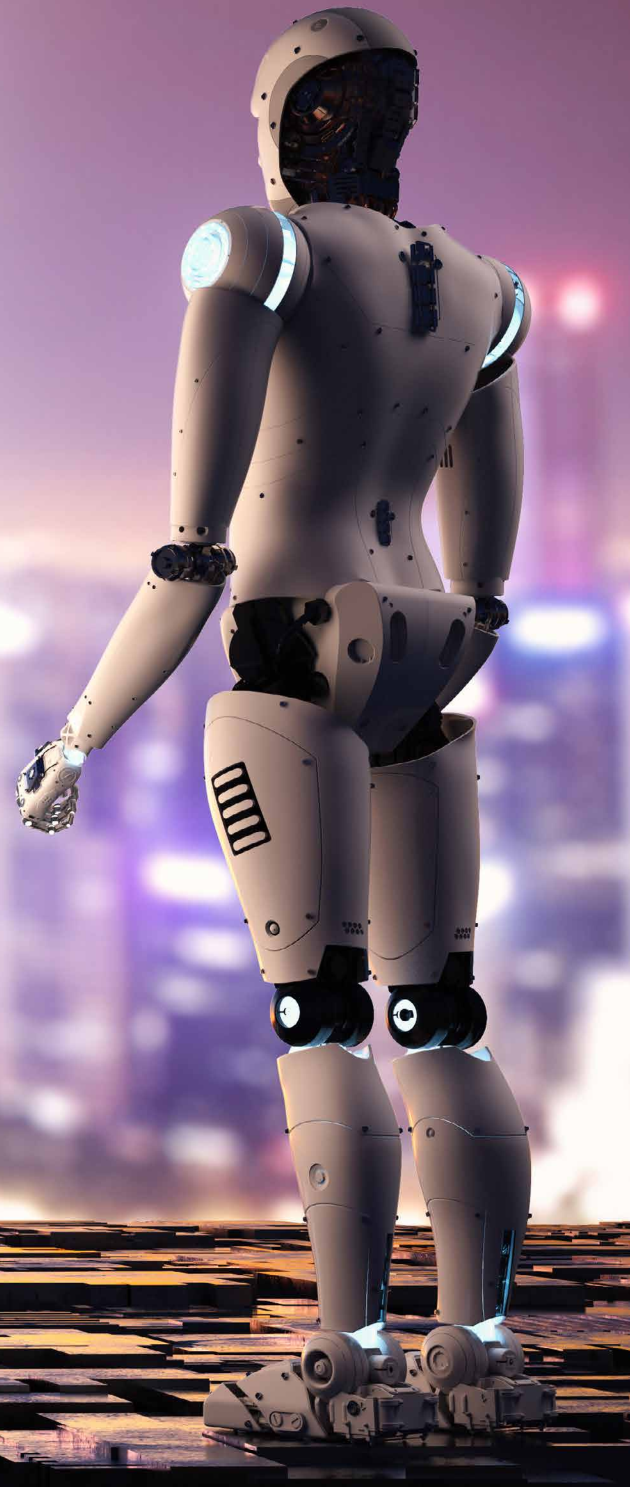
A Deloitte study has predicted that nearly nine in ten businesses will invest in AI by 2020. Among the respondents, most of the executives believed that AI would have the biggest impact on their organizations. The survey also highlighted that many organizations had started testing AI as more than three-quarters of respondents expect AI to disrupt their industries in the near future. “AI will have a profound impact on the future of work. Our view is that human and machine intelligence complement each other, and that AI should not simply be seen as a substitute. Humans working with AI will achieve better outcomes than AI alone,” said Paul Thompson from Deloitte, who was part of the survey.

“AI will have a profound impact on the future of work. Our view is that human and machine intelligence complement each other, and that AI should not simply be seen as a substitute. Humans working with AI will achieve better outcomes than AI alone”

The respondents also highlighted the need for investing in upgrading their cyber defenses and building bigger walls. Experts believe that one way to do this is to further inject the cutting-edge technology of AI into cybersecurity. Juliette Rizkallah, CMO of SailPoint, in one of her columns in *Forbes* points out that “Between the mountain of security data that IT teams must manage and the lack of visibility … now might be AI's time to shine. Cybersecurity could become one of the best AI applications that the business world has seen.” Machine learning is already being used to find anomalies and identify malicious behavior or malicious entities with some success. Cybersecurity programs are increasingly bringing AI-based products into their defenses. According to recent ESG research, “The future appears bright for cybersecurity technologies based upon machine learning as 12% of survey respondents say that their organization has deployed machine learning technologies for security analytics and operations extensively, while another 27% have deployed machine learning for security analytics and operations on a limited basis. Despite less than a third of respondents declaring themselves very knowledgeable about these technologies, the data indicates that organizations hope to use these nascent advances to improve the productivity, efficiency, and efficacy of their security analysts.”

AI is also becoming a key differentiator and requirement for major cloud providers. Nearly 62 percent of companies store sensitive data on public cloud platforms. Critical data assets are secured in third-party public clouds and vendors like Amazon Web Services (AWS), Google Cloud, Microsoft, et al are investing heavily in AI to secure their platforms. But security in cloud services is still at a nascent stage, and so is the understanding of AI among CISOs. “In the future, AI could be a cybersecurity game-changer, and CISOs should be open to this possibility. In the meantime, don't expect many organizations to throw the cybersecurity baby out with the AI bath water,” said Jon Oltsik, an ESG senior principal analyst, to *Tech Target*.

But there is a bigger concern: AI could be a very powerful tool for hackers. AI may make things easier for hackers and could create a new attack surface that they can exploit. Research by Webroot points out that more than 90% of cybersecurity



professionals are concerned that hackers will use AI to carry out sophisticated and harder-to-detect attacks against their companies. "The security cat-and-mouse game continues with AI. As soon as a security innovation comes to market, it is seized by bad actors and becomes part of their arsenal. The vast majority of cybersecurity professionals in both the U.S. and Japan are concerned that hackers will start using AI against them in cyberattacks," the report said.

"There is no doubt about AI being the future of security as the sheer volume of threats is becoming very difficult to track by humans alone," Hal Lonas, CTO of Webroot, said in a press release. "We stress to organizations the importance of a contextual view of threats that also incorporates visibility and data points from networks, endpoints, and human threat researchers to derive the most accurate cyber risk assessment. As the results reveal, AI is here to stay and it will have a large impact on security strategies moving forward."

But apprehension may deny better results. CISOs need to invest in tools and methodologies that enable their organizations to be more efficient and secure. Automation, orchestration, machine learning, and artificial intelligence can enable machines to take over the repetitive grunt work currently done by security personnel, allowing them to focus on anomalies or discrepancies, along with providing more time for critical decision making and strategic planning.

This is the opportunity, and it's not late. "There has never been a more tumultuous time in our industry. The lines between hackers, hobbyists, and nation state attackers are continuously blurred with security leaders having to scramble to defend against an ever-evolving slate of attacks. A CISO today has no idea if valuable data is being taken to make a national statement by someone with a vested interest, or purely for the market value. Because of this, one of the more interesting trends we've been seeing is the focus on the vulnerable insider or employee – as a potential root cause of any of the three scenarios above," shared Christy Wyatt, CEO of DTex Systems in a recent interview with *CISO MAG*. "As we move forward, however, and AI becomes a critical tool for both hackers as well as defenders, the "why" will matter increasingly less. The ability of each side to fulfil their mission will rely on visibility and the agility. The CISO needs to focus on lightweight, high-fidelity data collection to be able to identify and respond to new risks in real time – coupled with transparency and rapid learning. Analytics engines running in batch mode to cope with massive amount of heavy, unfiltered data, will not scale to meet the challenge."

Renowned author Pamela McCorduck in her book, 'Machines Who Think,' writes: "Artificial Intelligence began with an ancient wish to forge the Gods." Talos protected Europa in Crete from pirates and invaders and may well serve as a metaphor for the rest of the world.

An interview with JEFF CARPENTER

Vertical Market Director - Authentication

Crossmatch

Augustin Kurian

Jeff Carpenter is responsible for evangelizing Crossmatch's DigitalPersona® composite authentication solution. During his cybersecurity career spanning over a decade, Jeff has held positions with a number of top-tier cybersecurity and technology companies. Most recently, he was with RSA, a Dell Technologies company.

A frequent speaker and blogger, Jeff shares his thoughts on range of cyber topics, including the death of passwords, taking on challenging cybersecurity projects, and the future state of our digital world.

In an exclusive interview with CISO MAG, Jeff talks about the future of authentication and the importance of biometrics in ensuring a safer cyber space.

You have expertise in the authentication, can you briefly tell us about your journey, including your stint at the RSA?

I got into cybersecurity 10 years ago. I was really intrigued with the authentication and access management space. When I started working at RSA in 2007, I saw the challenges of the industry. This was in the mid-2000s when there was a belief that passwords were not going away and all you had to do was lengthen and strengthen these things and you would be all set. For more secure applications, you could deploy two-factor and a VPN. This, of course, was before we realized what was to come: the expanding threat landscape, IoT, holes being poked in the perimeter. At RSA, I was the product marketing lead for the RSA SecurID product that was best-known and most widely deployed authentication solution in the market at the time. Tens of thousands of individual customers use that product in businesses, organizations, nonprofits, and government entities. I was very gratified during my time there because I was able to really learn the authentication business and really understand the marketplace. While I was at RSA in 2011, we had the RSA breach and I was part of the team there that helped see RSA through that very difficult time.

But eventually, I saw the need to move beyond just token-based authentication to things that were more convenient and user-friendly, things like biometrics, behavioral and contextual factors that would be easier for users and potentially more secure.

Crossmatch is exploring the future of biometrics. Can you briefly tell us about how biometrics will play a crucial role in cybersecurity in the future?

Crossmatch's intellectual beginnings really happened in biometrics. We were founded in 1996 and our first products were biometric identity solutions, things like fingerprint scanners for border control, law enforcement, refugee management, and much more. It is an area where we now have a lot of intellectual capital today.

Our organization has a lot of domain expertise in this area. We believe the future of authentication will be almost free of passwords. I don't want to say that passwords are going to be completely obsolete – years from now, there will be some legacy applications that still rely on static passwords, but the world will move on. Passwords are just too easy to breach, phish, and guess. One way to help solve this problem is biometrics. Biometrics offer three things.

First, they offer raw, powerful security because there aren't many ways in which you can recreate someone's face, fingerprint, and iris and present it digitally in such a way that it will be accepted, especially when it is combined with other analytical factor. From a security point of view, all these

> "By 2020, 90 percent of businesses will be using biometrics in their identity scheme. So, the growth of this area is tremendous and we are fortunate to be right in the middle of this."

are still way more difficult than hacking passwords.

The second thing biometrics offer from the perspective of the user is convenience. Users love the ability to simply hold up their mobile device and do a selfie (face scan) or do a fingerprint scan, and get access to the applications they need. The field is also growing. We're figuring out how additional biometrics – such as how a user holds their mobile device – can be used to add additional identity confirmation that the user is legitimate.

And the third thing biometrics offer is something we call "proof of presence." In an advanced authentication system, you should be considering a lot of different factors. And one of those is, not only did the user swipe their finger but that they did it in the timeframe you asked for and that they did if from a known device that was bound to that user. And that is proof of presence. We know that the user has provided that biometric within the timeframe that we asked on a device that was bound to them, either a laptop with a fingerprint reader, a mobile device with a facial camera, PC with a high definition camera to scan an iris. It's a powerful combination that fraudsters would have a hard time spoofing.

By 2020, 90 percent of businesses will be using biometrics in their identity scheme. So, the growth of this area is tremendous and we are fortunate to be right in the middle of this.

Rank the best to worst when it comes to vectors of biometrics.

In cybersecurity, the answer in a lot of questions is: it depends. One of the things I mentor younger cybersecurity people in our organization is not to use absolutes, in other words, say things like that system can "never" be broken or this is the "safest" thing. We are a cautious bunch, us cybersecurity professionals. Well, it's generally understood that most fingerprint technologies are considered very strong. The minutia or electromagnetic image that can be derived from an individual's finger is very complex. Generally, most fingerprinting systems will settle on a certain amount of acceptable minutiae that makes for a nice level of security without having the user re-swipe again and again. In other words, biometrics system is all about making sure you have what's called a false acceptance rate (FAR) and a false rejection rate (FRR), and that you match those to a level where users aren't required to re-swipe their finger too many times.

Then come face and iris. These tend to be a little stronger for a couple reasons. The first is that you can get more data points from a face, especially with the new generation of high definition (HD) cameras. In facial and iris scan, the camera can go out to grab almost an infinite number of data points. Also, there's this concept of liveness, with the face you can actually require a user to do a second or more of movement such as move their mouth, maybe jaw, blink their eyes so the software can confirm it's an actual user and not a face reproduction. There are technologies out there that introduce a pixel somewhere on the screen that the user's eyes almost involuntarily move to the where the pixel is presented, thereby giving the software algorithm a confirmation of liveness. Pretty cool stuff out there, all in the service of trying to prevent these replay attacks where fraudster attempt to reproduce a user's biometric.

Crossmatch was recently awarded for going above and beyond for guard and reserve employees, which brings us to the question of insider threats. For most organizations, employees are the biggest vectors of insider threats. What is Crossmatch doing differently in this sphere?

We're very gratified to be awarded by the US Department of Defense for something called employer support for the Guard and Reserves (ESGR). The service members have a lot going on. They have to manage their work stress and family life and their current or impending deployments The last thing they need is to know their accounts are compromised and their benefits delayed because of this. So, across the various services, we allow service members to get access to the benefits that they need and they deserve, wherever they are in the world. The processes for getting their paycheck and benefits are the same irrespective of their location. Bottom line: it is making it easier for the service members and harder for the hackers.

As far as the insider threats are concerned, it is as big as the outside threat of being attacked or compromised from the dark web. It is very easy for somebody with your password to go over to your PC and compromise your documents. To counter that, we are also pioneering risk-based authentication technology that relies on things like proximity, behavior, biometrics, and more

For example, you may have your mobile device and it has Bluetooth or near field communication (NFC) enabled. When you get your device close to your PC that's one more assurance that it is you who is working on your PC. Now let's say you get up and you go to lunch and you take your phone with you. As soon as you move away from your PC, your PC locks down. If somebody else, a malicious insider, happens to have your password and tries to unlock your PC, our authentication system knows it is not you and the appropriate action can be taken (not allow access, alert the user and management of potential fraud).

In India, the government has embarked on a unique identity scheme with Aadhaar. Aadhaar relies heavily on biometrics, but is still looked down by many due to its security vulnerability. Where is government going wrong in this space, and how can it change for better?

Aadhaar is really a pioneering program that seeks to reach out to 400 million people who have previously never been part of the digital economy. A lot of these people were born in remote villages of India and don't even have basic documentation necessary to setup an online account, like a birth certificate. Biometrics creates a unique identifier for those individuals and allows them to get government and financial services that they've never had before.

Users can enroll for a driver's license, register to vote, open a bank account, and receive essential government benefits.. So, it pulls those 400 million people into the modern era that can help propel the Indian economy to the next level. There are a lot of detractors on the Aadhaar program and it has become very political. What I believe is that the benefits of this program over time to the Indian economy and the world economy will outweigh the fear, uncertainty and doubt the is currently being cast on the program.

Pharma industry is now becoming one of the biggest targets for hackers. How can biometrics be incorporated to spruce up cybersecurity in the pharma segment?

The pharmaceutical companies now more than ever need to protect their intellectual property that includes research, patents, and formulations of drugs that they have to share with authorized people across the globe. Our solutions enable them to confidently expose their most sensitive information to researchers and analysts using very strong authentication that involves biometric identity. So, finger swipe plus a password plus knowing where that user is in the world plus knowing their device, all these risk-based authentication factors give the organization confidence that they can share the information and keep it safe.

In the United States, we have an ongoing opioid epidemic. The U.S. government has created a regulation through the Drug Enforcement Administration(DEA) called ePrescribe. This scheme requires doctors who are prescribing certain levels of medications that they must digitally sign off on the transaction. This prevents forgeries from patients or even other health care professionals. We're pitching biometrics as a potential solution. A biometric solution provides a good convenience for the doctors because one of the things we know about health care professionals is that they are very busy and stressed out. They don't want a lot of additional security hurdles thrown in front of them. Doctors, in particular, don't want to be told, "Oh you have to adhere to

these security steps. Pull out your mobile device do this you know, go here do that plus a Smart Card, maybe a token." They just want to go to their terminals, swipe a finger, and enter their password or PIN. Done. So, biometrics provides convenience for the doctor, security for the organization and that proof of presence because a digital signature provides a type of non-repudiation that organization and health care professionals need to insure that unauthorized transactions aren't going out in their name.

Global Healthcare biometrics market is expected to reach $ 5.6 billion by 2022 from $ 1.34 billion in 2015. The market is growing at a CAGR of 22.1%. On the other hand, some security and privacy-related issues and prices are some of the factors that can hamper the growth of the healthcare biometrics market. Do you think healthcare organizations are still resorting to outdated solutions?

Yeah, I think so. It depends on the country. There are various healthcare regulations in Europe and the U.S. We are slowly getting multifactor identity management systems but we need to move toward risk-based authentication. Let me give you a kind of a before and after scenario. Currently, the applications, systems and networks that healthcare professionals log into are simply binary. You provide a correct password and you're into the system. What we are championing is more of a risk-based approach that looks at anywhere from 30 to 70 different factors about the user that can be used to calculate if that user should get access or not, or if they need to undergo another authentication method. And we always say at Crossmatch that the goal here is to actually have the users authenticate or log on to their applications less. You need to have less visible security to the end user and we're able to do that through risk-based authentication.

What are Crossmatch's views on the future of identity authentication and verification?

We talked about authentication being biometric-based but there is another interesting component of it called behavioral. There are behavioral technologies and they're actually very real. At Crossmatch, we have a behavioral keystroke.

It works like this: as you're typing your password, the software can look at how you're typing a password, your lift, your movement across the keyboard, your stroke, your press. With this keystroke behavioral biometric, we are able to distinguish between one user and another. To a casual observer watching two users type in the same password, the differences are almost impossible to detect; but to a computer algorithm, the difference between the two users is completely distinguishable. We can again feed that into the risk engine and that becomes one more factor that will determine whether that user should get the access or not.

Behaviral biometrics, like keystroke, will enable continuous authentication. This is the true future state of authentication. Today,ou go to get online with your application or your network or do a transaction. You're asked to authenticate only once at the beginning of your session. Now what we do know that the bad guys can have malware that not only steals your password but waits for you to enter that password and then can perform a session hijack. For example, when you log on to your account with your username and password, a black screen appears saying the site is down for maintenance. But it is actually the malware that is presenting the screen to the user. Behind the scenes, your session is open and the bad guys are draining your account. So continuous authentication using things like keystroke biometrics allows us to do more or less continuous authentication of that user throughout the day as they're typing into certain fields. That is really the next iteration we see coming down the pipe.

The other factors that we're seeing in the industry are things like how you hold your cell phones. The gyroscopic sensors inside of your mobile device create a unique biometric with how you hold that phone. Mouse movements are another biometric: how you move your mouse, for example, to wake up your PC when it goes to sleep, is very unique to you. Machine learning can pick up the differences. Innovations like this are very exciting in the future and have the potential to provide even more convenience for users and more security for organizations.

‘DevSecOps’ Mitigates Cybersecurity Risk from Digital Transformation

Jason Bloomberg
President, Intellyx

Achieving customer value with any digital transformation initiative requires an organizational and cultural shift across the enterprise to align people’s efforts with customer priorities.

We see such cultural change in software development shops in particular, as DevOps becomes the standard approach to delivering quality software at the velocity the business requires.

There is a dark underbelly to digital transformation-driven customer value, however: *cybersecurity risk*. The more technology-centric our organizations become and the faster they go, the greater the chance that a hacker will find that one vulnerability that will suck away all that hard-earned customer value.

The downside of cybersecurity risk certainly garners more headlines than the upside of digital efforts to be sure – and an increasing number of executives are realizing that they must address both together.

The inevitable conclusion: how organizations deal with cybersecurity risk must also transform. They cannot simply keep dealing with such risks as they have in the past.

The Transformation of Cybersecurity

Just as digital transformation requires breaking down organizational silos, so too with cybersecurity. “Security needs to be part of everyone’s job,” explains Fraser Scott, Cloud Security & DevSecOps at Capital One. “Security being a constant blocker just won’t scale. Either that or you end up with shadow IT.”

Traditional IT shops relegate ‘information security,’ or InfoSec, to a separate department. Developers must then run their code by InfoSec for approval. This state of affairs slows application development (‘appdev’) down and creates an adversarial relationship between the appdev and InfoSec teams.

From the perspective of modern appdev, such blocking both impacts customer value and also doesn’t serve the goals of cybersecurity. “The problem for the security person who is used to turning around security reviews in a month or two weeks is they’re just being shoved out of the game,” says Gene Kim, DevOps thought leader and coauthor of The Phoenix Project. “There’s no way with how InfoSec is currently configured that they can keep up with that. So, InfoSec gets all the complaints about being marginalized and getting in the way of doing what needs to be done.”

Large enterprises are clearly understanding this transformation within the cybersecurity ranks. “In order for InfoSec and agile to be effective in an organization, you can’t have it locked up with a few people or a few departments that are narrowly looking at their portfolio of work,” says Julie Tsai, director of engineering in

> There’s no way with how InfoSec is currently configured that they can keep up with that. So, InfoSec gets all the complaints about being marginalized and getting in the way of doing what needs to be done.

information security at Walmart Global eCommerce.

The Rise of 'DevSecOps'

If breaking down the siloed InfoSec team and spreading the responsibility for security across the organization sounds familiar, you'd be right – it's an extension of DevOps, the cultural and organizational shift that has been dissolving the boundaries between appdev and operations for several years now.

The result is 'DevSecOps' (or 'SecDevOps' or even 'DevOpsSec,' depending on whom you ask). "Because developers drive the software agenda, their participation is crucial for achieving a more secure framework," explains a white paper from security vendor Veracode, acquired by CA Technologies earlier this year. "Yet simply acknowledging this fact won't get the job done. As a developer, you need to position yourself at the center of an application security strategy, and DevSecOps represents the natural evolution of the concept."

In other words, DevSecOps doesn't simply amount to dropping a security person onto a DevOps team, a mistake many organizations have made. "The security teams, however, face the biggest adjustment," the white paper continues. "Security people need to abandon the mindset of check-box compliance, or else get left behind as DevOps takes off."

Capital One's Scott emphasizes this point. "DevOps doesn't mean one unicorn engineer doing all the things. It means breaking down the traditional silos," Scott explains. "You might end up with a single functional team that has a mixture of software engineers, QA, and security. Or maybe separate teams working together. The trick is getting the right people involved earlier on."

Zane Lackey, who built the cybersecurity effort at Etsy, ties the InfoSec team's role closely to DevOps. "Its role shifts from being this blocker or gatekeeper to actually thinking about, how do I enable the rest of the business to move faster—whether that's the development team, whether that's the DevOps teams—whatever side of the business they're interfacing with, the real shift becomes, how do we enable them to move faster?" Zane Lackey is currently the Co-Founder/CSO at Signal Sciences.

The Role of Tooling in DevSecOps

While DevOps is more of a culture change than a technology effort, it unquestionably depends upon better automation tooling – and so too with DevSecOps. "Automation has a big part to play here because it removes the typical human barriers that introduce slowness and latency," Scott explains. "Instead of emailing some team a document containing changes to review, a git commit could trigger automated tests that effectively carry out the decision-making process the person would have made."

Joshua Corman, Chief Security Officer, SVP at PTC emphasizes this point. "DevOps involves processes and tool chains, but I think the defining attribute is culture, specifically empathy," Corman says. "If you show DevOps teams how security can make them better, then as a reciprocation they tend to ask, 'Well, are there any choices we make that would make your life easier?'"

Security vendors also see the importance of tooling to DevSecOps, even though it takes a supporting role to the necessary organizational transformation. "We're baking DevSecOps into the entire software development process," says Otto Berkes, EVP and CTO of CA Technologies. "We need an understanding that customers are going through a culture change. We can't dump tools like Veracode into an organization and expect good use."

Berkes' boss, CA CEO Mike Gregoire, echoes this sentiment with advice for management. "Mandating DevSecOps is a fool's errand," Gregoire says. "You have to provide tools and training."

Lackey adds some words of warning. "A lot of the security tools or vendors … have caused us more problems than they've actually solved, and so you see developers or DevOps folks … wince when they hear a new security tool coming or something because they've had negative experiences in the past," Lackey warns. "When I think about … enabling those teams with security resources directly, it's about plugging into what they're already doing, and really thinking about security as a piece of the DevOps tool chain that folks are already thinking about."

Better tooling and automation are thus important enablers of DevSecOps, but more important is including security considerations in the DevOps effort broadly – and by extension, across the digitally transformed organization as a whole.

For such organizations, the central principle must be that security is everyone's responsibility. Given the fact that most of today's cyberattacks begin with phishing schemes that can target anyone in an organization, this principle is already of primary importance. DevSecOps is one way of making such a principle a reality across the software development efforts essential for any digital enterprise.

Copyright © Intellyx LLC. Intellyx publishes the Agile Digital Transformation Roadmap poster, advises companies on their digital transformation initiatives, and helps vendors communicate their agility stories. As of the time of writing, CA Technologies is an Intellyx customer. None of the other organizations mentioned in this article are Intellyx customers. CA Technologies covered Jason Bloomberg's expenses at CA World, a standard industry practice.

The opinions expressed within this article are the personal opinions of the author. The facts and opinions appearing in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.!

INFOSEC PARTNERSHIPS

In an age where cyber threats are increasingly frequent and the information security business landscape is evolving, it is imperative for CISOs to take a strategic leadership role and adopt a collaborative and inclusive approach. An acquisition or a collaboration can serve several purposes for organizations, from propelling them into new markets, to strengthening their critical IT infrastructure, to sharing information for turning knowledge into action. These partnerships can be difficult, challenging, or chaotic events, but can represent a positive change for a business. In this segment, we take a look at some notable collaborations and acquisitions in the cybersecurity domain.

CISO MAG Staff

NH-ISAC and Anomali partner for improving healthcare information sharing

The National Health Information Sharing and Analysis Center (NH-ISAC) partnered with threat intelligence platform Anomali to raise the security standards for data sharing processes in the healthcare industry. NH-ISAC is a global healthcare community for collaborating and spreading best practices. The council helps its members in the application of physical and cyber threat intelligence to adopt threat mitigation practices. Members of NH-ISAC include hospitals, healthcare insurance payers, pharmaceutical and biotech manufacturers, medical device manufacturers, laboratories and diagnostic centers, ambulatory providers, and more.

Anomali provides inputs to organizations, cautioning them against cyber actors and other distrustful activities on their networks through internal security monitoring programs. Anomali will be providing the infrastructure and tools to NH-ISAC and their partnership is expected to strengthen cybersecurity in the healthcare domain. The CEO of Anomali, Hugh Njemanze, commented on the partnership, "One organization's threat detection is the next organization's prevention. We are pleased to support the NH-ISAC mission to secure the nation's critical healthcare infrastructure, and help members better share intelligence and respond to threats."

Palo Alto Networks acquires Cloud Security Platform Evident.io

Palo Alto Networks announced the takeover of cloud security platform Evident.io. The deal, worth $300 million, will be completed during Palo Alto Networks' third fiscal quarter. Founded in 2013, Evident.io is a privately held firm backed by Google Venture, Bain Capital Ventures, True Ventures, and Venrock. Their Evident Security Platform (EVP) scans customers' public cloud footprint identifying and analyzing risks in the system and aiding security staff with remediation guidance.

Tim Prendergast, co-founder and CEO of Evident.io, commented on the acquisition, "We founded Evident.io to secure our customers' public cloud infrastructure and services without slowing down innovation. The combined capabilities of Evident.io and Palo Alto Networks will provide customers the confidence they need to run better, faster, and more securely in the cloud."

A new cloud security study conducted by Palo Alto Networks highlighted that around 70% of cybersecurity experts, especially those working in large organizations across Europe and the Middle East, agree that hastily shifting to the cloud environment also means ignoring some security risks. The next gen security company announced in its press release that in order to ensure a complete and secure move into a public cloud, security, DevOps, and compliance teams need to work on an automated and frictionless approach.

McAfee acquires VPN provider TunnelBear for safe connect

Toronto-based TunnelBear was recently acquired by McAfee for an undisclosed amount. The Virtual Private Network service provider will be helping McAfee boost Wi-Fi security progressions for its product Safe Connect.

Christopher Young, McAfee's CEO, said, "This investment is strategic for McAfee's consumer business as it further showcases our commitment to help keep our customers' online data and browsing private and more secure at a time when the threat landscape is growing in volume, speed and complexity." This is McAfee's second acquisition since it pulled out of Intel in 2016. The company acquired Skyhigh Networks for cloud services in November 2017.

TunnelBear announced the takeover in a blog on its official website, saying that after reaching the benchmark of 22 million users on their own, they know that they can reach a wider audience with McAfee. They also mentioned that both the companies will continue to carry out and publish annual security audits, a practice started by TunnelBear in 2017.

KPMG partners with Okta to strengthen its identity access management processes

KPMG announced its partnership with Okta, an identity management solutions provider, in a move to expand its cybersecurity infrastructure. The audit and tax advisory firm will use Okta Identity Cloud to automate their identity and access management processes.

Charlie Jacco, Principal, KPMG Cyber Security Services, said, "Our alliance with Okta is accelerating KPMG's status as a leading cyber security firm with the ability to help clients protect information as they pursue new digital interactions and enhanced productivity in the cloud. With

Okta, we can deliver fast and reliable IAM solutions to help keep data safe, while enhancing the user experience."

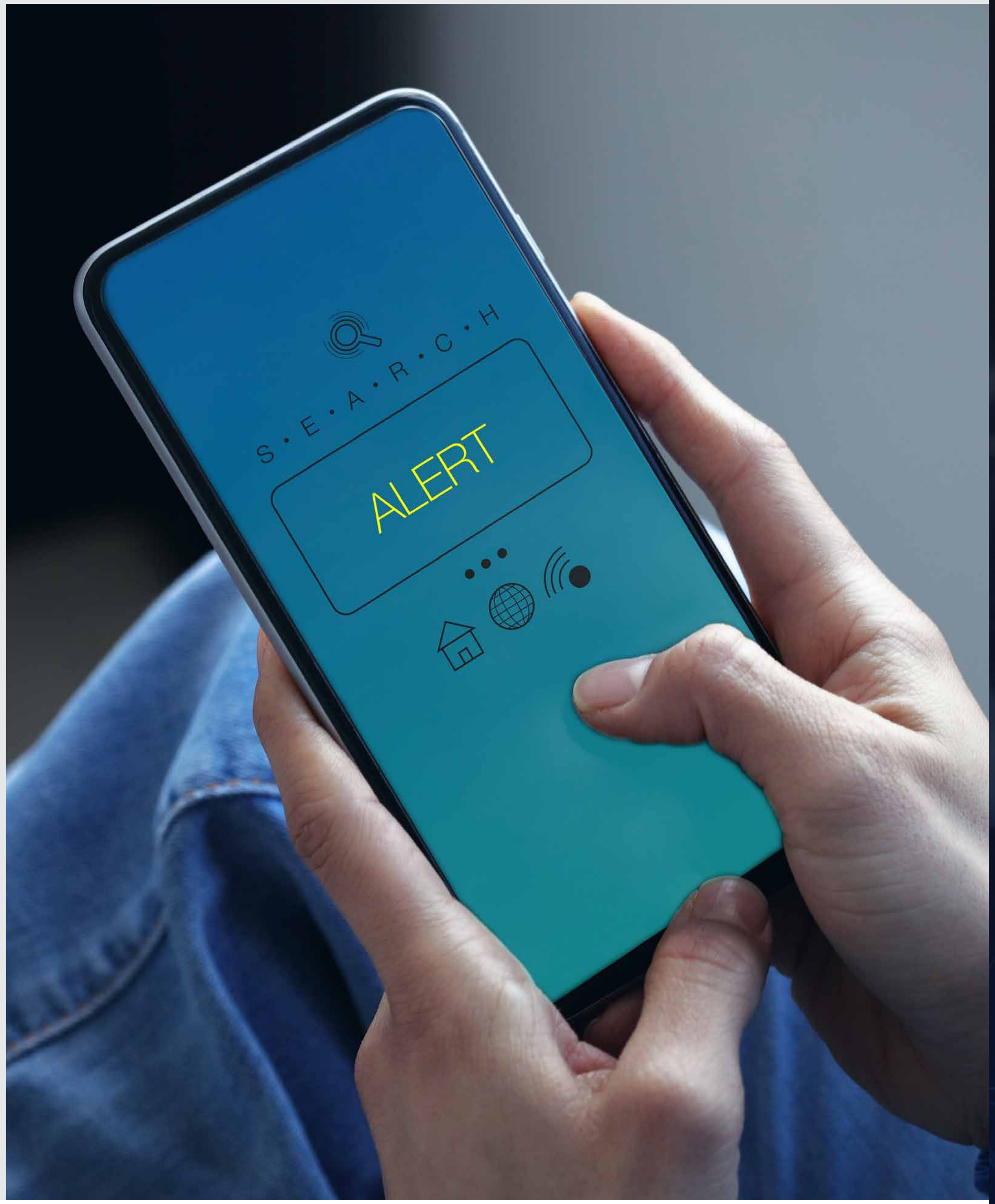
With this alliance, KPMG is looking to augment their identity and access management (IAM) capabilities, creating a robust infrastructure for data protection with agile enterprise for clients. The major competencies of the Okta Identity Cloud are single sign-on (SSP) facility, risk-based multifactor authentication, a turnkey identity layer, automated account creation, and use case interactions.

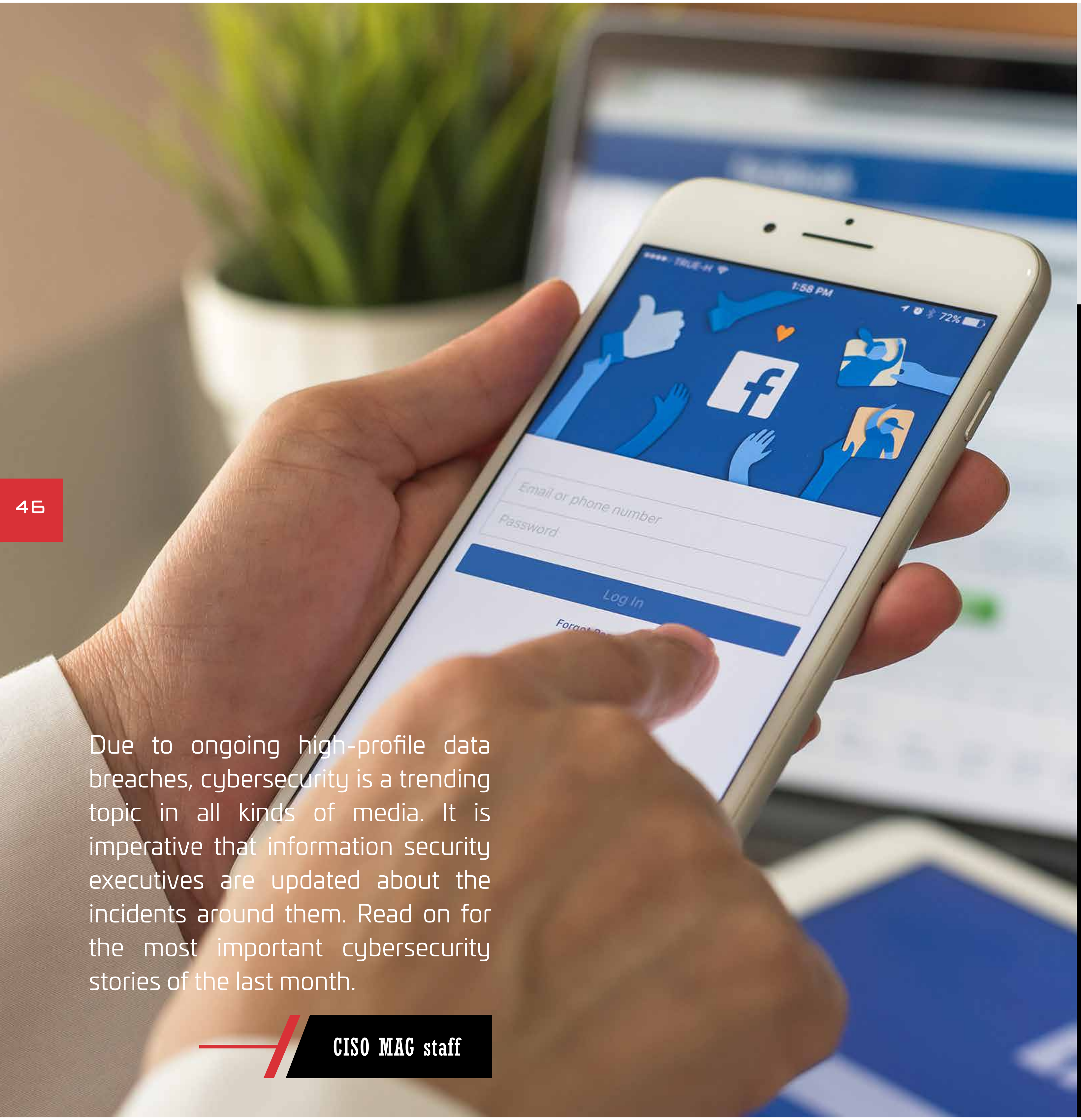
Spherix signs agreement to acquire DatChat

Spherix Incorporated, a technology development company, entered into an agreement to acquire DatChat Inc, a privately held personal privacy platform. DatChat recently launched an app that can control sent messages on recipient's phones. The company is also working on a peer-to-peer secure email system that will be built on Ethereum blockchain technology.

DatChat's acquisition is a part of Spherix's strategy to enter the cybersecurity market. Spherix recently established Ether Mining Company as a subsidiary to mine the cryptocurrency "Ether," a type of crypto token that fuels the Ethereum blockchain network, upon which DatChat's distributed network is being built.

Commenting on the acquisition, Anthony Hayes, CEO of Spherix, said, "Cybersecurity is a rapidly-growing sector based on the ever-increasing threats to privacy and confidential information. News of data breaches at companies large and small are becoming increasingly frequent. We believe that the DatChat Platform offers a solution by giving users total control of their information after transmittal. We believe that the further development of the DatChat's messaging technology into an email application will be the next evolution of blockchain, and that it will allow for permanent and ephemeral chains, content delivery, mining, and third-party application development."





Due to ongoing high-profile data breaches, cybersecurity is a trending topic in all kinds of media. It is imperative that information security executives are updated about the incidents around them. Read on for the most important cybersecurity stories of the last month.

CISO MAG staff

Alex Stamos to leave Facebook over information disclosure disagreement

The announcement of the resignation of Alex Stamos, Facebook's Chief Security Officer, brings increased scrutiny to Facebook's role in allowing Russian operatives to influence the 2016 U.S. presidential election. The cause of his resignation has made headlines as well. Stamos reportedly recommended more information be made public on how the social media platform was utilized by Russian agents to create propaganda and influence the 2016 presidential elections. Facebook did not follow his recommendations and Stamos later resigned.

After being taken to task by US legislators for its role in spreading hateful messages and fake news during the elections, Facebook faced more criticism when Cambridge Analytica, a firm hired by the Trump campaign, proclaimed they accessed the private data of nearly 50 million users in partnership with Facebook to influence the election.

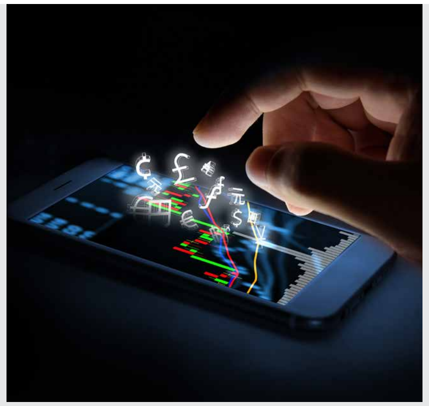
Japan's FSA disciplines seven cryptocurrency exchanges over regulatory flaws

After losing $530 million in a recent cyber attack, the Japanese cryptocurrency exchange Coincheck is once again in news after being served another notice by the Financial Services Agency. This is the second time they have been issued a warning regarding a lapse in proper internal control systems. Six other cryptocurrency exchanges were also reprimanded and ordered to improve their risk management practices, of which Bit Station and FSHO were barred from operating for a month.

Interestingly, all three cryptocurrency exchanges along with two others which have been taken to task are unregistered. The Minister for Internal Affairs and Communications told a news agency, "It's problematic that these 16 unregistered exchanges have been able to continue trading. In the first place, should they have been allowed to operate while their applications for registrations are still incomplete?"

After the cyber heist in January 2018, Coincheck had been instructed by FSA to improve its operations and to submit an incident report by February 13.

The cryptocurrency exchange issued a statement saying, "We will carry out a far-reaching review of our internal control and management systems to ensure proper and reliable business operations from the viewpoint of customer protection."



World Economic Forum creates **Fintech cybersecurity** consortium

On March 6, 2018, the World Economic Forum created an industry consortium to improve the cybersecurity of financial technology companies. Created to architect a framework to gauge the security levels of fintech organizations and data aggregators, the consortium brings together top companies such as Citigroup Inc (C.N), the Depository Trust & Clearing Corporation, Kabbage, Zurich Insurance Group (ZURN.S), and Hewlett Packard Enterprise (HPE.N), according to *Reuters*. The consortium will work with the organization's new Geneva-based Global Centre of Cybersecurity.

Fintech is a perfect foil for the consumers, businesses, and financial institutions who in today's connected, on-demand world want to transact in a convenient, timely, secured, and efficient manner. Traditional banks have realized that fintech is the future; they are trying to stay relevant by collaborating with the up and coming players in the sector.

"Many partnerships are forming between financial technology companies and incumbent institutions," said Matthew Blake, head of the Financial and Monetary System Initiative at the WEF, in an interview. "Through those linkages there is a potential introduction of risk."

Australia launches **Joint Cyber Security Centre** in Sydney

The government of Australia has launched the Joint Cyber Security Centre (JCSC) facility in Sydney with the goal of promoting cybersecurity across government, business, and academia. The facility is a part of the government's $47 million JCSC program that bridges the gap between several public and private sectors including defense, finance, transport, energy, health, mining, and education.

Led by the Computer Emergency Response Team (CERT) Australia, the JCSC will strengthen the cybersecurity infrastructure of the country and will also be involved in sharing actionable cyber threat intelligence among myriad bodies in both public and private space, thus ensuring information flows without any commercial bias.

At present, there are JCSC facilities located in Brisbane, Perth, Melbourne, and Sydney. By late 2018, a center in Adelaide will also join the list. "This is an important step to enhance Australia's defensive cyber capabilities. The JCSC is a critical hub for business and government to improve their cybersecurity practices and share information in a trusted environment," said Angus Taylor, minister for Law Enforcement and Cyber Security. "We have already run a number of cybersecurity exercises across these centers, particularly in the lead up to the Commonwealth Games."

US Lawmakers propose bug bounty program for State Department

House Lawmakers Ted Lieu and Ted Yoho have proposed the 'Hack the State Department' bill which would set up a bug bounty program to boost cybersecurity preparedness in the department. The program seeks to establish a Vulnerability Disclosure Program (VDP), which would encourage white hat hackers to penetrate the Department's systems to find vulnerabilities.

Katherine Charlet, the director of Carnegie's Technology and International Affairs Program who worked on cyber issues in the U.S. Defense Department, has supported the proposal.

Earlier, the Trump administration also proposed setting up bug bounty programs in the "Report to the President on Federal IT Modernization." During the Obama administration, the Department of Defense introduced the Hack the DoD program where ethical hackers were invited to find vulnerabilities and attempt to infiltrate the system. In 2016, Hack the Pentagon was piloted by the then-Secretary of Defense Ash Carter.

Ghana banks asked to disclose cybersecurity policies

Ghana banks have been instructed to publish their bank-specific cybersecurity policies. Speaking at the opening of the digital banking and cybersecurity summit, the Governor of the Bank of Ghana, Dr. Ernest Addison, stated that banks must publish cybersecurity policies which are in accordance with provisions in the Payment Systems and Services bill that is currently before the Parliament.

The Bank of Ghana will continue to be involved in preparing regulatory policies. "As policymakers and regulators, we will continue to exercise firm oversight of the payment system, monitor risks associated with digital innovation and develop appropriate regulatory responses without stifling innovation. So far, the Bank has prepared a banking sector Cyber and Information Security guidelines to protect consumers and create a safer environment for online and e-payments products," Addison said. "Among others, the guidelines seek to create a secure environment for transactions within the cyberspace and guarantee trust and confidence in ICT systems, provide an assurance framework for the design of security policies in compliance to global security standards and best practices by way of cyber and information security assessments, and protect banks, customers and clients against the potentially devastating consequences of cyber attacks."

He highlighted the cybersecurity threats specific to the banking sector of the country. According to him, a safe environment for online and e-payment transactions are the key factors to boost the sector. "Financial Institutions would also be required to implement an integrated approach to adopting enterprise-wide frameworks of cyber risk management in line with business objectives," he pointed out. "It is anticipated that the integrated approach to cyber security management, would support financial institutions achieve both business and security-focused objectives, as well as regulatory compliance in an efficient and effective way."

Chinese hackers targeting WhatsApp, Indian Army warns users

The Indian Army has issued a warning to users of the social messenger application WhatsApp, alleging that Chinese hackers are targeting them to extract personal data. The Army took to Twitter to urge users to use WhatsApp with caution. The Indian Army's official handle, the Additional Directorate General of Public Interface (ADGPI), also posted a video that said, "Stay cautious, stay alert, stay safe! The Chinese were penetrating the digital world." The video urged users to save contacts by name and to constantly keep a vigil on all WhatsApp groups and numbers. "Chinese are using many platforms to penetrate your digital world. WhatsApp groups are a new way of hacking into your system. Chinese numbers barge into your groups and start extracting all the data," it advises. "If you change your mobile number, inform the group admin; if you change your SIM card, destroy it completely,"

A few months ago, the army had ordered its personnel stationed within its borders to uninstall several applications and format their phones to safeguard its data from Chinese hackers. According to the notifications issued earlier, the army had suspected that Chinese-developed applications were scripted with malware which could potentially endanger the national security of India. Smartphones manufactured by Chinese firm Xioami are particularly scrutinized by the Indian Army and the Indian Air Force over security hazards. "As per reliable inputs, a number of Android/iOS apps developed by Chinese developers or having Chinese links are reportedly either spyware or other malicious ware. Use of these apps by our force personnel can be detrimental to data security having implications on the force and national security," the advisory read.

German government computer networks attacked

According to dpa-international, the German government's computer networks were attacked by APT28, a Russia-backed hacker group. The isolated attack, which was noticed in December, targeted Germany's foreign and defense ministries with an intention to steal data.

A spokesperson for the German Interior Ministry said the situation has been brought under control and appropriate measures were taken to investigate the incident and protect data. "The attack was isolated and brought under control within the federal administration," the spokesman said. He added that authorities are addressing the incident "with high priority and significant resources." However, he did not comment on whether APT28 was involved in the attack.

This is not the first time APT28 has been associated with a cyber-attack on the German government. The infamous group was accused of carrying out an attack on the German Parliament in 2015. It has also carried out attacks on a number of entities in the U.S., Eastern Europe, and other parts of the world.

Reuters reported that the German parliamentary committee that oversees the intelligence agencies and the digital committee will discuss the attack during their next session. It has also been reported that authorities had been aware of the attack for some time.

Atlanta suffers ransomware attack

On March 22, the city of Atlanta was hit with a ransomware attack, causing disruptions across the city and shutting down some government offices. A statement released by the mayor's office assured that systems would soon be operational and offices would return to normalcy, but manual processes would be used until full functionality could be restored. After a week of the attack, the city was still grappling with the effects of the attack.

Five of the thirteen departments of the city had to resort to manual processes for things like the payment of bills and parking tickets, and the Department of Corrections had to manually process inmate paperwork. The government website ATL311 is functioning and accepting requests again after a week, while some services are still down.

Online travel company Orbitz loses customer data to hackers

Travel metasearch engine and fare aggregator website Orbitz became the victim of a grim cyber heist on Tuesday, March 21, 2018. Orbitz, a subsidiary of Expedia Inc., fears that hackers may have accessed the payment card data of nearly 880,000 customers. According to Orbitz, their investigation shows that their old website was hacked some time during the beginning of the 2016 and the end of 2017, adding that the new website wasn't affected.

The hackers might have been able to exfiltrate customer information which included names, phone numbers, email IDs, and billing addresses, said the online travel services provider. "To date, we do not have direct evidence that this personal information was actually taken from the platform and there has been no evidence of access to other types of personal information, including passport and travel itinerary information," informed Orbitz. The company found out about the breach in the beginning of March 2018, following which the shares of Expedia fell 1.9 percent. Orbitz is offering a year of free credit monitoring and identity protection service to those affected, which include both consumers and business partners.

The ways in which the world's infrastructure is vulnerable to cyber attacks is constantly growing thanks to technology advancements. There is some good news, though. As organizations around the world are learning to take information security more seriously, we are seeing more appointments of cybersecurity leaders across several organizations. Here are some of the most noteworthy:

CISO MAG staff

EdgeWave appoints three cybersecurity veterans

EdgeWave, Inc., a provider of cybersecurity solutions, bolstered their organizational structure with the addition of three IT and cybersecurity veterans. The company appointed Anita Boghoussian as their new Vice President of Sales, Gang Ding as the Director of Engineering, and Aron McGrane as Director of Customer Success. The move is expected to help EdgeWave consolidate its market position and grow in the field of email and web security.

Boghoussian joins EdgeWave from Dassault Systèmes where she provided the company sales enablement, coaching, mentoring, and structuring in the North American market. Ding, on the other hand, was working with ZitoVault as the Director of Engineering. He has also worked with Qualcomm, Olympus Communication Technology of America, and Kiyon. McGrane is a 15-year veteran in technical support and has previously worked with Forcepoint and Websense.

"As businesses and government organizations struggle to balance risk, usability and price in their fight against ever-increasing cyber threats, we at EdgeWave are accelerating our efforts to mitigate those risks and reduce costs and complexity through products like ThreatTest," says EdgeWave CEO Lou Ryan. "A big part of this effort includes hiring these three outstanding executives. We're excited to utilize their talents as part of our strategic growth in 2018."

Kroll appoints Timothy Gallagher as Managing Director for Cyber Security and Investigations practice

Kroll, a company offering risk mitigation, investigations, compliance, cyber resilience, security, and incident response solutions, appointed Timothy Gallagher as a Managing Director in its Cyber Security and Investigations practice.

Gallagher, a highly regarded law enforcement executive, has worked with the Federal Bureau of Investigation for two decades and has immense investigative experience in financial fraud and cyber crime. Last year, Gallagher was working as Deputy Assistant Director of the Criminal Investigative Division in the FBI.

"Tim's exemplary track record dovetails well with Kroll's commitment to our global clientele. His investigative tenacity and expertise coupled with his sophisticated knowledge of digital threats will enable him to make an immediate impact," said Jason Smolanoff, Senior Managing Director and Global Cyber Security Practice Leader for Kroll. "Most significantly, his demonstrated capacity to lead and to solve complex problems further reinforces the extraordinary team of professionals we have at Kroll."

Burr & Forman appoints **Eddie Saunier** as CSO

Burr & Forman LLP, an American law firm, recently announced Eddie Saunier is the company's CSO. Saunier, who has been associated with the firm since 2002, is leading Burr & Forman's overall information security program in his new role. He will also manage the compliance and risk management

in the Southeast regional firm that has 300 attorneys and 12 offices across the country.

"Eddie's devotion to managing and securing Burr & Forman's systems and networking infrastructure with the utmost level of scrutiny furthers our confidence in his ability to meet all the information security needs of the firm and our client information," said Burr & Forman Chief Executive Officer Ed Christian. "Eddie will ensure we are at the forefront of best practices to provide a consistent level of data security. We are proud to have Eddie in this new role."

Scotland Digital Office appoints **Andy Grayland** as CISO

To support local authorities against the risk of cyber attacks, Scottish Digital Office for Local Government has appointed Andy Grayland as CISO.

Grayland will be involved in providing leadership to help local authorities achieve goals of the Cyber Resilience Strategy for Scotland, the National Cyber Security Strategy, as well as the recently announced Action Plan on Cyber Resilience which involves "developing the cybersecurity workforce, raising public awareness, and increasing cyber resilience in the workplace." Other stakeholders in the action plan include the education and skills development sectors of Scotland.

Grayland will also assist CEOs and several council management teams, so that organizations are prepared to avert cyber attacks at all levels. He will also help IT managers, cybersecurity officers, and data protection officers to review cybersecurity regulations and compliance to develop collaborative actions plans.

"In the current climate of evermore sophisticated cyber attacks that private and public sector experience day-to-day, Andy and his experience is a great asset for the Digital Partnership to accelerate and enhance our cyber credentials," Martyn Wallace, Chief Digital Officer for Scotland, said in a statement.

With cybersecurity gaining more importance than ever, cybersecurity startups have become a huge attraction for venture capitalists. The cybersecurity market has seen tremendous growth despite the slowdown in the global economy, with many companies inking record-breaking funding deals with venture capital firms. The influx of money has driven innovation and solutions to important security challenges. In this section, we look at some emerging companies making waves in the information security domain.

CISO MAG staff

Cognigo

Founded in 2015, Cognigo, earlier known as D.Day Labs, is a cybersecurity startup based out of Tel Aviv, Isreal, and was founded by Guy Leibovitz.

What sets Cognigo apart: The company specializes in data protection, dark data, critical data visualization, breach detection, cybersecurity, and GDPR.

Market Adoption: Cognigo is a single point of control to manage and secure critical data assets and PIIs. The company was founded by team of machine learning experts, and cybersecurity veterans, with a mission to ensure that critical data assets, which are now more important than ever before, will not fall into the wrong hands. Its product DataSense generates the comprehensive insights into structured and unstructured data silos. Leveraging AI algorithms, DataSense develops a human-like understanding of any data record at scale, providing visibility and out-of-the-box GDPR and security policies enforcement.

Elastic Beam

Founded in 2014 by Bernard Harguindeguy and Uday Subbarayan, Elastic Beam is an AI-powered API Security company, based out of the Silicon Valley.

What sets Elastic Beam apart: The company's ABI Behavioral Security (ABS) solution uses artificial intelligence to examine API transactions for cyber attacks.

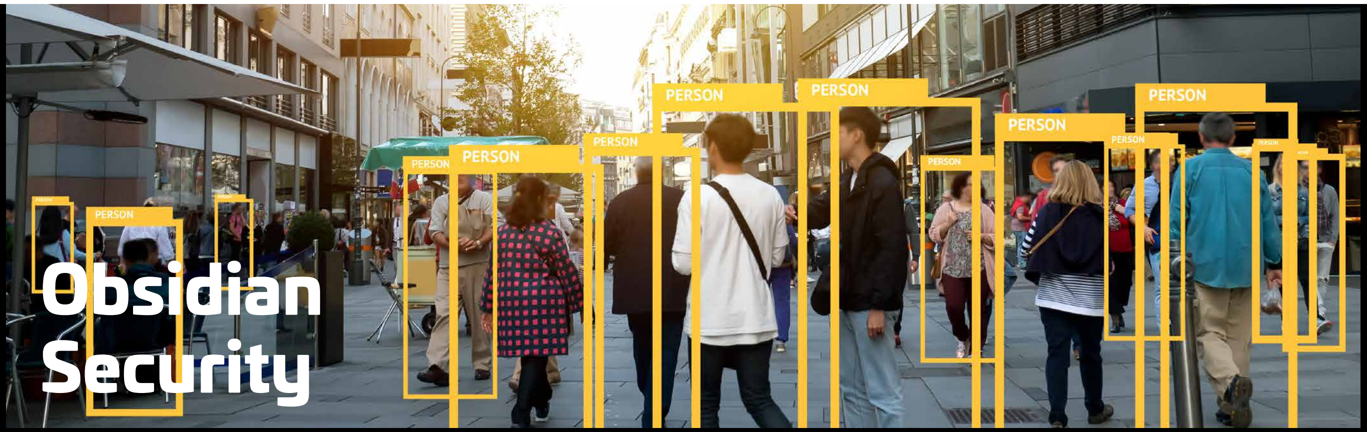
Market Adoption: Since its inception, Elastic Beam has assembled the best AI technology, team, and IP assets to address the growing need for more sophisticated defense against API-based cyberattacks. It's API Security Enforcer (ASE) delivers high-performance processing of API traffic with real-time security, as well as API deception as a trap for hackers. Both solutions can be deployed on-premises, cloud or even cloud bursting.

JASK

Founded in 2015 by Greg Martin, JASK is a AI-based cybersecurity company, based out of San Fransisco.

What sets JASK apart: The company leverages AI and machine learning to automate basic and repetitive security operations tasks.

Market Adoption: Headed by industry leaders from ArcSight, Carbon Black, Cylance, and the counter-intelligence community, JASK brings together decades of experience solving real-world SOC issues. Founded to address the technology gaps that restrict security modernization efforts, the company is revolutionizing security operations to reduce organizational risk and improve efficiency through technology consolidation, enhanced AI and machine learning. JASK is backed by Dell Technologies Capital, TenEleven Ventures, Battery Ventures and Vertical Venture Partners.



Obsidian Security

Founded in 2017 by Ben Johnson, Glenn Chisholm, and Matt Wolff, Obsidian Security is a Newport Beach, California-based AI powered cybersecurity company focused on hybrid-cloud environments.

What sets Obsidian Security apart: The company specializes in hybrid cloud security, Advanced Threat Protection, insider threat protection, threat detection, threat response, automated intelligence, machine learning, and information security software.

Market Adoption: Obsidian Security is applying artificial intelligence to enable user security for enterprise hybrid-cloud environments. The company is backed by Greylock Partners. It recently raised $9.5M in Series A funding which the company will use to grow its product team working at the intersection of security, artificial intelligence and hybrid-cloud technology.

Shift Technology

Founded in 2014 by David Durrleman, Eric Sibony and Jeremy Jawish, Shift Technology utilizes AI to combat insurance fraud.

What sets Shift Technology apart: Shift Technology provides insurance companies with an innovative SaaS solution to improve and scale fraud detection. The analyses performed by Shift are fast, thorough, quantitative and qualitative. Its efficient algorithms are tailored to reproduce fraud handlers' deductive reasoning, making investigations quicker and easier than ever.

Market Adoption: Shift recently announced that MS & AD Insurance Group's Mitsui Sumitomo Insurance Co., Ltd. and Aioi Nissay Dowa Insurance Co., Ltd. will implement Shift Technology's FORCE as a solution to improve existing capabilities to detect fraudulent insurance P&C claims for domestic business. The company has successfully engaged more than 50 insurers globally. To date, Shift has raised over $40 million in capital investment and was named by CB Insights as one of the Global AI Top 100 in both 2017 and 2018.

FEW MINUTES WITH JASON LIM

Vice President of Cyber Security Wiki Labs

Rahul Arora

Jason Lim is the man responsible for setting up Wiki Labs' cybersecurity business division. An information technology expert, Jason is a regular public speaker at several cybersecurity conferences.

Prior to Wiki Labs, he was the General Manager & Business Development Director at Silverlake MasterSAM Group where he was responsible for the entire company operation and strategic direction in Malaysia, and Singapore, well as the company's expansion to Asia Pacific region. In an interesting conversation, discusses the challenges he faced while setting up the cybersecurity Jason division at Wiki Labs, his views on Privilege Access Management Risk, and much more.

How did you get into cybersecurity?

It was through my puzzle – I always feel amazed of how the hackers can get into your network and retrieve sensitive data without anyone knowing it. My first career with a telco exposed me to the black and green screen with lots of UNIX command scripting, it somehow made me feel like I'm the hacker! I then started my cybersecurity career as a technical consultant at MasterSAM in 2011, going around to meet customers and listen to their challenges in managing privileged access. From a pure engineer background, I gained presales knowledge, built my professional services team, and continuously challenged myself to be the subject matter expert. I wrote some whitepapers and data sheets and built marketing campaign. I then challenged myself to grow in business development role. My successful, seven years journey from being technical consultant to becoming general manager has enriched me with great experience in various roles in several domains, ranging from information security, professional services, advisory & consultancy, business development, marketing strategy and service delivery across multiple industries such as financial services, telco, government, oil & gas, MNC, etc. I provide advisory of effective privileged access management framework. I have strong passion toward cybersecurity domain, and often exchange views with other information security professionals. I am also a regular public speaker in several cybersecurity conferences.

According to your LinkedIn bio, you set up the cybersecurity business division in Wiki Labs. What are the things you keep in mind while building a business of this kind?

I follow my business philosophy – People, Strategy, Vision. In my opinion, the most valuable asset in a company is PEOPLE. I always remind myself that your people work for the company, not you. Your role is to help your people to discover their potentials, and enable them to think like a leader and make precise decision for the benefit of the company. Motivation is very important, not just one time but in a continuous nature. Mentoring is equally important to help individual career development. Your success depends on your team. Startup is always a very challenging journey - I need to prepare to lose my project, face high market competition, pick the right technology, count budget every week, motivate my team and hire the right talents. I also need to be ready if someone leaves my team anytime or if I find it hard to gain a customer's trust. I share my vision with the team and motivate them to grow together to achieve our goal. On the other hand, I keep challenging myself and the team . We try to find answers to the questions such as how can we create our uniqueness in the market under strong pressure competition? What makes our customer trust us? Cybersecurity portfolio is getting complex today; I choose to advance in my expertise domains of identity & privileged access management and insider threat management, and motivate my team to excel in SIEM and some cybersecurity services such as vulnerability assessment & penetration testing, cyber maturity assessment, etc. I believe having the right people with the right business strategy and vision would be the key for success in any business.

Do you think cybersecurity practices that organizations are following these days

would be relevant in another two years?

Today, cyber threats are evolving. Cyber attacks are getting more sophisticated and organized. Prevention is no longer an effective strategy because you can't protect if you don't have the visibility. Visibility is the key in today's complex environment. While we have billions of data collected from different sources, it is important to know how can we get good information and provide better insights from it to make decision. Organizations should start leveraging good analytical platform that uses artificial intelligence, machine or deep learning technologies to accelerate data processing and analysis for quicker business value and decision. Organizations today also lack response capability. Many times, when they are under attack, they often panic.

I realize organizations today spend so much time and effort in ensuring they have good policy and they stay compliant to the regulations such as PCI DSS, ISMS, etc. There is nothing wrong with this, but the fact is that it is not just about gaining a tick at the compliance level. Even if you are 100% compliant, it does not mean you are 100% hack-proof. Organizations need to start building a holistic approach towards cyber resilience. Cyber maturity assessment is recommended to provide an in-depth review of an organization's ability to protect its information assets from cyber threats. It combines the view of people, process and technology to identity areas of vulnerability, prioritize areas for remediation, and demonstrate both corporate and operational compliance, turning information risk to business advantage. My advise for organizations would be to continuously review their cyber resilience strategy and preparedness against cyber threats.

According to a recent Privilege Access Management Risk and Compliance Report, 70 percent of organizations fail to fully discover privileged accounts and 40 percent do nothing at all to discover these accounts. How worrying is this and what can be done to counter this?

Visibility is the power – what you don't know can't get you further. Privileged accounts are always the prime target of attackers as they provide the direct path to your network. There is no need to break the windows if you have the key. With privileged account access, you become the "king" and you could do anything you want, including suspending critical service, extracting sensitive information, installing malware, injecting malicious code into programs, deleting entire filesystem, etc. Statistics show that most of the data breach incidents reported today are caused by compromised credentials, lack of visibility and access control, and unauthorized access to the critical systems. Ask yourself few questions – how many firewalls and servers are there in your organization? How many privileged accounts are there within each system? Has anyone changed the default passwords? Do you control who can access those critical systems? How do you monitor third party vendor access? How do you mitigate the risk of password sharing?

I would recommend the 4A principles to complete your privileged access management framework:

Authentication

It is important to know that securing a system with just the password is no longer a good protection strategy. Password is always a hacker's best friend. Hackers may take time to crack the password, depending on its complexity and algorithm. But, the fact is, once the password is compromised, they can access your critical data freely. There is a need to build an extra layer of protection for privileged access to reduce the attack surface. Many security compliance standards have emphasized the needs of multi-factor authentication in their regulatory guidelines as a part of the best security practice today.

Authorization

It is highly recommended to adopt least privilege model as the best security practice. At Zero-Trust principle, it emphasizes on trusting nobody by default, meaning that nobody should have the access to the system until they are granted with proper authorization.

Access

To satisfy the Role Based Access Control (RBAC) principle, the access should always be restricted and relevant to the user's function role. Use auto login technology to connect to critical systems, thus, eliminating the exposure risk of privileged credentials. Each privileged access should be restricted within specific period and none should have administrative access at all times. The privileged credentials must be periodically randomized – either right after use, schedule or manual trigger, based on strong password complexity requirements.

Audit

Auditing is an important process that examines and ensures proper security control is always in place to fulfil regulatory compliance standards. Some of the frequently asked questions from auditors are: when was your last change of password, How do you audit their activities performed on the server? Do you restrict your administrators' access? What is your approval process?

Be sure to monitor and record user activities; the recorded data must be available instantly to allow real time monitoring or session playback, so that one can take immediate action when necessary.

You also hold great expertise in Identity and Access Management. According to you, what are the major challenges in this area?

In the past, cyber attackers spent their time devising ingenious malware, hunting vulnerabilities, stealing credit card information, and exploiting systems for financial gain. Today, cyber attacks are getting more sophisticated and identity theft has become one of the prominent attacks. Attackers just need to find only one weakness among millions of exposure points to gain the door access to organization. The top three challenges are:

Compliance gap due to lack of access review

It's often a nightmare for IT department when it comes to access review audit - processes tend to be manual and they struggle hard to collaborate with business units to generate application entitlement report, and often collect inconsistent outcome, run manual consolidation, and eventually fail the regulatory compliance. Most organizations struggle to answer the basic question: "Who has access to what?" Over time, certain employees may have been granted excessive rights or privileged access to critical systems. Organizations tend to be weak in this visibility context, as a result, audit does flag out these scenarios. There is no centralized and holistic view of user access matrix across the entire organization. You can never get it right without the fundamental visibility.

Manual provisioning and deprovisioning of access

I have seen several examples where a new hire, especially a replacement, is simply granted the same access rights as the existing staff - often by "cloning" their account - without reviewing his/her appropriateness of existing access. During the hiring process, HR would typically inform IT to manually create identity and assign appropriate rights to the new employee. Over time, the employee may have requested for additional access which requires manual grant and revoke operations according to the approved timeframe. If an employee gets promoted or transferred to a different department, his/her current and new roles will also need to be managed properly. When the employee leaves the organization, his/her account would eventually be deactivated and removed one day. Can you imagine there are so many gaps exist due to a huge hassle of manual operation running behind this? Orphan accounts are the best scenario to prove this challenge.

Too many passwords to manage

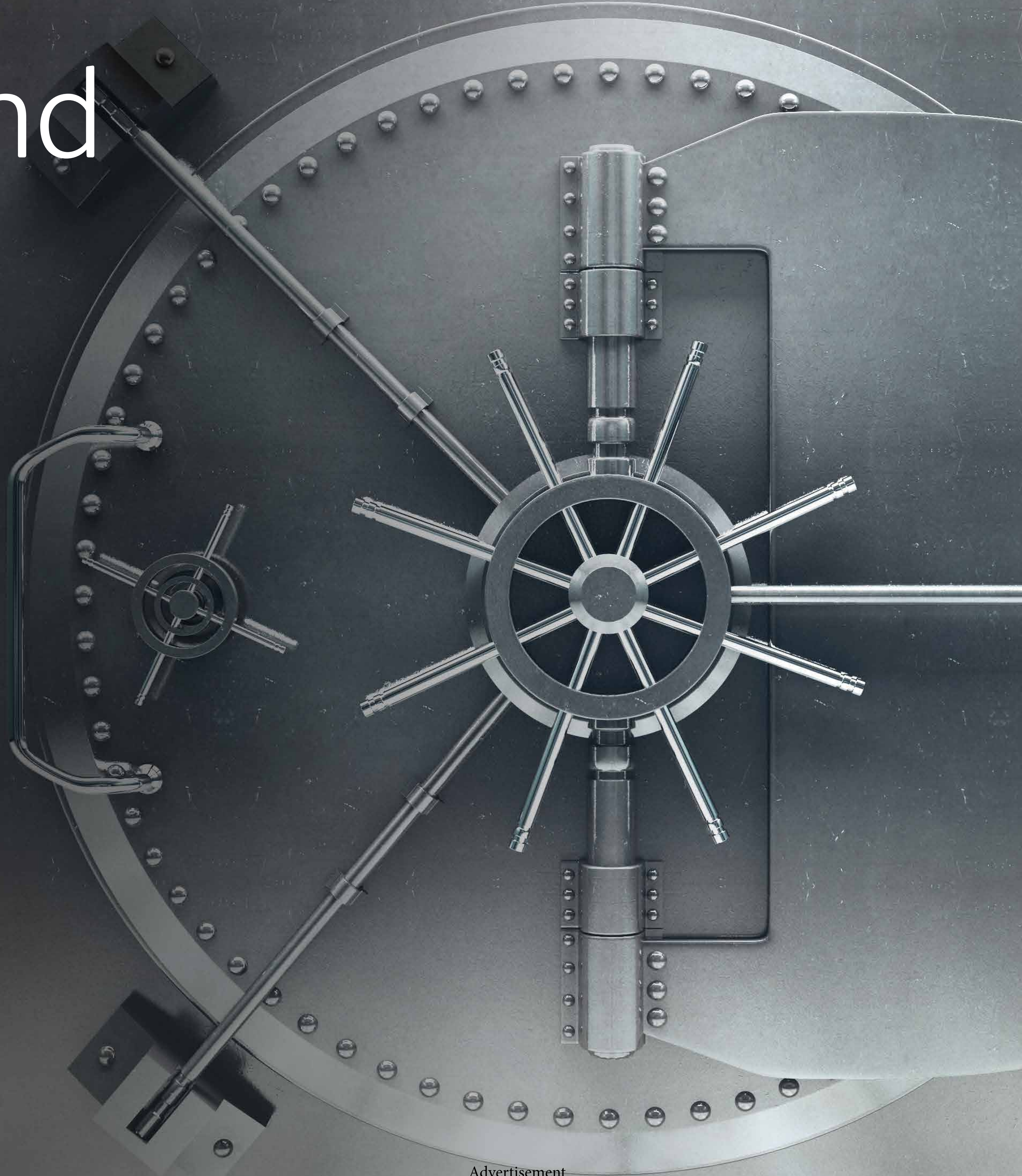
We've all been there before. We waited too long, and our password expired. Or we made a change, and somehow that change didn't trickle down to all of the relevant systems we need to access. If we need to use multiple applications at work, do we use different passwords and make it complex? Most people hate complex and expired passwords and figure out another easy password to remember. Password creation, update and deletion (CRUD) is a real issue with real costs that IT wants to reduce. Having automated tools that are easy to use and can integrate with existing systems can alleviate much of the pain here along with single-sign-on solution that is protected with multi factor authentication.

What are the plans of Wiki Labs for 2018?

Today, Wiki Labs have four core business operating functions – enterprise open source, cybersecurity, network security, and data centre infrastructure. We continue to expand our business and create more holistic values to our clients. We aim to help our enterprise clients in addressing digital transformation requisites, such as cloud and IoT adoption, digital core banking, fintech security by leveraging our expertise and technologies in enterprise open stack platform, software defined network, hyper convergence, and cybersecurity.

What is one piece of advice you would give to budding information security professionals?

Cybersecurity is a *JOURNEY*, not a *DESTINATION*. While cyber attacks are getting more sophisticated, detection and prevention mechanisms are no longer good enough defence strategy. Organizations need to adopt proactive model equipped with mature response and resilience strategies to ensure quick turnaround in return to minimize business impact and risk.



Authentication doesn't have to be complicated.
Unless you're the bad guy.