SECURING FINANCIAL SERVICES VR

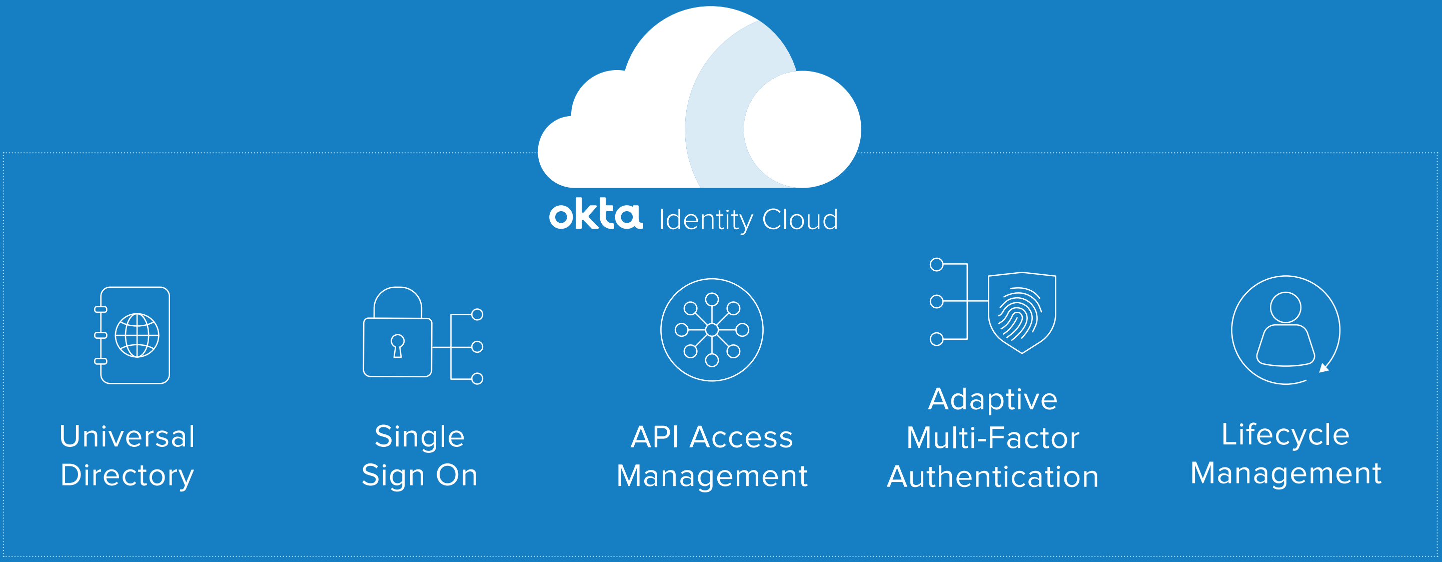
8th July 2020
Online

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Protecting the customer, securing critical global infrastructure

Security, privacy and financial crime priorities for wholesale and retail financial institutions



At the onset of 2020, security teams in the financial services tackled a set of intertwined problems; heavy regulatory demands; the cumbersome inefficiency of legacy systems that seemed posed against digitisation; higher reliance on remote banking services; third-party risk in the supply chain; the heavy appeal financial institutions have for would-be hackers and malicious insiders.

Just a few months into the year, the Covid-19 pandemic hit, forcing security teams to reevaluate their aims as well as the threats posed towards their organisations.

As the full breadth of the crisis has been exposed, old challenges have been amplified and new problems have manifested. The workforce has dispersed with security controls having to be transformed; reliance on mobile and online channels has increased; market critical functions, such as trading rooms, have been pushed out of the bank and into the home highlighting new problems in surveillance and behavioural risk. The process of digitisation has increased rapidly, with cloud configuration a more pressing issue than ever, and the problem of legacy systems still posed but unanswered.

Regulation has prepared the financial services to deal with the security and privacy issues now rife in the newly digital world, and high investment gives financial organisations the edge to tackle complex technological issues. But as change continues, financial institutions must be innovative to mitigate their risks and protect their customers.

We invite you to join us at our first financial services specific event, and our first English language virtual conference. Join us to engage with leading voices from the financial services and interact with peers, colleagues and experts. Through this virtual conference we hope to generate solutions and start dynamic conversations, so make sure to utilise our networking sessions. Don't hesitate to contact a member of our team with any queries.

Will Kaye | Editor

@eCrime_Congress #ecrimecongress

8th July 2020

Online

SECURING FINANCIAL SERVICES VR

Editor:
Will Kaye
e: will.kaye@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
27 John Street
London WC1N 2BX
t: +44 (0)7950 270 051
e: will.kaye@akjassociates.com

Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does.

Those organisations sponsoring or supporting Securing Financial Services VR bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting Securing Financial Services VR, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

SECURING FINANCIAL SERVICES VR

Security resilience in the face of evolving attacker tradecraft

Stories from the cyber battlefield.

CrowdStrike reports

The impact left in the wake of a successful intrusion can be massive when customer data or other confidential information is stolen, exposed, changed or deleted. It's an inescapable certainty that where valuable digital assets exist, threat actors follow. From the global WannaCry ransomware attack to the destructive stealth propagation techniques of NotPetya malware, threat actors are continuously adopting new means to achieve their objectives.

To keep pace, security stakeholders from CISOs and SOC managers to incident responders must evolve their security strategies and ensure resilience in the face of new attacks. Below is real-world case study featured in the CrowdStrike *Cyber Intrusion Services Casebook, 2017.* This much anticipated publication offers detailed accounts of some of the cases the CrowdStrike Services incident response (IR) team has investigated over the past year, and provides expert, real-world analysis and practical guidance that can further your organisation's progress toward that goal.

Drawn from real-life engagements, the Casebook provides valuable insights into the evolving tactics, techniques, and procedures (TTPs) used by today's most sophisticated adversaries. It also describes the strategies the CrowdStrike Services team used to quickly investigate, identify and effectively remove dangerous threats from victims' networks.

One key trend the CrowdStrike team observed is that the lines between nation-state sponsored attack groups and e-crime threat actors continue to blur. As part of this trend, the increase in criminal hackers using fileless attacks and 'living off the land' techniques has been especially pronounced. This uptick in fileless attacks is also documented and independently verified in a recent report from Ponemon Research.[1] Fileless attacks include exploiting processes that are native to the Windows operating system such as PowerShell and Windows Management Instrumentation (WMI). 'Living off the land' describes how adversaries move within the victim's environment once they gain access, often employing anti-forensics tools to erase signs of their presence and increase dwell time.[2] Evidence of this trend is also reflected in the prevalence of brute-force attacks on RDP (remote desktop protocol) servers, which was also observed by the CrowdStrike Services team during their 2017 client engagements.

Situational analysis

A commercial services organisation contacted CrowdStrike Services after being hit by the SamSam ransomware variant, which is commonly associated with xDedic, a Russian-operated darknet forum. The e-crime operators of xDedic have been implicated in a number of nation-state attacks against public sector organisations (you can read more about them at: https://www.crowdstrike.com/blog/education-darknet-hackers-profit-data/).[3]

xDedic operates a market for the selling and buying of crimeware and compromised credentials used for accessing RDP servers. After xDedic sells access to these compromised RDP servers, they are then used in attacks against government agencies and other commercial targets.

Although the organisation had already paid the ransom when they contacted CrowdStrike, they sought help to prevent the ransomware from spreading to other systems and to determine the original point of entry by the attackers.

The CrowdStrike Services team first verified the exact ransomware variant used in the attack. Notably, the variant involved automatically encrypts files on the victim's network – a common ransomware tactic – however, it doesn't give the attacker the ability to access, acquire or exfiltrate data from the network.

The team observed that the adversary used Sticky Keys to launch brute-force attacks and gain RDP login credentials so they could move about the victim's environment freely. Sticky Keys is a Windows Ease of Access feature that enables keyboard shortcuts. Once compromised, it can provide an adversary system-level access without needing to authenticate and provided the attackers with an effective persistence mechanism.

Other fileless or 'living off the land' TTPs tied to xDedic that the investigators found included compromised privileged accounts and network login brute-force attacks, both of which reflect the varied toolsets a sophisticated threat actor leverages in order to penetrate a target environment.

Incident investigation and analysis

After conducting forensic analysis by deploying CrowdStrike Falcon® endpoint monitoring, the team was able to identify the root cause of the intrusion that led to the deployment of the SamSam ransomware within the victim's network. Because they were able to identify the persistence mechanism used by the ransomware, the team could immediately stop its propagation and prevent it from encrypting any additional files. During this process, the team provided comprehensive analysis of a number of areas including:

- Forensic artifacts commonly seen in IR investigations
- Known malicious indicators in each image collected, including file names and MD5 hashes of malicious software
- System registry hives
- Artifacts indicating process execution of malicious and benign software

The analysts also included the manual review of the forensic data looking for other indicators not included above. CrowdStrike determined that an attacker accessed systems within the client environment to create user accounts and to deploy and execute ransomware and batch scripts. Investigators also determined that the attacker's goal was to secure more RDP server logins to sell to other cybercriminal threat actors.

Results and key recommendations

CrowdStrike Services was able to rid the client's environment of the damaging SamSam ransomware completely and help the organisation close the security gaps that had allowed the attack to occur. The team concluded their investigation by providing the client with tailored recommendations to help them strengthen their defences against future attacks. These recommendations included the following:

- *Enforce Network Level Authentication (NLA) for RDP sessions:* Any server that is public-facing on the internet and accessible via RDP should be configured to require NLA for RDP sessions. This forces a user to successfully authenticate prior to receiving the Windows logon screen.
- *Implement two-factor authentication (2FA) to prevent unauthorised access:* 2FA requires users to provide a one-time generated token on a separate device after entering login credentials.
- *Consider CrowdStrike Falcon endpoint protection:* The CrowdStrike Services team begins every investigation by deploying the CrowdStrike Falcon platform to provide endpoint visibility and real-time Indicators of Attack (IOA). You can test drive Falcon[4] or try a no-obligation trial[5] and see first-hand what your current security may be missing.

You can learn more details about this specific case and others investigated by the CrowdStrike Services team by downloading the CrowdStrike Services Cyber Intrusion Casebook 2017[6] which also covers:

- The emerging trends observed in attack behaviours, including the tactics threat actors use to gain entry and maintain a foothold in targeted environments
- Key takeaways – based on the CrowdStrike Services team's extensive experience in the field – that can help both executive stakeholders and security professionals respond more effectively to future attacks
- Recommendations your organisation can implement proactively to improve your ability to prevent, detect and respond to attacks

CrowdStrike® is the leader in Cloud delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The CrowdStrike Falcon platform deploys in minutes to deliver actionable intelligence and real-time protection from Day One. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its Cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike Falcon protects customers against all cyber-attack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack (IOA)-based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, Falcon instantly correlates over 70 billion security events from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection, but there's only one thing to remember about CrowdStrike: WE STOP BREACHES

For more information, please visit **www.crowdstrike.com**

[1] http://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/

[2] https://www.crowdstrike.com/blog/why-dwell-time-continues-to-plague-organizations/

[3] https://www.crowdstrike.com/blog/education-darknet-hackers-profit-data/

[4] https://www.crowdstrike.com/resources/demos/test-drive/

[5] https://www.crowdstrike.com/resources/free-trials/try-falcon-prevent/

[6] https://www.crowdstrike.com/resources/reports/cyber-intrusion-services-casebook/

Improving security: It’s a question of trust

As businesses look to securely enable a long-term remote workforce, they need a security framework that can provide support both today and in the future, keeping people, data and the infrastructure safe.

Okta reports

Millions of people throughout the country are now working remotely. To some, this new way of working comes as a welcome relief; no more commuting, no more distractions and a noticeably improved work-life balance. For others, however, this overnight shift to remote working has caused issues.

It has also led to challenges for businesses. Many companies, across sectors, have not implemented flexible or remote working strategies and are having to put in place new measures for their workforces rapidly. This puts a lot of pressure on CSOs, who are instructed to make this happen securely across complex digital infrastructures.

Rising security issues

In nature, sudden and sizeable migrations attract the inevitable attention of predators looking to take advantage. This is exactly what is happening now. The sudden increase in the threat surface, with entire workforces working remotely, has pushed IT security to the top of the agenda as employee endpoints look increasingly vulnerable when used outside the office.

The CTI League, an online, global community of cyber threat intelligence researchers, infosec experts and CISOs, examined the cybersecurity landscape in March 2020 and took down 2,833 indicators of compromise (IOCs) during this four-week period. The majority of these (99.4%) were malicious domains attempting to exploit the pandemic. Further, the group witnessed a large number of vulnerabilities – 136 per day on average – targeting the healthcare sector, along with a spike in the spread of disinformation, such as campaigns that associated the current pandemic with the rollout of 5G equipment, and others that encouraged citizens to break lockdown orders.

> The sudden increase in the threat surface, with entire workforces working remotely, has pushed IT security to the top of the agenda as employee endpoints look increasingly vulnerable when used outside the office.

Proofpoint also found that threat actors are actively using COVID-19 social engineering themes to try to take advantage of remote workers, health concerns, stimulus payments, trusted brands, and more. Initially Proofpoint’s threat intelligence team were seeing about one campaign a day worldwide, they are now observing three to four each day.

How zero trust can help

This increased threat level combined with more people working from home has put technology to the test at an unprecedented scale and speed. And while we’ve seen a lot of rapid success with firms spinning up remote working security tools, for many this short-term firefighting approach isn’t sustainable, especially as technology and business leaders expect changes like expanded work from home policies to persist long after the crisis. And that’s what workers want. According to Okta’s *The New Workplace: Re-imagining Work After 2020* report, only one in four UK workers want to go back to the office full-time and 35% saying they’d prefer a flexible arrangement where they can work from home on a part-time basis.

As businesses look to securely enable a long-term remote workforce, they need a security framework that can provide support both today and in the future, keeping people, data and the infrastructure safe. That’s why the zero trust principle of ‘never trust, always verify’ is essential.

Building employee trust

Businesses need to do more than implement a zero trust framework. They need to ensure that they are trustworthy to their employees in order to facilitate this new way of working.

Okta’s report found that less than a third of office workers said they were completely confident that the working from home online security measures implemented by their employer would keep them safe from cyber-attacks, with just 4% saying they weren’t confident at all. This level of preparedness varies between sectors; while 58% respondents working in the IT industry trusted that their employer was completely prepared from a security point of view, just a quarter of those in the retail and education sectors had a similar level of confidence.

But the issue of trust extends beyond the technology we use. It is now certain that we will move towards a

It's not just about enabling remote working for those employees who thrive in that environment, it's about focusing on providing the same quality of employee experience that the office life can give us.

more distributed workforce, where communication and culture will move beyond the boundaries of a physical location so that everyone is included and engaged and working efficiently, regardless of where they live.

Reaping the rewards of a new, dynamic way of working

Companies that want to succeed in this new era of working need to be secure, technologically-enabled and culturally-ready to manage the challenge. It's not just about enabling remote working for those employees who thrive in that environment, it's about focusing on providing the same quality of employee experience that the office life can give us.

This dynamic approach to work also offers bigger picture gains, such as improving the average employees' work-life balance. Balancing these two worlds is often key to feeling happier, reducing stress and being more productive while at work, which in turn benefits any company. Businesses will get the most out of this new way of working if they focus on securing their workforce, ensuring that their employees trust them and by working together to fight off the inevitable attention of the circling predators. □

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 8,000 organisations, including 20th Century Fox, Engie, Nordstrom, Slack, Gatwick Airport and Twilio, trust Okta to help protect the identities of their workforces and customers.

For more information, please visit **www.okta.com/uk**

okta

Menlo Security thwarts Covid-19-related phishing attacks

Malicious actors around the world are taking advantage of the global pandemic.

Mehul Patel reports

Threat actors can be ruthless. They use social engineering to comb through people's personal and professional lives to uncover details that they can use in spear phishing campaigns to manipulate users into unwittingly downloading malware or giving up their credentials.

This tactic often takes the form of finding out an application or vendor the person uses and spinning up a legitimate-looking email from a trusted brand with a believable call to action, such as approving a transaction or logging into a Software as a Service (SaaS) platform. The most evil spear phishing campaigns take advantage of current events such as natural disasters and tragedies to prey on people's emotions, vulnerabilities, or good will.

Covid-19 has provided a particularly large opportunity for attackers to use this heinous deception. Malicious actors around the world are taking advantage of the global pandemic and its fallout to trick users. It's sick and disturbing and desecrates the memory of the more than 400,000 people globally who have died of the disease to date.

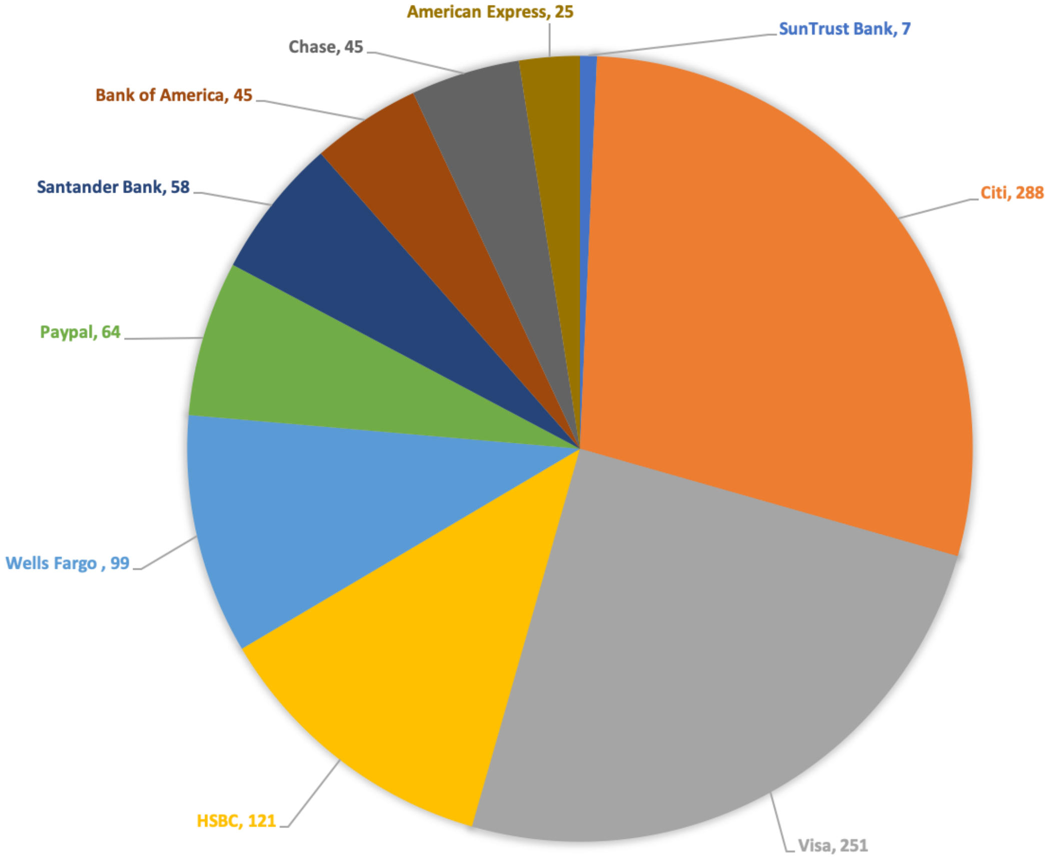
But, unfortunately, it's effective.

According to industry data, phishing attacks have a 30% or higher success rate – the most successful of any threat category. This is scary when you consider that all it takes is a single click by one user to put an entire organisation at risk.

Menlo Security Research is constantly analysing threat data across our customer base to uncover trends that could help us protect our users. Sure enough, we saw a spike in Covid-19-related phishing attacks in the first three months of 2020. In fact, 50% of all phishing attacks impersonating financial services companies leveraged a Covid-19 topic.

Many companies sent communications to customers warning of the attacks, citing attempts they had uncovered that offered medical products,

Number of successful phishing attacks impersonating financial services companies



It's not surprising that malicious actors would use a global pandemic to take advantage of people. They are, after all, malicious. It's up to organisations to protect users from spear phishing and other cybersecurity threats that use email as an attack vector.

guidance, or a safe haven for money, but their warnings weren't enough. Our data reveals that a single Covid-19-related attack targeting HSBC customers in Hong Kong, Singapore, and Australia had had a 3% success rate – lower than the industry average, yet still successful. Menlo Security customers were not impacted – even the users who clicked on the malicious link. Instead, the content was isolated in a remote web browser in the cloud while web forms were rendered in read-only mode. This prevented the malware from downloading on users' devices and stopped users from divulging their login credentials.

Not everyone was so lucky. It's likely that more than a few HSBC customers who aren't protected by Menlo Security were duped and had their devices compromised. From there, who knows what systems the attackers were able to infiltrate.

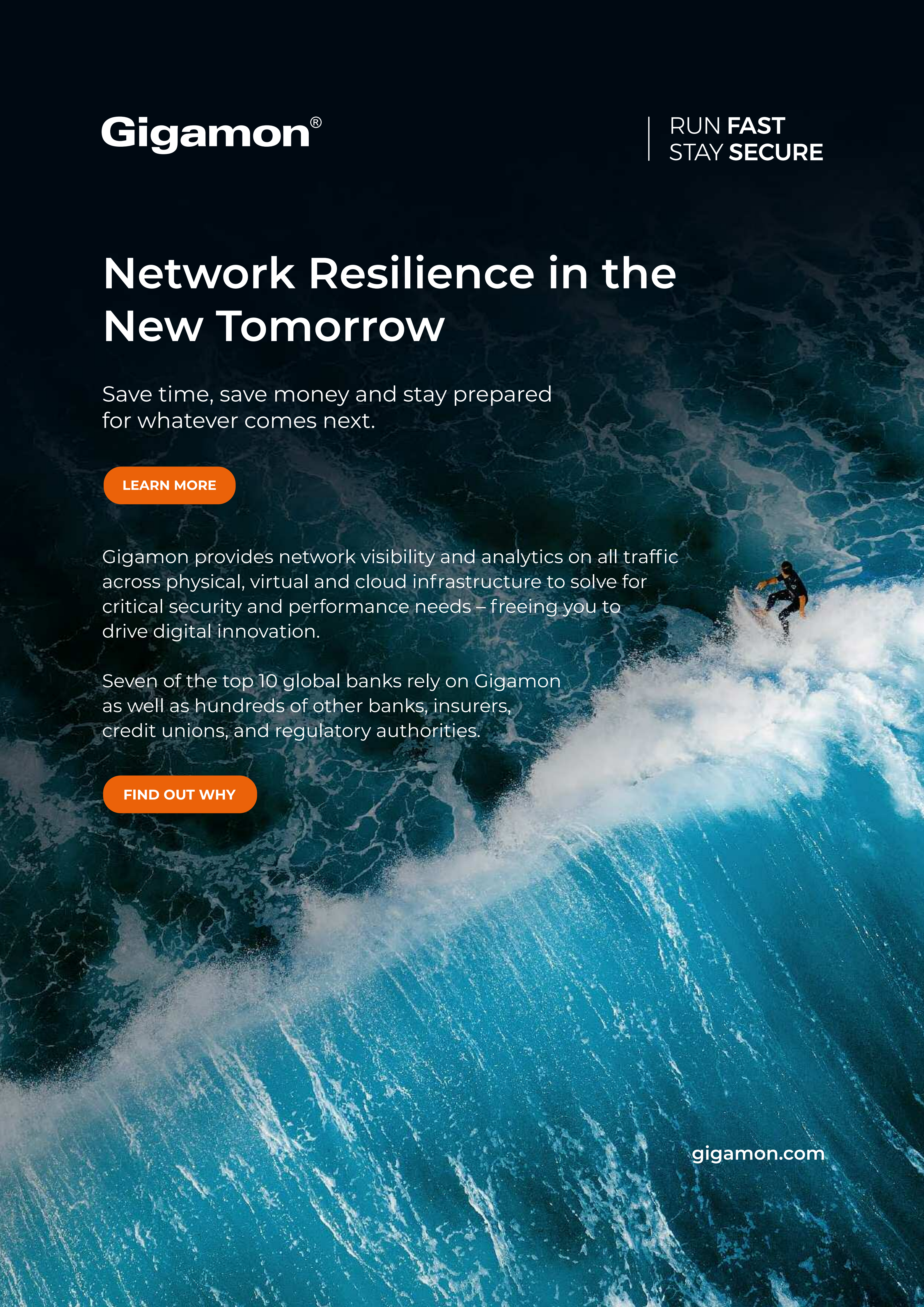
Of course, HSBC customers aren't the only ones being targeted. Other Covid-19-related attacks that Menlo Security stopped included impersonated official communications from Wells Fargo, Capital One, and FirstBank in the US. In the FirstBank example, users were directed to a legitimate-looking website where they were prompted to input their credentials in a fake web form. The attacker attempted to steal customers' usernames, passwords, account PINs, email addresses, and email passwords. Armed with this information, threat actors would be able to wipe out a customer's account balance in a matter of minutes.

It's not surprising that malicious actors would use a global pandemic to take advantage of people. They are, after all, malicious. It's up to organisations to protect users from spear phishing and other cybersecurity threats that use email as an attack vector.

Learn how Menlo Security helps Fortune 500 companies keep users safe from phishing attacks. □

For more information, please visit
www.menlosecurity.com

Menlo Security



Gigamon®

RUN **FAST**
STAY **SECURE**

Network Resilience in the New Tomorrow

Save time, save money and stay prepared for whatever comes next.

LEARN MORE

Gigamon provides network visibility and analytics on all traffic across physical, virtual and cloud infrastructure to solve for critical security and performance needs – freeing you to drive digital innovation.

Seven of the top 10 global banks rely on Gigamon as well as hundreds of other banks, insurers, credit unions, and regulatory authorities.

FIND OUT WHY

gigamon.com

Creating a secure new tomorrow for financial services

As the economy starts to reopen, security must remain front of mind.

Adrian Rowley reports

The financial services industry has been in a period of transformation over the last few years. Digital initiatives have been at the centre of such change; competition between long-established traditional firms and digital-first newcomers has been fierce, and companies have been working tirelessly to modernise their processes, enhance the customer experience and keep up with the pace of technological evolution. According to Forrester, in 2019, 66% of financial services firms were undergoing digital transformation journeys, while 19% were looking into how to start theirs.

As if this weren't challenging enough for a sector rooted in traditionalism, the COVID-19 pandemic only complicated matters further. The economic downturn prompted businesses of all types and sizes to seek loans and financial support – the UK government announced in March a £330b package of government-backed, guaranteed loans to help struggling companies, and has since instated additional schemes and measures with the same objective. This move inevitably put banking systems under increased pressure, as they rushed to process an overwhelming number of loan applications with reduced resources. Furthermore, social distancing measures made it even more urgent to finetune services such as online banking and contactless payments. Customer success depended on banks' ability to be agile and for its infrastructure to be capable of seamlessly delivering what had now become essential digital services.

Simultaneously, just like all other businesses, financial services providers also saw the majority of their workforce working remotely, thereby creating an additional layer of complexity and widening the security threat surface. While cybersecurity is a priority for all businesses, financial services firms in particular are responsible for helping prevent crimes such as fraud and identity theft, so maintaining customer data privacy is of the utmost importance.

> Customer success depended on banks' ability to be agile and for its infrastructure to be capable of seamlessly delivering what had now become essential digital services.

Far from the protection of their physical premises, financial services employees found themselves suddenly exposed to heightened risks from attackers, meaning security efforts had to be enhanced.

Blurred network perimeters and fierce cyber-threats

As the economy starts to reopen, the challenges for financial services providers might have evolved, but security must remain front of mind. Preoccupied with plans for managing a fluid workforce and customer, and ramping up operations to make up for lost time and revenue, financial services providers must not take their eye off the ball when it comes to protecting their infrastructure and data. The only way to drive thorough protection of these fragmented, intensely active IT infrastructures is ensuring uncompromised visibility into network traffic, which flags potential threats.

Business networks are now more complex than ever before. Financial workers are now accessing the network via a mix of company and own desktops, laptops and mobiles, using 4G data or home WiFi connections, meaning attack surfaces have expanded and perimeters have become harder to defend. While the majority of organisations are having to deal with similar technical challenges, things are even tougher in the financial services space: attacks exploiting banking trojans surged sharply in May 2020, and the notorious Qbot banking trojan has made a return with more robust capabilities that allow it to steal victims' financial data more effectively. To cope with the increased complexity and the new exacerbated threats, IT leaders in financial firms must understand visibility is the key to security. Not only is it crucial to have a clear view of what takes place in this incrementally staggered and hybrid infrastructure, it is also fundamental to ramp up monitoring of encrypted traffic and keep a close eye on malware potentially hiding there.

The role of application metadata intelligence

Defending financial services providers against targeted attacks in the current climate means constantly monitoring all elements of their networks. But, due to the acceleration of digitalisation and the fluid workforce, infrastructures are more intricate, with a combination of on-prem and cloud-based applications. This inevitably means more blind spots and creates a more pressing need for pervasive

The COVID-19 outbreak might just be the catalyst financial institutions needed to finally embrace digitalisation and strengthen their security posture in a fast-moving world where no organisation is safe from cybercrime.

visibility – you simply can't protect what you can't see. Visibility isn't just about spotting threats, it's also about compiling network traffic and optimising monitoring tools by streamlining its decryption – this, in turn, improves security outcomes.

At a time where budgets are tight and IT teams are constantly swamped, financial services providers should turn to technology that can enable resource optimisation and make employees' life easier. Generating application metadata helps ensure each network monitoring tool only receives relevant traffic to analyse, enabling IT and NetOps teams to filter packets by application and deduplicate traffic. On the whole, this empowers financial organisations to make the most of their monitoring tools, maximising their investments and existing resources. From a security point of view, information extracted from application metadata allows IT professionals to pinpoint suspicious events more accurately and efficiently. Think of, for instance, users connecting remotely, carrying out anomalous activity. In the era of flexible working, these insights are critical to prevent malicious actors from exploiting the current situation.

Saying no to implicit trust

With money being a key driving factor behind cyber-attacks, it's no surprise financial services providers find themselves in the eye of the hurricane, and flexible working obviously presents some serious concerns. While cybersecurity should always be everyone's responsibility, and each worker should be mindful of tactics used to exploit credentials, the fact that people now often work outside of the office walls makes these risks even more prominent: a survey carried out this June shows 94% of IT professionals in this industry are not confident their colleagues can effectively safeguard customer information. Even as financial institutions prepare to reopen some of their offices, flexible working and the constant traffic shifts (LAN to WAN, to LAN again) mean security difficulties continue to exist. With social engineering attacks still at their peak and employees undefended by office walls and on-prem infrastructures, no one on the network can be implicitly trusted.

Adopting a zero trust approach means never granting automatic access to any user based on their privileges, but analysing their behaviour, as it may reveal malicious intentions. This is yet another area of the financial services infosecurity puzzle where the visibility piece fits perfectly as the enabling feature of zero trust. A clear view of all network activities paves the way for user or asset behaviour monitoring, empowering systems to authorise access only when appropriate.

Current global events have affected financial services providers in ways many of them were not prepared for. Forcing workers to connect more flexibly, compelling customers to interact digitally and causing businesses to seek support in larger numbers, the crisis has exposed existing infrastructure difficulties and created new ones, leaving these companies no choice but to increase their focus on IT and security. While these may sound like negative considerations, the COVID-19 outbreak might just be the catalyst financial institutions needed to finally embrace digitalisation and strengthen their security posture in a fast-moving world where no organisation is safe from cybercrime. By enhancing visibility across their networks, traffic, applications and all data in motion, financial services providers can achieve these goals and emerge stronger in the new tomorrow. □

Adrian Rowley is Senior Director Sales Engineering EMEA at Gigamon.

Gigamon is the first company to deliver complete network visibility and analytics on all information-in-motion, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyse network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organisation to drive digital innovation.

For more information, please visit **www.gigamon.com**

Gigamon®

Return to base: The CISO's guide to preparing a COVID-19 exit strategy

The return to the office will require organisations to adapt and act differently.

SentinelOne reports

While governments are looking into the timing and manner of reopening the economy, it is clear that at some point in the hopefully not-too-distant future restrictions will be eased and businesses will return to normal operations. Returning to offices will certainly signify a return to normality, and for most, that will be a welcome relief. However, just as the shift to working from home required organisations to adapt and act differently, so will the return to the office. In this article, we discuss the preparation CISOs should consider making to offset a number of security implications that arise from returning your workforce back to the office.

Making sure returning devices are safe to use

When returning to the office, employees will haul back all the IT equipment they have used at home. Some of this is trivial office equipment like screens, docking stations and cables, but computing devices can be a security blindspot.

Rogue devices

While unknown connected devices pose a security risk at all times, the return to the office represents an even bigger risk. People could have used all sorts of devices during their time at home, for leisure and convenience. While there, such devices may not pose a serious security risk, but if they are introduced to the corporate network, they could become one.

Do run a scan on your network to identify new, unknown devices.

Home laptops

Some employees working from home may have had to use their own laptops, either because in the rush to vacate offices the IT department might not have had sufficient inventory or just through personal preference. In such cases, they are likely to bring these laptops with them when they return to the office, plug them into the corporate network and continue to work as they had been doing at home. These devices could potentially be infected with malware if they have not been running updated, corporate-grade EDR solutions.

Do forbid work on personal laptops in the corporate environment whenever possible.

Employees should transfer their work to their company-issued laptop and take their personal laptop back home.

Do install NAC for employees who now find they must work with their own device, and ensure they use company-issued EDR.

USBs and NAS

Another practice employees may have adopted while working from home is the use of USB thumb drives and network storage devices. Personal storage devices should be prohibited in the corporate environment and not allowed to connect to company computers and networks.

Do enforce device control to block unauthorised USB and other peripheral devices.

Inventory

As many employees took equipment home, it is necessary to register and keep an up-to-date inventory of this equipment and its whereabouts. In the first instance, this makes sense to avoid wasting resources: ensure employees return cables and screens that they have borrowed from the workplace. It is possible that some staff took an extra laptop home and that the device is now stranded somewhere, perhaps even connected to the home network and exposed to the world.

Do keep an up-to-date inventory. It will also help in the event employees have to move back to working from home in the future.

Keeping insecure software off your network

Even if the devices used at home were company-issued, they can still be a threat if they are not installed with updated software and security systems.

Updated OS and software

Unpatched and outdated Operating Systems can facilitate data breaches. Some employees may have ignored the update prompt or rescheduled these indefinitely. In addition, some computers and servers left on-premise may have been shut down throughout this period. After restarting these, it is important to install all available software patches and updates.

Do make sure that all software is patched on all devices returning to the office as soon as practically possible.

Updated and active EDR

An updated EDR solution was vital to securing the laptop at home, and it is of course crucial in securing all devices in the work environment. It's not unheard of for

Unlike the rushed, unexpected manner in which many organisations sent their employees home with little opportunity for planning or preparation, the return to the office is something that can be planned for in a more organised and orderly fashion.

some employees to disable security software in order to perform certain actions on their devices.

Do ensure that all your endpoints have an active and up to date EDR solution.

Unregistered software

It is possible that some employees have installed software for their own use, perhaps because they were unable to use company resources or simply because it was more convenient than asking for the approval of the IT department.

Do make sure your EDR solution can inventory software and can report on application risk levels.

Software licence inventory

Working from home may have required certain software licences that are no longer needed when working at the office. For instance, at SentinelOne we licensed Zoom Pro for all employees as part of the great transition to remote work. For any software that employees no longer need access to, it's sensible to cancel these licences to reduce costs. The same logic applies to cloud resource usage, which may have skyrocketed while people were working from home but which now may no longer be necessary.

Do revoke unnecessary software licences and transition staff back to using resources provided on-site.

Preparing processes and procedures

In addition to inspecting devices and ensuring proper software is installed, certain processes and procedures must be implemented in order to facilitate security.

Password reset

It is possible that employees have shared their laptops and credentials with their family or friends. They may have re-used passwords on new services or devices at home, or lapsed into other insecure habits. It is advisable to reset credentials and ensure 2FA/ MFA for all company devices and software.

Do ensure that all your employees are aware of company password policy and enforce compliance.

New employees

Some companies have recruited new employees during the COVID-19 outbreak and have onboarded them remotely. Moving into the office will be a new experience for these new hires and they may need an early refresher on training that was not applicable while they were working from home.

Do ensure new hires are up to speed on additional company security policies that are pertinent to working in the office.

Maintain readiness for WFH

At some point in the future, it could be necessary to transition to work from home again, and there's always the real possibility in the near-to-mid term future that individual employees could contract the virus and need to self-isolate again.

Therefore, it is prudent to use the lessons learned from the mass transition to work from home in early 2020 and be better prepared to do it again, whether on a small scale or throughout the company. This includes having an up-to-date inventory of all IT equipment, having all company laptops installed with a modern EDR and ensuring that employees have access to company assets via VPN protected by 2fA.

Do formalise the lessons learned from this unprecedented crisis so that they can be used to help your business manage future crises with less pain.

Conclusion

Returning to the office environment might come sooner or later, but come it surely will. In order to reduce the risk and facilitate a quick return to normal operations, CISOs should consider the possibility that employees may bring threats with them when they shift back to the office desk.

Unlike the rushed, unexpected manner in which many organisations sent their employees home with little opportunity for planning or preparation, the return to the office is something that can be planned for in a more organised and orderly fashion. Prepare now to ensure the necessary processes and tools are in place before this happens. □

For more information, please visit
www.sentinelone.com

SentinelOne™

Focus on metrics to manage risk in financial services

How can security professionals help their financial services organisations move from traditional governance, risk and compliance to integrated risk management that integrates risk activities from across an organisation to enable better strategic decision making?

Eoin Keary reports

IT systems, in general, are moving towards software-defined networks and governance. From oversight and governance regarding IT networking to deployment of systems, much is software defined, and managed as such.

Governance is also moving in this direction through software-defined governance, where services such as configuration management, patching and vulnerability management orchestration are increasingly automated. Compliance dashboarding and tracking compliance metrics was the first step in measuring governance, but we're moving towards auto-configuration management and compliance monitoring via software-defined solutions.

Software-defined governance helps with integration to risk management since metrics and data can be collected and processed on a near real-time basis. This provides an overall view of risk and governance from a single standpoint, which can in turn result in rapid response and ease of oversight in an organisation in continuous flux.

Understanding and having the correct metrics certainly assists with making strategic and operational decisions quickly. Trends over time push strategy, while real-time metrics can assist with operations. Information security professionals can assist by focusing on metrics, as we can't improve what we can't measure. Many metrics of value in the information security world overlap with risk management and overarching strategy. Items such as system stability, usage downtime, vulnerability density and time to fix – to name a few – can all be used to assist with focusing one's budget on doing the right things to move the dial in a positive direction.

Information security needs to look at integration and alerting, and how these events and associated data can be correlated with other business as usual aspects of the organisation. Metrics and alerting integrations can provide strategic 'food for thought' and assist executives in considering where to allocate budget and resources. For example, a business unit with a high vulnerability count may require training or improvements to maintenance or deployment. By detection of the symptom, we can try to understand the root cause and act accordingly.

There is a wide overlap between governance, compliance and IT security if data is 'merged' in this way. We can analyse high-level trends and 'drill' deeper into the technical and root cause of symptoms, which provides us with both operational and strategic views of the same issue. The traditional method of receiving reports from internal/external consultants, tracking the discovered non-compliant issues, rinse and repeat is just way too slow to keep pace with the rate of chance in a contemporary environment.

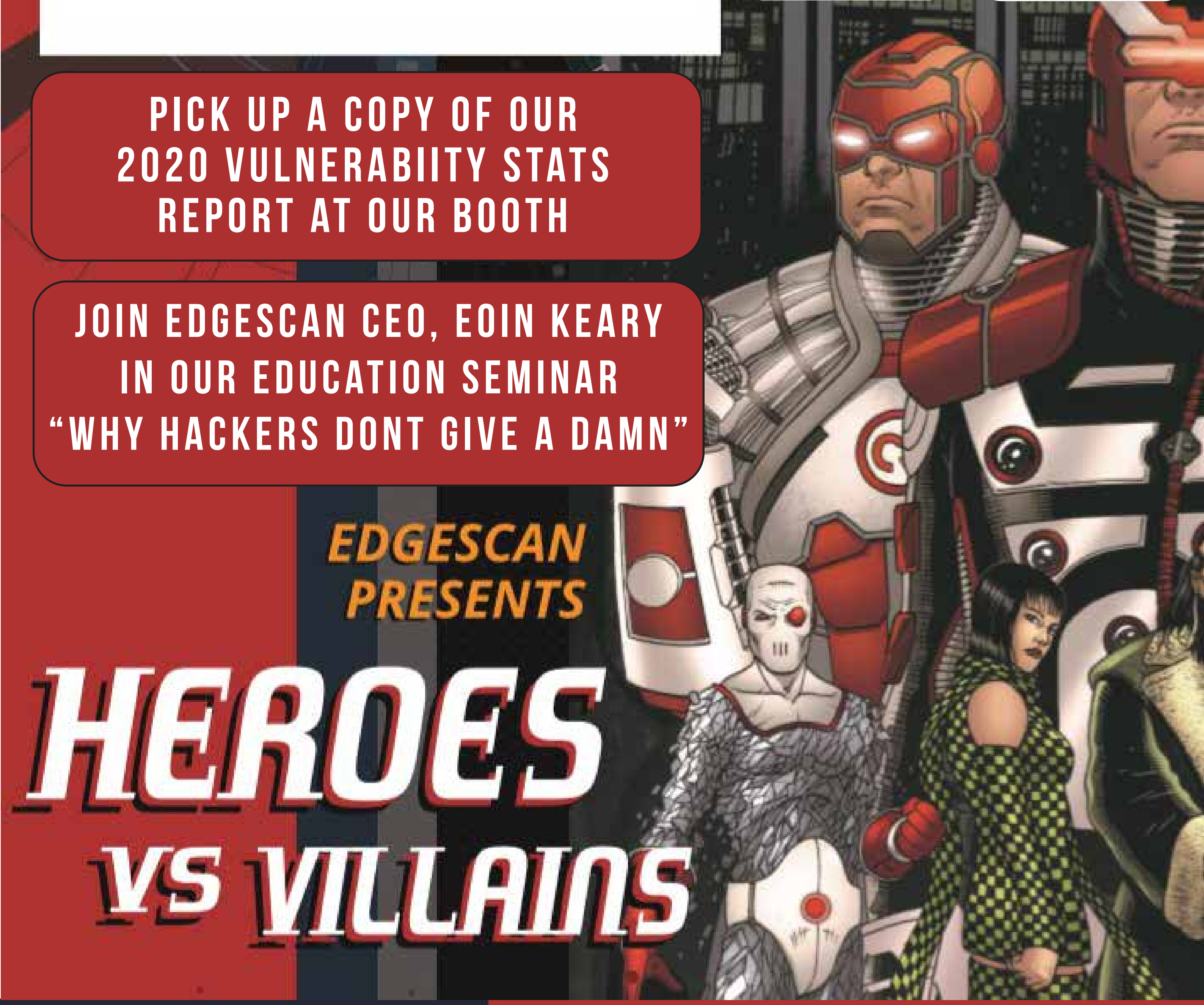
An integrated metrics-driven approach using some decent analytics can change the posture of any organisation significantly. Metrics to consider which can assist risk governance are suggested as follows:

- *Development security touchpoints and toll gates:* Gather metrics relating to security fails early on in the system development lifecycle. Earlier detection is cheaper and more effective. Root cause identification can assist with quality and compliance (and also security posture).
- *Simple fixes can result in huge dividends:* Tracking security posture of non-compliant live systems (for example, systems not configured correctly or systems which require patching). Trying to answer questions such as 'why, how, where' in terms of misconfigured or neglected systems. The measure of time-to-remediate (TTR) is a by-product of this.
- *Mean time to remediation:* Measure how quickly system vulnerabilities are being fixed and if they are being fixed at all. Many compliance requirements demand continuous improvement and evidence you are taking compliance seriously.
- *Establish asset inventory:* Automated continuous profiling can aid updating an asset inventory in near real time. Visibility and scope are a common root cause for non-compliance or breach – for example, 'We did not know that server existed…'.

The traditional approach of using siloed (standalone) tools and processes no longer works. Integrations into governance ecosystems are key to achieving an overall view of an organisation's risk landscape. □

Eoin Keary is Founder/CEO at Edgescan.

For more information, please visit **www.edgescan.com**


EDGESCAN
PRESENTS
HEROES
VS VILLAINS

Dark web monitoring: the good, the bad, and the ugly

Monitoring these sources is challenging, and few solutions have sophisticated coverage.

Digital Shadows reports

Gaining access to dark web and deep web sources can be extremely powerful – if you focus on relevant use cases. The most successful strategies we observe have clear requirements, such as fraud detection, threat monitoring, and finding exposed credentials.

However, monitoring these sources is challenging, and few solutions have sophisticated coverage. 'Deep and dark web' spans a huge range of potential sources: marketplaces, closed forums, messaging apps, and paste sites. Few companies span all these sources; fewer still have capabilities to go beyond simple scraping of sites.

Unfortunately, there is a lot of FUD (fear, uncertainty, and doubt) concerning the dark web. Iceberg analogies have been common for several years, ostensibly demonstrating the deep and dark web is significantly larger than the open web. In truth, the dark web only contributes to a small chunk of cybercrime – we must consider additional sources to get a truer sense of the threat landscape.

What is the dark web?

The dark web is an area of the internet that is only accessible with specific browser software, such as Tor or I2P. It is a web of anonymity where users' identities and locations are protected by encryption technology that routes user data through many servers across the globe – making it extremely difficult to track users.

The anonymity of the dark web makes it an attractive technology for illegal purposes. Unfortunately, gaining visibility into criminal locations is difficult: it requires specialised knowledge, access to closed sources, and technology that's capable of monitoring these sources for misuses of your data.

However, let's first dispel some misconceptions about the dark web.

- Assumption 1: *The dark web is synonymous with the criminal internet.* While the dark web is home to lots of crime, it also hosts many legitimate companies like *New York Times* and Facebook who offer Tor-based services, as well as generally benign content. The dark web is not synonymous with cybercrime.
- Assumption 2: *The dark web is the same thing as the deep web.* To clarify, the deep web is broadly defined as anything that is not indexed by traditional search engines. Unsurprisingly, the deep web is also home to criminality – but so too is the clear web. The dark web does not monopolise cybercrime.

Simply because it isn't accessible by a traditional search engine, it does not mean the deep web is necessarily interesting. Most of the data on the deep web is mundane or 'normal'; for example, email or Facebook accounts might fall under this definition as they require registration to see the content. While some deep and dark websites are valuable sources, you need to know what you're looking for, otherwise it's easy to waste time and resources.

The fight over dark web marketplaces

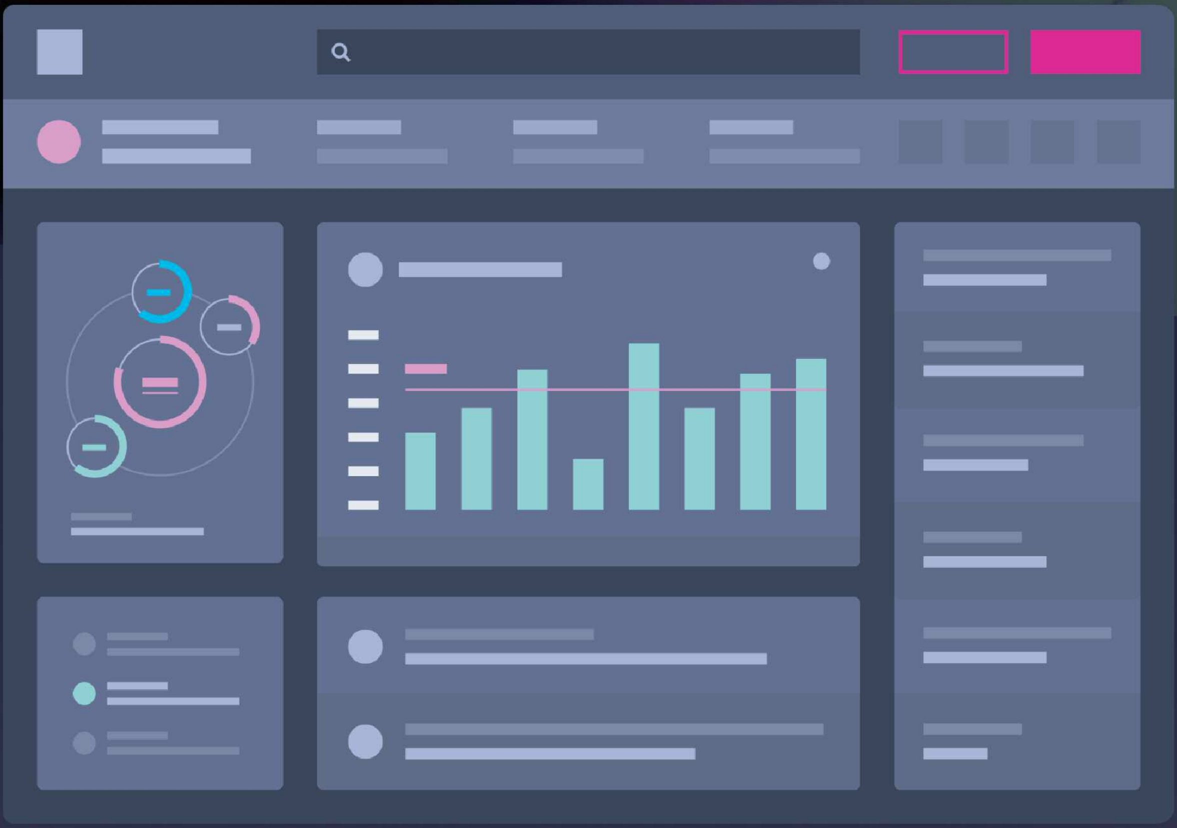
In July of 2017, United States and Dutch law enforcement launched Operation Bayonet where they seized and disabled two of the most prominent dark web marketplaces, AlphaBay and Hansa. United States Attorney General Jeff Sessions described the operation as: *"one of the most important criminal investigations of the year…because of this operation, the American people are safer – safer from the threat of identity fraud and malware, and safer from deadly drugs."*
Before Operation Bayonet, English-speaking cybercriminal activity mainly took place on online dark web marketplaces such as Alpha Bay and Hansa, where hundreds of thousands of vendors and buyers were doing an estimate of over $1 billion in illegal trade.

Law enforcement action didn't stop there – on May 7, 2019 an internationally coordinated operation led to the takedowns of two more dark web marketplaces, Wall Street Marketplace and Valhalla Marketplace (Silkkitie). In the same operation, law enforcement simultaneously disabled one popular dark web news source and review page, DeepDotWeb. DeepDotWeb did not sell contraband; instead, administrators profited from promoting criminal sites and marketplaces through affiliate links. Its recent seizure displayed law enforcement's willingness to target more of the illegal trade network beyond the marketplaces – including promoters and launderers. □

You can find the full article here:
www.digitalshadows.com/blog-and-research/dark-web-monitoring-the-good-the-bad-and-the-ugly/

For more information, please visit
www.digitalshadows.com

digital shadows_



Forthcoming events

e-crime & cybersecurity NORDICS VR

23rd September 2020
Online

e-crime & cybersecurity MID-YEAR VR

15th October 2020
Online

e-crime & cybersecurity MIDDLE EAST VR

21st October 2020
Online

e-crime & cybersecurity SPAIN VR

17th November 2020
Online

e-crime & cybersecurity BENELUX VR

1st December 2020
Online

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

Sponsors and exhibitors

CrowdStrike | Principal Sponsor

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.
Qualifying organisations can gain full access to Falcon Prevent™ by starting a free trial.

Learn more at www.crowdstrike.com

Gigamon | Strategic Sponsor

The Gigamon Visibility and Analytics Fabric enables you to stay competitive and secure by optimising your security tools providing visibility, availability and security solutions that power the highest levels of consumer experience and innovation.

Gigamon is the first company to deliver complete network visibility and analytics on all information-in-motion, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyse network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organisation to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

Gigamon has been awarded over 75 technology patents and enjoys industry-leading customer satisfaction with more than 3,000 organisations, including 80% of the Fortune 100.

Seven of the top 10 global banks rely on Gigamon as well as hundreds of other banks, insurers, credit unions, and regulatory authorities.

Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you, please visit www.gigamon.com

LogRhythm | Strategic Sponsor

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyber-threats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) framework serves as the foundation for the AI-enabled Security Operations Centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

For more information, please visit logrhythm.com

Menlo Security | Strategic Sponsor

Menlo Security protects organisations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

For more information, please visit www.menlosecurity.com

Okta | Strategic Sponsor

When technology is able to act on a consistent stream of information about a person, and still keep that information safe, it can do great things. Okta is built on that understanding. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections. Our platform securely connects companies to their customers and partners. As the foundation for secure connections between people and technology, Okta helps companies fulfill their missions as quickly as possible. Today, thousands of organisations trust Okta to help them work faster, boost revenue, and stay secure.

For more information, please visit www.okta.com

Proofpoint | Strategic Sponsor

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com

SentinelOne | Strategic Sponsor

SentinelOne is the only cybersecurity solution encompassing AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform. With SentinelOne, organisations gain full transparency into everything happening across the network at machine speed – to defeat every attack, at every stage of the threat lifecycle.

To learn more visit www.sentinelone.com

Cybereason | Education Seminar Sponsor

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Founded by elite intelligence professionals born and bred in offence-first hunting, Cybereason gives enterprises the upper hand over cyber-adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioural patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface.

Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.

For more information, please visit www.cybereason.com

Digital Shadows | Education Seminar Sponsor

Digital Shadows makes threat intelligence work for organisations of all sizes. Companies no longer need to invest a disproportionate amount of resource to get real value out of threat intelligence. Our industry-leading SearchLight service delivers relevant threat information that allows organisations to quickly understand and act on their external exposure minimising their risk without hiring additional headcount.

Get started today and see how SearchLight can protect your digital risk, visit www.digitalshadows.com/fr

Edgescan | Education Seminar Sponsor

Edgescan is an award-winning fullstack vulnerability assessment solution that gives our clients the tools needed to control, understand, prioritise and mitigate cybersecurity risks on a continuous basis. The solution is a cloud-based managed service, it provides a combination of technology and human expertise to supply on-demand, verified security risks.

Edgescan is one of a few cybersecurity companies that enables enterprises to secure and be proactive in their defence of their digital businesses. From application and host development to production deployment, and from the desktop to API to cloud to mobile devices, they secure the web applications and infrastructure that people rely on in their personal and professional lives.

For more information, please visit www.edgescan.com

Egress | Education Seminar Sponsor

Our vision is for a connected world in which people communicate efficiently and securely. To achieve this, we provide human layer security to protect individual users and stop breaches before they happen. Our patented technologies are built using leading-edge contextual machine learning and powerful encryption that mitigate modern risks in ways that other solutions simply can't achieve.

Today, we provide intelligent email security and collaboration solutions that prevent accidental and intentional breaches, protect sensitive data, and equip CISOs and their teams with the detailed reporting required for compliance purposes.

Egress is headquartered in London, with regional offices in the UK, the US, Canada and the Netherlands.

For more information, please visit www.egress.com

Illumio | Education Seminar Sponsor

Illumio enables organisations to realise a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data centre or cloud.

Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite trust Illumio to reduce cyber-risk.

For more information, visit www.illumio.com/what-we-do and: engage with us on Twitter; follow us on LinkedIn; like us on Facebook; read our blog; subscribe to our YouTube Channel

IntSights | Education Seminar Sponsor

IntSights is revolutionising cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralise cyber-attacks outside the wire. Our unique cyber reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defence has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo.

For more information, please visit intsights.com

Kaspersky | Education Seminar Sponsor

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help over 270,000 corporate clients protect what matters most to them.

For more information, please visit www.kaspersky.com

ThreatConnect | Networking Sponsor

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralise your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place.

To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit www.ThreatConnect.com

Veracode | Networking Sponsor

Veracode gives companies a comprehensive view of security defects so they can create secure software and ensure the software they are buying or downloading is free of vulnerabilities. As a result, companies using Veracode are free to boldly innovate, explore, discover, and change the world.

With its combination of automation, integrations, process, and speed, Veracode helps companies make security a seamless part of the development process. This allows them to both find and fix security defects quickly so that they can use software to achieve their missions.

Companies collaborating with Veracode are able to create comprehensive application security programs that focus on reducing risk, achieving compliance with industry regulations and customer requirements, increasing the speed of secure software delivery, and making secure software a competitive advantage.

The Veracode Verified Program allows customers to provide attestation of their secure development processes, demonstrating their commitment to creating secure software.

Securing software is a priority for any company looking to change the world. With Veracode, companies can start securing their software immediately, without the need for additional staff or equipment.

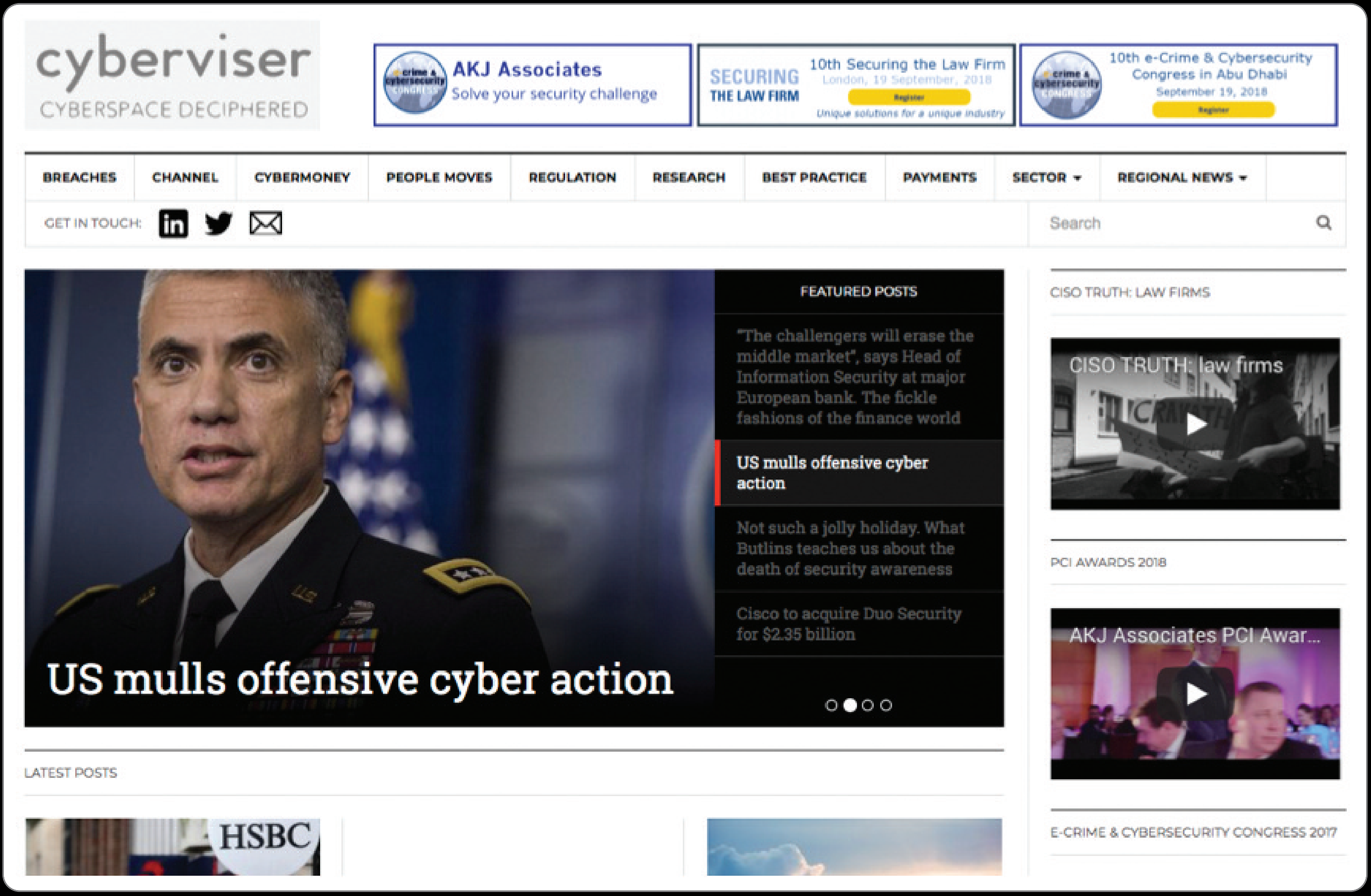
Learn more at www.veracode.com, on the Veracode blog and on Twitter

www.cyberviser.com

You know AKJ Associates for its 20-year record of market-leading conferences and events in cybersecurity and compliance. Under the e-Crime Congress, Securing the Law Firm and PCI London brands, we have consistently tried to get ahead of the trends shaping your market and careers, instead of rehashing the same old ideas.

We were first to bring CFOs and institutional investors to you, to reveal what business and stakeholders really think about cyber. We were at the forefront of understanding the collision of cybersecurity, operational risk and compliance. And we have not been afraid to confront cybersecurity's many inconvenient truths.

To expand the resources we provide to you, we have launched a website to continue our mission of delivering independent thought leadership, news and views.



cyberviser
CYBERSPACE DECIPHERED

AKJ Associates
Solve your security challenge

SECURING THE LAW FIRM
10th Securing the Law Firm
London, 19 September, 2018
Unique solutions for a unique industry

10th e-Crime & Cybersecurity Congress in Abu Dhabi
September 19, 2018

US mulls offensive cyber action

FEATURED POSTS

"The challengers will erase the middle market", says Head of Information Security at major European bank. The fickle fashions of the finance world

US mulls offensive cyber action

Not such a jolly holiday. What Butlins teaches us about the death of security awareness

Cisco to acquire Duo Security for $2.35 billion

LATEST POSTS

CISO TRUTH: LAW FIRMS

CISO TRUTH: law firms

PCI AWARDS 2018

AKJ Associates PCI Awar...

E-CRIME & CYBERSECURITY CONGRESS 2017

www.cyberviser.com brings you:

- ✓ **Research and data:** AKJ Associates' proprietary data and conclusions gathered from security professionals around the globe. Our first project, 'Who Secures the UAE' is now live.
- ✓ **News and comment:** the most significant news stories with interpretation and comment from AKJ editors and the market.
- ✓ **Best practice:** what works and what doesn't, direct from leading end-users and security practitioners.
- ✓ **Regulation:** the latest global news on regulation and compliance, cross-sector, cross-region.
- ✓ **People:** who is firing, who is hiring and what are they paying? CISO profiles and interviews.
- ✓ **Vendors:** start-ups, funding, M&A, new solutions and new technologies.

SECURING FINANCIAL SERVICES VR

AGENDA

08:00 Login and registration

09:05 Chairman's welcome

09:10 **Managing working from home to protect customers during COVID-19**

Sally Webmark-Taylor, Head of Financial Crime Risk Name Screening, Aviva

- Keeping 'Business as Usual' going: helping customers during the health crisis
- Coping with working from home and managing financial crime risks
- Financial crime, fraud and security – Covid threats and challenges to Aviva and its customers

09:30 **e-Crime does pay: the new reality of ransomware attacks!**

Zeki Turedi, Lead Global Technical Threat Advisor, CrowdStrike

- What does ransomware mean to you? An annoyance that can easily be fixed, an automated attack, or a tool used by a human actor to take your business to ransom?
- Learn about the tactics, techniques and procedures e-Crime actors have been using to benefit
- How can finance organisations better arm themselves against these evolving attacks

09:50 **On the money: SIEM in financial services**

Kevin Eley, Enterprise Client Director, LogRhythm

- According to the Verizon Data Breach Investigations Report 2020, organised criminal gangs are the top threat actor for the financial services, and financial gain is the main motivation
- How a SIEM can be leveraged to detect and respond to such attacks and provide defence for financial service organisations
- The importance of continual alignment between SIEM and the threat landscape
- The criticality of teaming with the business for success

10:10 **Information security – could it be child's play?**

Lorraine Dryland, Chief Information Security Officer, First State Investments

- ADAPTING: Morphing policy and standards
- COMMUNICATION & COLLABORATION: Using goals to talk to the business
- SECURITY CONSCIOUS CULTURE: Speak the language of employees and make learning interactive
- DEFENCE for GLOBAL BUSINESS: Don't get trapped in complexity

10:30 **Education Seminars | Session 1** — **See pages 28 to 30 for more details**

CrowdStrike	Cybereason	Kaspersky
Navigating the current threat landscape in the financial sector	**EventBot: a new mobile banking trojan is born**	**Cybersecurity in enterprise blockchain. Best practice, experience, tips**
Josh Burgess, Lead Global Technical Threat Advisor, CrowdStrike	**Pavel Mucha,** Systems Engineer, Cybereason	**Maxim Denizhenko,** Business Development Lead Enterprise Blockchain Security, Kaspersky

11:00 Networking break

11:30 **Protecting the digital customer**

Martin Farrelly, Information Security Architecture and Strategy, Allied Irish Bank, and
Denis Heneghan, Cyber Security Outreach Manager, Allied Irish Bank

- The community of branch-based customers have now gone digital
- The rise in phishing, smishing and multi-channel fraud
- Methods of educating customers on security best-practice
- The increase in reliance on remote banking services: tackling the security challenges

11:50 **The threat hunting challenge: detect, prevent, respond and hunt – every second, every day**

Jan Tietze, Director Security Strategy EMEA, SentinelOne

- Learn how Endpoint Detection & Response (EDR) technologies pick up where antivirus technologies leave off
- Understand why EDR should be an essential part in every Endpoint Security Strategy
- Learn how EDR auto-immunises the endpoints against newly discovered threats and provides rich forensic data, mitigate threats and performs network isolation
- Demo

12:10 **Securing financial services in the age of digital transformation**

James Easton, Senior Solutions Architect, Gigamon

- The old cliché "you can't protect against what you can't see" holds as true for cybersecurity as for physical security
- Financial services organisations have been at the forefront of digital transformation and have realised that, without the right planning and tools, security can become a casualty in this process
- Gigamon discusses these issues and highlights ways you can protect yourselves and your customers in the digital transformation process

12:30 **Zero trust internet – moving beyond 'almost safe'**

Jonathan Lee, Sr. Product Manager, Menlo Security

- Enterprise spending on cybersecurity continues to go up, yet they keep getting infected again and again and again
- Digital transformation is accelerating the adoption of cloud-based apps and services, rendering legacy security architectures obsolete
- How we need to invert our thinking from being app/data centric to a cloud-based, user centric approach
- Can we move beyond good vs. bad and 'almost safe' to zero trust?

12:50 **Education Seminars | Session 2** **See pages 28 to 30 for more details**

Digital Shadows

Dark web digest: gaining valuable threat intelligence from cybercriminal forums

Alex Guirakhoo, Team Lead, Threat Researcher, Digital Shadows, and **Kacey Clark,** Team Leader Cyber Intelligence Analyst, Digital Shadows

Edgescan

Enemy at the gates…why traditional vulnerability management has failed. AKA 'Why hackers don't give a damn'

Eoin Keary, CEO & Founder, Edgescan

IntSights

Protecting the business with intelligence from outside the wire

Michael Owen, Head of Systems Engineering UK&I, IntSights Cyber Intelligence BV

13:20 Lunch and networking break

14:10 **Who secures the financial services?**

Simon Brady, Managing Editor, AKJ Associates

- A broad and comprehensive overview of cybersecurity trends within the financial services informed by AKJ Associates' original research
- From the trading floor to the employee home; how a crisis has transformed our understanding of operational resilience throughout the organisation and the supply chain
- Accelerated digitisation and an expanded attack surface. Where are the major vulnerabilities in the financial services?

14:30 **You're only supposed to blow the bloody doors off! Defending against the next generation of bank jobs**

Max Faun, EMEA Head of Business Consulting, Okta

- The finance sector finds itself at the centre of persistent, sophisticated hacks and attacks just as customers are demanding the same frictionless experience they have with the world's largest online retailers
- This session re-examines traditional security approaches and to these challenges and explores how Identity and Access Management must now take centre stage to defend against future security attacks
- Topics include: Credential theft and compromise; Gaps in the security landscape; The missing ingredient, Identity; Adaptive multi-factor authentication; Strategic direction for identity-driven security

14:50 **A people-centric approach to managing the risk of insider threats**

Rob Bolton, Senior Director, Insider Threat Management, Proofpoint

Insider threats are on the rise. According to a new research study from Ponemon, the financial services sector experienced the highest total average annual cost to contain insider threat incidents, at $14.50 million a 20.3% increase since 2018. In this session learn:

- Why insider threats are unique, and require context around both user and data activity
- How to gain visibility into the different types of insider threats your organisation faces
- How a modern people-centric approach can help you manage the risk of insider-led data breaches
- The types of insider threat profiles and how to address them
- How to reduce response time by accelerating investigations

15:10 **Education Seminars | Session 3** **See pages 28 to 30 for more details**

CrowdStrike

Navigating the current threat landscape in the financial sector

Josh Burgess, Lead Global Technical Threat Advisor, CrowdStrike

Egress Software Technologies

Solving your #1 security risk

Fahim Afghan, Senior Product Marketing Manager, Egress Software Technologies

Illumio

Why you should implement micro-segmentation for regulatory compliance

Raghu Nandakumara, Field CTO EMEA, Illumio

15:40 Networking break

16:00 **Using standardised digital identification and electronic signatures in data governance**

Andrew Fleming, Global Compliance MI Senior Risk Reporting Manager, HSBC

- Reducing financial crime risk to the business through bio metrics
- Enhance the customer experience across different internal divisions
- Overlay the personalised data across transaction monitoring to reduce false positives and improve alert generation

16:20 **Data management in the financial sector Q&A**

Liz Banbury, Head of Information and Cyber Policy, Standard Chartered Bank

- What are your critical assets, and how is your data managed?
- What has the WFH period taught you about your data governance methodology?
- How strong cyber risk policy can become core to operational resilience strategy
- Securing a global financial institution

16:40 **EXECUTIVE PANEL DISCUSSION** **Fintechs in 2020: Security and financial crime under lockdown**

Like any organisation, fintechs and digital banks have had to transform their operations to adapt to C19 and WFH. Having often been portrayed as being more naturally suited to security and financial crime prevention due to their digital nativeness, smaller size, and lack of silos and legacy systems, has security flourished in the new environment? And as larger financial institutions witness migration from branch banking to virtual customer interaction, are fintechs leading the way?

Matt Bryant, CISO, Monese

Andrew Mason, Head of Financial Crime, Bó

17:00 Closing remarks

17:10 Networking

17:30 Conference close

Education seminars

Throughout the day a series of education seminars will take place as part of the main agenda. Delegates will be able to choose to attend any of the seminars, all of which will provide vendor-neutral, hands-on advice. Seminars within each session run concurrently.

Session 1: 10:30–11:00

CrowdStrike

SESSION 1
10:30–11:00

Navigating the current threat landscape in the financial sector

Josh Burgess, Technology Strategist, EMEA, CrowdStrike

At CrowdStrike, we put a lot of time and effort into understanding intelligence trends and profiling the attackers behind attacks. We even name our attackers individually to give them identity – since we spend so long trying to learn all about them! One thing we have learnt is that nation-state and criminal threat actor groups can have a particular threat to the financial sector. In this session, we will review associated threat actor capabilities and infrastructures as well as their tactics, techniques and procedures.

- Discuss specific implications to the financial sector
- How current events (such as the Covid-19 pandemic) are influencing cybersecurity threats to the financial sector and what the latest attack types are
- Understand mitigation strategies to stop these attacks
- Truly 'know' the adversary in order to properly build the best defences to stop the actor and not just the malware

Cybereason

SESSION 1
10:30–11:00

EventBot: A new mobile banking trojan is born

Pavel Mucha, Systems Engineer, Cybereason

The Cybereason Nocturnus team has been investigating a new type of Android malware dubbed EventBot, which was first identified in March 2020. This malware appears to be newly developed with code that differs significantly from previously known Android malware. EventBot is under active development and is evolving rapidly; new versions are released every few days with improvements and new capabilities.

In this session you will learn:

- How Cybereason classifies EventBot as a mobile banking trojan and infostealer based on the stealing features discussed in this research. It leverages webinjects and SMS reading capabilities to bypass two-factor authentication, and is clearly targeting financial applications
- How EventBot targets users of over 200 different financial applications, including banking, money transfer services, and crypto-currency wallets
- Introducing a new offering, Cybereason Mobile, that strengthens the Cybereason Defense Platform by bringing prevention, detection, and response capabilities to mobile devices. With Cybereason Mobile, our customers can protect against modern threats across traditional and mobile endpoints, all within a single console

Kaspersky

SESSION 1
10:30–11:00

Cybersecurity in enterprise blockchain. Best practice, experience, tips

Maxim Denizhenko, Lead Business Development, Enterprise Blockchain Security, Kaspersky

At the session you will get a recap about blockchain technology in enterprises, overview of the threat landscape and corresponding cybersecurity measures. We will talk about best practices from real life use cases based on our experience.

In this presentation we will discuss:

- Enterprise vs Crypto
- Main attacks in corporate blockchains
- Enterprise blockchain case studies
- How to secure trust?

SECURING FINANCIAL SERVICES VR

Session 2: 12:50–13:20

Digital Shadows

SESSION 2
12:50–13:20

Dark web digest: gaining valuable threat intelligence from cybercriminal forums

Alex Guirakhoo, Team Lead, Threat Researcher, Digital Shadows, and **Kacey Clark,** Team Leader Cyber Intelligence Analyst, Digital Shadows

In our team's latest dark web findings, we have observed notable changes in criminal forum activity and trends. Dark web forums harbour a dynamic environment for criminals looking to buy or sell compromised data, zero-day exploits, and system accesses. This environment and the findings associated with it can uncover how criminals may use your individual or organisational information on the dark web, leading to further compromise, profit loss, data loss, or reputational damage. During this session, we will cover the risk impact of dark web findings, explore the evolution of dark web forums, and trends observed across platforms.

Key takeaways:

- Insights into current dark web trends
- Tactics and techniques attackers use to collect or share your data
- How to gain visibility into your organisation's dark web risk
- Strategies for fortifying your defences and mitigating dark web risks

Edgescan

SESSION 2
12:50–13:20

Enemy at the gates…why traditional vulnerability management has failed. AKA 'Why hackers don't give a damn'

Eoin Keary CISSP CISA, CEO & Founder, Edgescan

- Why traditional vulnerability management has failed in keeping us secure
- What it takes to deliver vulnerability management at scale and how can we keep pace with the speed of development
- What is the trade-off between speed and accuracy and why is this acceptable?
- We shall also cover off highlights of the Edgescan Vulnerability Stats report 2020 focusing on the most common vulnerabilities and what it means to deliver a robust cybersecurity programme for any enterprise

IntSights

SESSION 2
12:50–13:20

Protecting the business with intelligence from outside the wire

Michael Owen, Head of Systems Engineering UK&I, IntSights Cyber Intelligence BV

Threats exist well before the targets are aware of them. In this fast moving environment, time is your most valuable asset. Understanding that a threat exists, or has growing potential before the attack has been weaponised, can be a major element of defence in your arsenal against the attackers.

This presentation will cover how intelligence gathered from outside your business can help you better protect it. In this 25 minute presentation elements such as what the problem is, how we can use this intelligence and what it can be used to protect against as well as where and how we find it in the first place, will be discussed and examples given.

What the attendees will learn:

- Where the problem exists and how it manifests itself
- The type of intelligence that can prove useful to providing an early warning of attacks
- How that intelligence can be used to mitigate the threat

SECURING
FINANCIAL SERVICES
VR

Session 3: 15:10–15:40

CrowdStrike

SESSION 3
15:10–15:40

Navigating the current threat landscape in the financial sector

Josh Burgess, Technology Strategist, EMEA, CrowdStrike

At CrowdStrike, we put a lot of time and effort into understanding intelligence trends and profiling the attackers behind attacks. We even name our attackers individually to give them identity – since we spend so long trying to learn all about them! One thing we have learnt is that nation-state and criminal threat actor groups can have a particular threat to the financial sector. In this session, we will review associated threat actor capabilities and infrastructures as well as their tactics, techniques and procedures.

- Discuss specific implications to the financial sector
- How current events (such as the Covid-19 pandemic) are influencing cybersecurity threats to the financial sector and what the latest attack types are
- Understand mitigation strategies to stop these attacks
- Truly 'know' the adversary in order to properly build the best defences to stop the actor and not just the malware

Egress Software Technologies

SESSION 3
15:10–15:40

Solving your #1 security risk

Fahim Afghan, Senior Product Marketing Manager, Egress Software Technologies

Employees sending emails in error is the top cause of security incidents reported to Information Commissioner's Office. And large-scale remote working isn't helping: the COVID-19 pandemic has resulted in more information being shared by email than ever before – significantly increasing the risk of a security incident. For financial services firms, this risk is aggravated by high-pressure and fast-paced environments. So, how can CISOs and their security teams ensure employees send the right email to the right recipients, with the right level of security, while maintaining efficiency during remote working?

Join Egress Senior Product Marketing Manager, Fahim Afghan as he explains why human-activated email data breaches are your most significant security risk, examines the most common causes of these incidents, and looks at how contextual machine learning can eliminate this threat.

Key learning points:

- Understand the changing risk from human-activated email data breaches and identify the common causes of these incidents in your firm
- See how contextual machine learning can understand individual employee's email usage to prevent these incidents and protect data
- Learn how intelligent email security can increase effective TLS usage for enhanced data protection and usability
- Identify the areas where human layer security and contextual machine learning can improve data security in your firm

Illumio

SESSION 3
15:10–15:40

Why you should implement micro-segmentation for regulatory compliance

Raghu Nandakumara, Field CTO EMEA, Illumio

Whether a sophisticated adversary or a fast-spreading ransomware attack, a common element across all high-profile breaches is lateral movement – the ability for malicious actors or malware to traverse a network.

This session will:

- Explain Illumio's approach to micro-segmentation focuses on blocking any network communications that are not explicitly authorised, stopping an adversary or malware in its tracks
- Prove the value of micro-segmentation in how it stops an adversary or malware in its tracks
- Discuss how a host-based approach can be used to help achieve compliance with industry standards. □

Speakers and panellists

Fahim Afghan

Senior Product Marketing Manager, Egress Software Technologies

Fahim has spent his entire career building products and value propositions that support critical customer objectives. Having joined Egress as Senior Product Marketing Manager in 2019, he is currently driving revenue growth by leading on the go-to-market strategy, as well as product positioning and launch. Before joining Egress, Fahim served as Head of Product Marketing at GlobalData plc, a leading data and analytics company headquartered in London.

Prior to that he was Vice President of Content at SCM World (now Gartner Supply Chain), where he generated thought-leading content and research to help supply chain leaders innovate and deliver profit. Fahim is a keen guitarist, having played for the best part of three decades, while he also likes to ruin a nice walk with a round of golf. He lives in London with his wife and son.

Liz Banbury

Head of Information & Cyber Policy, Standard Chartered Bank

Liz Banbury spent approximately 15 years working in technology within the financial industry and started out in JPMorgan working in the back office settlements systems and progressed to release/environment management. She has now been in the information security space for 6+ years firstly with ANZ Bank as the Security, Risk and Compliance Manager on a global online and mobile banking infrastructure project, which progressed to a role as the Regional Portfolio Manager for Information Security & Technology Risk within the Information Security Office and currently with Standard Chartered heading up the Information & Cyber Security Policy. She is passionate about what she does and particularly interested in people and the impact that behaviour and culture has on our security holistically. Cybersecurity is a very interesting, dynamic, fast moving, fast changing area where she feels that each individual should have a certain basic level of knowledge in the key threats we face and controls that need to be put in place to safeguard themselves and their assets both at home and in the workplace. She is CISSP (Certified Information Systems Security Professional) certified and has been a member of (ISC)² since 2016 and as a progression of that passion and interest in how people and technology interact joined the (ISC)² London Chapter as one of the founding officers when it was originally incorporated in January 2018. Since leaving school, she has been fortunate enough to have been able to travel a fair amount and has spent 20 years living in Asia, first in Hong Kong and more recently in Singapore, returning to London in June 2017.

Rob Bolton

Senior Director, Insider Threat Management, Proofpoint

Rob leads the Insider Threat Management business unit for Proofpoint's international markets. The frequency, cost, and complexity with security events that involve an insider is increasing each year. Rob and his teams are working with customers and partners alike to provide a level of visibility and control around the risks associated with insider threats, with a focus on helping companies protect against risky behaviour, protect their data and IP, and reducing the investigation cycles. For almost 23 years, Rob has been working alongside some of the most recognisable companies in the world, helping to solve some of the most critical security and technological issues. Originally from Washington, DC, now residing in London, Rob is a published author international sales and operations leader.

Matthew Bryant

CISO and Data Protection Officer, Monese

Matthew has a career spanning 15 years in the design, delivery and management of secure systems for the private sector and UK Government & intelligence agencies.He is currently the Chief Information Security Officer (CISO) and Data Protection Officer at Monese, a digital challenger banking service.

Prior to this, he was the CISO of 3i, a FTSE 100 private equity company, in addition to providing consultancy services to multinational organisations in the finance, investment and professional services sectors. At the communications regulator Ofcom, Matthew led investigations into major security breaches at multinational UK-based PLCs on behalf of UK regulators. He also represented the UK on EU security working groups and at European Network and Information Security Agency pan-European security initiatives. Matthew is a Chartered Engineer, a Certified Information System Security Professional (CISSP) and the co-author of several legally mandated UK and European security standards.

Josh Burgess

Lead Global Technical Threat Advisor, CrowdStrike

Josh Burgess has over 10 years of cyber-threat analysis and mitigation experience, holding multiple positions in the intelligence community, the U.S. Department of Defense and the financial sector. In the majority of his roles, he has served as the technical lead Threat Intelligence Officer for large security operations centres (SOCs), advising on the latest threats to ensure a sound security posture. As the Lead Technical Strategic Advisor at CrowdStrike, Josh applies his experience in actioning both short-term tactical and long-term strategic intelligence data and reporting for customers.

Kacey Clark

Team Lead Cyber Intelligence Analyst, Digital Shadows

Kacey is a Team Lead Cyber Intelligence Analyst at Digital Shadows, leading a team of analysts in providing client-facing threat intelligence reporting to add context to potential digital risks. After receiving a Bachelor of Science degree in Psychology from University of Texas in Dallas, Kacey began working in talent acquisition. In her role, she partnered with government agencies and specialised in defence and intelligence contracting within the information security vertical. After working on the recruiting side, she decided to take a leap into the practitioner side and landed a job with Digital Shadows' US analyst team, which she now leads. Kacey is passionate about data privacy, open-source intelligence, and tracking down the bad guys.

Maxim Denizhenko

Lead Business Development, Enterprise Blockchain Security, Kaspersky

Maxim has been working in the information security and blockchain spheres since 2014 and has over 15 years' experience in IT business development around the world. At Kaspersky, he manages enterprise-grade blockchain security services, analysing trends in the practical uses of blockchains, evaluating the potential benefits and risks they can bring enterprises, while proactively offering the best comprehensive security solutions.

Lorraine Dryland

Chief Information Security Officer, First State Investments

Lorraine is the current Global CISO at First State Investments. She is a motivated, highly capable technology and cybersecurity professional with deep knowledge and skills in cyber-intelligence and investigations. Lorraine's background offers both an operational and strategic skill set, ranging from the management of complex cyber-dependent operational activity to the design, implementation and maturing security strategy including leading operational security for large organisations. Lorraine has held senior roles at a range of organisations including: Department of Work & Pensions, Vodafone, Bank of England and the National Crime Agency (NCA). Lorraine also has a master's degree in Forensic Computing and Cyber Crime Investigation.

James Easton

Senior Solutions Engineer UK & Ireland, Gigamon

James has been working in the networking industry since the early 90s building Cisco appliances and has worked at various network and security service providers and manufacturing companies. James has a wealth of experience in assisting organisations in improving their network and security posture ranging from providing initial consultation right through to full implementation of network and security solutions and helping businesses reduce risk, costs and optimise their networks. James has been with Gigamon for two years and enjoys motorsport, fishing, golf and travelling.

Kevin Eley

Enterprise Client Director, LogRhythm

Kevin leads the financial services sector in the UK helping information security teams improve their capabilities to detect and respond to cyber-attackers on their network through the introduction of innovative technology. He cares deeply about ensuring the teams he works with achieve their goals and gain the improvements they seek. He primarily works with financial services organisations and has worked with some of the largest enterprises in the

UK. He is very interested in all aspects of cyber and its implications on society.

Martin Farrelly

Information Security Architecture and Strategy, Allied Irish Bank

Martin Farrelly is currently a key senior member of the Information Security Architecture and Strategy Team at Allied Irish Bank, a position he has held since August 2016. In this role, he is responsible for a number of aspects of the bank's cybersecurity strategy and infrastructure, including: regular analysis of the threat landscape and mitigation strategies, advising business stakeholders on the appropriate control set in respect of new/emerging business initiatives, collaborating on digital security programmes underpinning AIB's information security strategy and oversight of the implementation of key security initiatives. Martin is also involved in the ongoing control testing programme to provide assurance to the business that the information/cybersecurity programme is delivering the expected outcomes and underpinning the bank's core values. Before AIB, Martin held a number of senior positions in IT risk management, business continuity and disaster recovery across a number of sectors.

Max Faun

EMEA Head of Business Consulting, Okta

Max Faun leads Okta's European Business Consulting Practice. Prior to joining Okta he worked at Accenture, advising Global 2000 clients across numerous industry groups on strategic decisions. He is passionate about the business implications of modern identity from a financial, security and user productivity perspective as well as wider technology trends. Max holds an MA in Intelligence and Security as well as a BA in International Relations.

Andrew Fleming

Global Compliance MI Senior Risk Reporting Manager, HSBC

Andrew Fleming was a career detective with the Metropolitan Police investigating international fraud, money laundering, terrorist financing and cybercrime in partnership with regulatory and investigatory bodies from around the globe. During this time, he took on cybercrime, fraud and money laundering and in the process identified funds being used to finance terrorism. In the private sector, Andrew has worked with a number of banks and private bodies managing and investigating transaction monitoring, money laundering, fraud and sanctions and addressing the risk issues attached to each. He has also provided training to governments, public sector bodies and private entities on terrorist financing, money laundering, fraud risk and cybercrime.He is passionate about financial crime and the need to embrace AI and machine learning to counter the threats of cybercrime and the growth of criminal financial activities.

Alex Guirakhoo

Team Lead, Threat Researcher, Digital Shadows

Alex Guirakhoo is a Team Lead – Threat Researcher at Digital Shadows. Having joined the company in mid-2016, he primarily conducts research and provides analysis on cybersecurity trends. Alex earned his master's degree in Intelligence and International Security from King's College London, and holds a bachelor's degree in Politics and International Relations from the University of Kent. His interests include the intersect between global politics and the cyber sphere, as well as all things OSINT and Shiba Inu.

Denis Heneghan

Cyber Security Awareness Manager, Allied Irish Bank

Denis is an experienced financial crime investigator and cybersecurity professional. He is currently the Cyber Security Awareness Manager at Allied Irish Bank, a position he's held since 2016. Denis has a wealth of experience in leading investigation teams in payment fraud, commercial fraud, cybercrime and AML, both in law enforcement and financial industry roles and he has managed a number of IT change projects to reduce financial crime risk and exposure. Denis worked in fraud prevention at AIB from 2012–2015 as part of the legal, compliance and risk functions. In this role, he managed the group fraud prevention policy, framework, initiatives and training. Prior to this, Denis was Detective Inspector at Garda Bureau of Fraud Investigation. In this role, he managed the national unit responsible for the investigation of payment card fraud and counterfeit currency and was the national police representative to the European Commission and Europol for these crime types.

Eoin Keary

CISSP CISA, CEO & Founder, Edgescan

Eoin Keary is the Founder and CEO of Edgescan and recently secured investment funding from Ireland's largest growth capital investor, BGF. With 20 years of software development and security experience, he is a veteran of the cybersecurity industry, previously Global Vice Chair of the OWASP foundation and lead of both the OWASP Testing & Code Review Guides. Eoin was Lead for an EMEA penetration testing team, leading global enterprise cybersecurity engagements with a big 4 consultancy for five years prior to founding BCC Risk Advisory Ltd and Edgescan in 2011. He was also OWASP Person of the Year for 2015 and 2016 for contributions to the industry and was awarded the Tech Excellence Rising Star Award for 2015.

Jonathan Lee

**Senior Product Manager,
Menlo Security**

Jonathan Lee is Menlo Security's Senior Product Manager. He is experienced in leading the ideation, technical development, launch and adoption of innovative security products. He has served as a trusted advisor to numerous enterprise clients in the area of information security and compliance. As an industry leader in the cybersecurity space, Jonathan is well-versed in data protection, threat analysis, networking, internet isolation technologies, and cloud-delivered security.

Andy Mason

**Head of Financial Crime & Fraud,
Bó**

Andy spent his early career designing and implementing operating models for financial services companies, followed by time spent working as and with Lean Six Sigma Black Belts from companies like Toyota, Motorola and Jaguar Land Rover. From there Andy created and led the global Service Improvement and Service Management functions for the RBS Shared Services business, being asked to support the RBS Americas operations with solving some problems in the Customer Due Diligence teams, which started off a career in financial crime. Since then, Andy has worked in all areas of global financial crime (anti-money laundering, sanctions, customer due diligence, fraud etc.) across retail, business and investment banking, where he was Director, Innovation & Development in the Natwest Markets Anti-Money Laundering team; recruiting people from law enforcement and pharmaceuticals to look at solving banking problems from a different perspective.

Most recently, Andy has been the Product Owner and Head of Financial Crime at Bó, RBS' digital bank, accountable for the design & implementation of the Bó Financial Crime function, all of which has been built entirely from scratch.

Pavel Mucha

**Systems Engineer,
Cybereason**

Pavel Mucha is a Senior Pre-Sales Specialist at Cybereason and one of the good guys working tirelessly to give our customers the upper hand against adversaries. His experience with Cybereason and McAfee makes him a valuable asset for anybody needing to understand how to defend their organisation against the next generation of cyber-threats. A fluent Russian speaker, in his spare time Pavel collects old Saab cars – we guess somebody has to.

Raghu Nandakumara

**Field CTO EMEA,
Illumio**

Raghu Nandakumara is a Field CTO at Illumio, based in London, UK, where he is responsible for helping customers and prospects through their segmentation journeys. Previously, Raghu spent 15 years at Citibank, where he held a number of network security operations and engineering roles. Most recently, he served as a Senior Vice President, where he was responsible for defining strategy, engineering, and delivery of solutions to secure Citi's private, public, and hybrid cloud environments. Raghu holds an undergraduate degree in Mathematics and Computer Science from the University of Cambridge, and a master's degree in Advanced Computing from Imperial College London.

Michael Owen

**Head of Systems Engineering UK&I,
IntSights**

Michael Owen heads up the Pre-Sales Engineering for IntSights in the UK & Ireland. He has been in the information systems technology and security arena for over 30 years. His career bridges manufacturer, strategic partners, and end-users and so he brings a useful perspective that covers all parts of the chain. For the last four years, Owen has been heavily involved with big data vendors around data analytics, smart buildings, and more recently cyber-threat intelligence. Owen is currently leading the charge in the UK & Ireland to educate and introduce organisations to increasing their visibility on the many dark web threats that pose a serious risk to them.

During his career, Owen has held positions at BT, Siemens, Aruba & Hewlett Packard Enterprise and has been involved in numerous large scale projects.

Jan Tietze

Director Security Strategy EMEA, SentinelOne

Before joining SentinelOne in 2020, Jan Tietze served in senior technical and management roles ranging from engineering to CIO and CTO roles for global IT and consultancy organisations. With a strong background in enterprise IT and an early career in senior field engineering roles in Microsoft and other security and consulting organisations, Jan understands real world risk, challenges and solutions and has been a trusted advisor to his clients for many years.

Zeki Turedi

Technology Strategist, EMEA, CrowdStrike

Zeki Turedi has extensive experience working within private sector, law enforcement and government, consulting on incident response, endpoint and network cybersecurity throughout Europe, Middle East and Africa. In his current role as a Lead Security Engineer for CrowdStrike, Zeki works with organisations to incorporate and streamline threat intelligence and endpoint protection. Zeki has also contributed to several publications and research papers including 'Issues in Cybercrime, Security and Digital Forensics'.

Sally Webmark-Taylor

Head of Financial Crime Risk Name Screening, Aviva

Sally is an experienced financial crime risk & compliance professional, and a subject matter expert in customer and sanctions screening. Sally is currently responsible for name screening globally within the financial crime risk function at Aviva – ensuring effectiveness in line with regulatory expectation, governance, internal controls and reporting. She has held this position since 2017, after holding a similar position at HSBC for five years. She has previously had roles in fraud and collaboration technologies. Sally is also the Data Governance Officer for the financial crime function and holds an ICA Diploma in Financial Crime. □

EventBot: A new, mobile banking trojan is born

Cybereason's Nocturnus research team has dissected a rapidly evolving Android malware in the making.

Cybereason reports

Back in April, Cybereason's Nocturnus research team began investigating a new type of Android malware dubbed EventBot, which was first identified in March 2020. This malware appears to be newly developed with code that differs significantly from previously known Android malware.

EventBot abuses Android's accessibility feature to access valuable user information, system information, and data stored in other applications. EventBot can intercept SMS messages and bypass two-factor authentication mechanisms.

The Cybereason Nocturnus team has concluded that EventBot is designed to target over 200 financial applications, including banking, money transfer services, and crypto-currency wallets. Those targeted include applications like: Paypal Business, Revolut, Barclays, UniCredit, CapitalOne UK, HSBC UK, Santander UK, TransferWise, Coinbase, paysafecard, and many more. It specifically targets financial banking applications across the United States and Europe, including Italy, the UK, Spain, Switzerland, France, and Germany.

EventBot is a mobile malware banking trojan that steals financial information and is able to hijack transactions. Once this malware has successfully installed, it will collect personal data, passwords, keystrokes, banking information, and more. This information can give the attacker access to personal and business bank accounts, personal and business data, and more.

Letting an attacker get access to this kind of data can have severe consequences. 60% of devices containing or accessing enterprise data are mobile. Giving an attacker access to a mobile device can have severe business consequences, especially if the end user is using their mobile device to discuss sensitive business topics or access enterprise financial information. This can result in brand degradation, loss of individual reputation, or loss of consumer trust.

Much like we have seen in recent months, anyone can be impacted by a mobile device attack. These attacks are only becoming more common, with one third of all malware now targeting mobile endpoints. Care and concern both for using a mobile device and for securing a mobile device is critical, especially for those organisations that allow bring-your-own-devices.

The Nocturnus team has dissected a rapidly evolving Android malware in the making. This malware abuses the Android accessibility feature to steal user information and is able to update its code and release new features every few days. With each new version, the malware adds new features like dynamic library loading, encryption, and adjustments to different locales and manufacturers.

EventBot appears to be a completely new malware in the early stages of development, giving us an interesting view into how attackers create and test their malware.

Cybereason classifies EventBot as a mobile banking trojan and infostealer based on the stealing features discussed in this research. It leverages webinjects and SMS reading capabilities to bypass two-factor authentication, and is clearly targeting financial applications.

Although the threat actor responsible for the development of EventBot is still unknown and the malware does not appear to be involved in major attacks, it is interesting to follow the early stages of mobile malware development. The Cybereason Nocturnus team will continue to monitor EventBot's development.

To ensure you don't fall victim to EventBot:

- Keep your mobile device up-to-date with the latest software updates from legitimate sources.
- Keep Google Play Protect on.
- Do not download mobile apps from unofficial or unauthorised sources. Most legitimate Android apps are available on the Google Play Store.
- Always apply critical thinking and consider whether you should give a certain app the permissions it requests.
- When in doubt, check the APK signature and hash in sources like VirusTotal before installing it on your device.
- Use mobile threat detection solutions for enhanced security.

For more information, please visit
www.cybereason.com

cybereason

cybereason

PROTECT IT ALL_

STOP TOMORROW'S THREATS TODAY

ENDPOINT PREVENTION

- NGAV
- RANSOMWARE
- FILELESS MALWARE
- ENDPOINT CONTROLS

ENDPOINT DETECTION & RESPONSE

- EDR
- MOBILE
- CONTAINERS
- THREAT FINDER
- FORENSICS
- LIVE RESPONSE

ENDPOINT SECURITY ANALYTICS

- THREAT HUNTING
- INFINITY

MANAGED SECURITY SERVICES

- INCIDENT RESPONSE
- ASSESSMENTS

WWW.CYBEREASON.COM

BOSTON | TEL AVIV | LONDON | TOKYO

Generating actionable intelligence

Intelligence comes in many different forms and from a variety of sources. Each of the possibilities has value in uncovering the motives driving cybercriminals, as well as their tactics and tools.

IntSights reports

The goal of cyber-threat intelligence is to provide advance warning and detection of cyber-attacks so you can take proactive protection measures. That second part, the part about taking action, is key. Intelligence isn't much good if you can't act on it. Therefore, strong, actionable intelligence is the foundation of DRP (Digital Risk Protection).

No one needs to tell you that the Internet is an astonishingly big place, with an ever-expanding collection of data and information. The total number of websites out there is right around 2 billion. And that's just the part of the Internet that people *want* you to see.

Beyond that lies the *dark web,* a much more secretive part of the Internet that allows users to access websites anonymously. Plenty of legitimate activity takes place there, but it's also the home of the cybercriminal underworld. Their part of the dark web hosts all kinds of nefarious activities, hidden more or less in plain sight, if you know where to look. Meanwhile, social media has become a popular attack vector for cybercriminals, paste sites are openly accessible to any browser, and app stores allow cybercriminals to target users on their mobile devices.

Surveys of the people who use cyber-threat intelligence tools have found that many are overwhelmed by the information they get. For those who are using traditional or first-generation, tools, there's just so much data to process, normalise, and determine whether it's relevant to their operations and brand. These users are hit with what they feel are excessive and generic alerts. There's just a lot of noise, and it's hard to make sense of that noise.

Newer, more advanced tools understand the multidimensional nature of threats and use your digital footprint to provide context and relevancy. That gives organisations a much better ability to understand if and how a specific threat impacts them, which means they can act much more promptly to mitigate the threat.

Sources and types of intelligence

Intelligence comes in many different forms and from a variety of sources. Each of the possibilities has value in uncovering the motives driving cybercriminals, as well as their tactics and tools.

Here are some of the types of intelligence on the menu:

- *Open source intelligence:* Known as OSINT for short, this is the kind of intelligence you can derive from publicly available or open sources. Web pages are open sources, as are many online forums and intelligence feeds. They're out there for any user, including you.
- *Signals intelligence:* This refers to collecting intelligence by way of signals from communications and electronic sources. You'll see it referenced as SIGINT, and some people call it machine intelligence. Cell phones and computers are the most common sources of SIGINT.
- *Social media intelligence:* You may view intelligence gathering via social media channels and networking sites to be a subset of open source intelligence. A lot of organisations see SOCMINT as its own unique kind of intelligence, because social media play such a big role in the major threats of customer phishing and brand impersonation.
- *Human intelligence:* Also known as HUMINT, this is what it sounds like – intelligence gathered by contacting and engaging with actual people, rather than automatic monitoring or digging through feeds and technical processes. Human intelligence gathering takes just the right knowledge and skills to gather intelligence this way without raising suspicion.
- *Dark web intelligence:* This is what you gather when you monitor the various dark web sources, such as black markets, private chat rooms, dark web forums, and other anonymous and villainous places.

As you can see, some of these types of intelligence overlap. Social media intelligence is related to open source intelligence, and a fair amount of human intelligence gathering takes place in dark web places. Despite the overlaps, there may be differences in the intent of the research. □

Can you measure the efficacy of micro-segmentation?

“If you cannot measure it, you cannot control it” – Lord Kelvin.

Raghu Nandakumara reports

Quantitative measurements inform everything we do – whether it’s comparing different products, determining the success of a project or tracking the development of a sports team. We are able to make real, objective, ‘like for like’ comparisons, as opposed to solely relying on subjective opinions. Yet when it comes to many of the security products for the enterprise, we seem to be happy with products that will make us *more* compliant, *improve* our security, or provide a *better* way of detecting threats. Increasingly, however, we are seeing that the savvy security buyer is now asking for the numbers to back up vendor claims. They’re asking questions like, ‘how will the success of that product or solution be measured?’

The outpouring of articles in the security media over the last few years make it clear that micro-segmentation is now an essential security control for organisations. In particular, the central role of micro-segmentation in any zero trust strategy is unsurprising given it limits lateral movement and impedes an attacker’s ability to navigate the network to find the intended target. Micro-segmentation is the quintessential example of ‘least privilege’ – only allowing things to communicate that should be allowed to communicate, nothing more, nothing less. However, those implementing micro-segmentation have historically lacked quantitative measures to demonstrate its efficacy.

At Illumio we felt it was important to quantitatively demonstrate the benefits of micro-segmentation, how the impact changes as the size of environment increases, and a clear testing methodology that could be repeated by any organisation that wishes to validate these results in their own environments. To achieve this, we partnered with red team specialists Bishop Fox to conduct and document an industry-first blueprint for how to measure the efficacy of micro-segmentation based on the main components of the MITRE ATT&CK® framework.

The Bishop Fox team were tasked with finding a pair of ‘crown jewel’ assets in a test environment over a series of rounds. Think of this like a ‘capture the flag’ exercise, but with no blue team to actively defend the environment. In total, there were four rounds of testing including the control test. With each test, the micro-segmentation policy became tighter and tighter.

The Bishop Fox team had no prior knowledge of the test environment, and the entire environment was destroyed and rebuilt for each test. Meaning that in each round of testing, nothing carried over, in particular topology and IP addresses were blown away. All the micro-segmentation policies were defined using a white list or default deny approach – i.e. rules were written to explicitly allow authorised traffic, thus anything without a rule was, by default, not permitted and therefore blocked. The initial set of tests were done on a 100-workload environment (considerably smaller than the deployment size of most medium sized organisations), with repeats of Use Case 2 at 500 and 1000 workloads.

The headline from the first round of tests – wouldn’t you like to make the adversary’s job anywhere between 3x – 10x more difficult? If so, implement micro-segmentation.

The key takeaway from the second round of tests is that **as the size of the protected estate increases, the attacker’s job gets measurably harder (between 4.5x and 22x), even with no changes to the nature of the segmentation policy implemented.**

So, what does this all mean:

1. Micro-segmentation needs to take a white list approach – only by taking this approach can you truly measure the improvement in security posture.
2. Micro-segmentation, even with a simple environmental separation policy, makes it at least 3x more difficult for an attacker to achieve their outcome – of its own strong justification for investing in this capability.
3. Increasing the deployment size of micro-segmentation without needing to change the policy definition results in overall security benefits of itself – organisations should aim to extend segmentation to their entire estate, not just a small tactical subset.
4. Increasing sophistication of a micro-segmentation policy forces a change in approach by the attacker, often at a cost of time and heightening the chances of detection. □

Raghu Nandakumara is Field CTO at Illumio.

For more information, download a copy of the report or visit **www.illumio.com**

ILLUMIO HELPS 10 OF THE TOP 20 BANKS GLOBALLY TO SECURE THEIR CRITICAL BUSINESS APPLICATIONS FROM INTERNAL BREACH.

BNP PARIBAS

BAILLIE GIFFORD

Morgan Stanley

VISIT OUR STAND TODAY TO LEARN MORE.

illumio

WWW.ILLUMIO.COM

Preventing your #1 security risk

The idea of insiders exfiltrating data and knowledge is nothing new for financial services firms; you've been monitoring and detecting this behaviour for years.

Egress reports

But there's a group of insiders who are frequently overlooked: those that make mistakes while simply trying to get their jobs done. They're not malicious and they're not looking for personal gain – so they're often seen to pose less of a threat to sensitive data, if firms have been able to quantify this threat at all!

Yet according to the Information Commissioner's Officer, this group of insiders are your top security risk in 2020. And in particular, misdirected emails are the top cause of security incidents.

This risk is only growing in lockdown. We've increasingly turned to email to enhance communication and replace physical processes. We're also more distracted than ever. We've gone from one to one million offices – with people working remotely surrounded by the pressures of both their work and home lives combined. And we know that when people are tired, stressed and distracted, they're much more likely to make an honest mistake, such as sending an email in error or attaching the wrong document.

A new approach to tackling an old problem

The problem of misdirected emails exists not because CISOs and their security teams are unwilling to address it, but because it's been difficult to do so using the static technologies that, until recently, have formed the main defence against it. When your AV filter doesn't detect an inbound spear phishing attack or autocomplete suggests the wrong recipient, your busy, tired and otherwise unpredictable employees become your last line of defence. And, ultimately, static technologies are not designed to adapt to their behaviours. An email is either encrypted or unencrypted, recipients are either included or not. Static technology is unable to provide the dynamic safety net required to stop human-activated security breaches before they happen.

But there is good news: technology now exists that can truly mitigate this risk – and in doing so, bring added benefits to financial services firms.

Static technology is unable to provide the dynamic safety net required to stop human-activated security breaches before they happen.

Human layer security can use contextual machine learning to determine the actual risk of a data breach in real time, as individual employees use email. This includes both accidental breaches – providing a dynamic safety net that helps individuals correct mistakes – and intentional incidents, including blocking content from being shared.

Even when the correct recipients and files are attached to an email, sensitive data still needs to be protected. For financial services firms, adoption of message-level encryption by recipients has traditionally proven difficult, often leading to information being sent in plaintext. Additionally, it's previously been impossible for individual employees to know when TLS is properly enabled by recipient organisations as they send emails. But your duty of care to clients and compliance obligations mean you must ensure confidential information is secure not only in transit but also when it reaches the recipient.

Intelligent email security technology can now tell whether TLS is properly enabled and appropriate for use, or recommend tighter security and control when it's not, empowering employees to make the best decisions when sharing sensitive data via email. The technology can also use network intelligence for a frictionless recipient experience when using message-level encryption. This reduces pushback to ensure data is always protected.

By taking this human layer approach to security using intelligent technology, CISOs and their teams are now in a position to truly prevent human-activated breaches, protect data and accurately report their compliance status. Where static solutions have failed them in the past, new technologies can now make email safe to use.

For more information, please visit
www.egress.com

egress

Blockchain in enterprise. How to succeed with technology

So you've heard of blockchain. But how can you use it in your enterprise today? Maxim Denizhenko explores the benefits and security challenges.

Maxim Denizhenko reports

Blockchain can help you reduce costs and improve certain processes, for example, better product and customer data tracking and security, and reducing the risks of fraud or product counterfeiting.

Blockchain technology is fast becoming integrated into business processes in its customised form for enterprises, commonly called Distributed Ledger Technology (DLT). It's used to do things like verify transactions and control deliveries. More organisations are joining the blockchain economy: According to Gartner's June 2019 CIO Agenda: Blockchain's Emergency Depends on Use Cases (report available to Gartner subscribers), in the 2019 Gartner CIO survey, 57% of typical performing enterprises plan to start deploying blockchain services within the next one to three years; it's even greater (64%) in developing economies. Further, according to Gartner, financial services, services and transportation are the industries who have already deployed or will deploy blockchain services in the next 12 months.

Blockchain can make your data immutable

Blockchain is a perfect tool to support data immunity through the distributed registry of data. There's nothing particularly cool about the blockchain itself – it's basically just distributed data storage. But what's really interesting is how the data is synchronised, so all nodes have the same data-testing mechanism. This ensures it stays intact. It's a literal chain: every transaction is linked to the previous one, and the next one. Whoever is working in the blockchain ecosystem – whether they read or feed the data – their changes are recorded. This helps to distribute, ensure consistency and makes the data immutable – virtually impossible to hack, manipulate or steal. Although blockchain guarantees a secure process, it can never guarantee the security of your decentralised applications. And the risk of mistakes made by people and logic errors in the blockchain code can still cause vulnerabilities that can lead to an attack.

How to solve the security risks of blockchain

Organisations should concentrate on ensuring their own infrastructure is safe and secure, so you're well protected if others with weaker security join the blockchain. Implementing this technology requires careful protection. Blockchain technology itself is usually the strongest link in the chain: the weakest ones are every system that the company builds on top of the blockchain; these must be protected by blockchain security services.

The consequences of a successful attack can also be far more serious for blockchain than with other data systems; if attackers decide to target an enterprise blockchain project, huge quantities of data could be exposed.

You will still need to invest in cybersecurity services like security audits, penetration testing and an incident response strategy. It will provide protection for decentralised applications and enterprise blockchain infrastructure. In DLT, each endpoint should be secured against breaches, while applications and smart contracts are thoroughly analysed for vulnerabilities.

Don't worry, it's not as complex or costly as it may sound – some elements like the blockchain application security assessment are a one-off charge, tiny in comparison with the overall investment in new technologies. And, of course, the high costs of what a data breach could cost your business and reputation, particularly if legislation like GDPR applies to you.

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help over 270,000 corporate clients protect what matters most to them.

For more information, please visit **www.kaspersky.com**

kaspersky

The ultimate cybersecurity for blockchain-based projects.

Kaspersky Enterprise Blockchain Security service to mitigate the risks of attacks on blockchain applications, smart contracts and blockchain infrastructure.

BRING ON
THE FUTURE

www. kaspersky.com

The real cost of fighting the threat within

Unlike outside-in attacks, insiders do not need to breach defences, and many are unaware they're a threat at all – making them hard to profile, harder to detect and extremely difficult to defend against.

Rob Bolton reports

Cybersecurity professionals spend much of their time focusing on keeping threats out. And with good reason. From business email compromise attacks (BEC) to malware there are a host of threats that, once inside our defences, can do significant damage. However, not all attacks are perpetrated by outside forces. Sometimes, the threats are coming from inside the house.

These insider threats are increasingly common. According to a recent study from ObserveIT, a Proofpoint company, with Ponemon institute and IBM, the frequency of insider threats has risen by 47% in only two years and insider threats cost organisations 31% more than they did in 2018. In addition, McKinsey states that over 50% of data breaches in the past year involved an insider, whether full-time employee, part-time contractor or strategic business partner.

Just like outside threats, those that stem from the inside have the potential to cause significant damage. Not all insider threats are malicious, however. When we consider unintentional threats – such as the installation of unauthorised applications or the use of weak or reused passwords – this figure is likely much higher.

Whether due to human error or malicious intent, threats from within are notoriously difficult to defend against. Not only is the 'attacker' already within your defences, but in the case of malicious insiders, they may be able to use privileged access and information to actively avoid detection.

Understanding insider threats

The first step in defending against insider threats is to understand exactly what drives an insider to pose a threat to your organisation. Motivating factors can generally be grouped into three categories:

- *Unintentional:* From installing unauthorised applications to misplacing equipment or reusing passwords, careless employees can pose a serious threat to your organisation.
- *Emotionally motivated:* Threats of this nature are posed by employees with a personal vendetta against your organisation. Emotionally motivated malicious insiders may seek to cause damage to your reputation by leaking privileged information or disrupt internal systems for maximum inconvenience.
- *Financially motivated:* There are many ways to profit from privileged access, be it through the leaking of sensitive data, selling access to internal networks or disrupting internal systems in an attempt to affect company share price.

The financial impact of insider threats

As with external threats, attackers' tactics and motives differ. Unlike outside-in attacks, insiders do not need to breach defences, and many are unaware they're a threat at all – making them hard to profile, harder to detect and extremely difficult to defend against.

No matter the intent of an insider threat, the financial impact can be extremely significant.

Whether criminal intent or human error, the result is the same. Total annual costs for negligence-based threats average $4.58m, compared to $4.08m for those with malicious motives. Should either result in the loss or theft of credentials, these cost an organisation an average of $2.79m.

Figures of this magnitude can be difficult to relate to. But for the organisations behind them, the impact of an insider threat is incredibly real. Costs quickly arise from additional labour and investment in technology, through to business disruption and revenue loss. The average financial outlay for a single incident is estimated at $307,111 for a negligent threat, $755,760 if malicious, and $871,686 if it involves the loss of credentials.

As the defence against insider threats is broad, layered and varied, so too are the costs involved. From the proactive, monitoring and surveillance, to the reactive, post-analysis and remediation, an insider threat impacts numerous activity centres across an organisation.

Threats must be thoroughly investigated to determine the source and scope, escalation and planning meetings are required to inform all necessary stakeholders, and a response strategy must be put into action. All of which carries a substantial cost. As a result of a single insider threat, organisations spend around $22,000 on monitoring and surveillance and $125,000 on investigation and escalation.

It's vital that you know who has access to your data, and that you understand why and how they are accessing it. The greater your understanding, the easier it is to spot irregularities or changes in behaviour – and the faster you can nullify potential insider threats.

All this before accounting for the costliest part of the operation: containment.

Containing an insider incident accounts for one-third of the total costs involved, at approximately $211,000. Closely followed by remediation at $147,000 and incident response at $118,000.

Unsurprisingly, technology and labour are the two largest cost categories, accounting for almost half of the total outlay between them. This covers overtime, additional personnel, contractors and any software and hardware needed to remedy the situation.

The most effective way to avoid such substantial financial consequences is to minimise the risk of an insider threat occurring in the first place. While proactive measures also carry a cost, it is always better to spend a penny on prevention than a pound on cure.

How to spot the warning signs

External attacks are usually detected within hours or even minutes. Insider threats, however, often lay undetected for long periods.

Just 10% of cases are discovered within days of a breach while 40% remain undiscovered for up to five years.

Spotting the potential for an insider threat before an incident occurs is extremely valuable. This is by no means an exact science but there are certain behaviours to look out for.

When it comes to unintentional threats, be on the lookout for slack security practices such as writing down passwords, installing unauthorised applications or otherwise circumventing security for greater convenience.

Unfortunately, spotting the potential for a malicious threat is more of a challenge, as perpetrators will usually try to cover their tracks.

Be vigilant for any unusual attempts to access internal systems, particularly without a valid reason or if it is outside the job scope of the employee. Apply the same scrutiny to employees who suddenly begin working unusual hours without reason.

These behaviours should be particularly alarming when displayed by a disgruntled employee or one that may be exploitable for any reason.

Defence in depth

Detecting and protecting against insider threats requires a broad and robust defence, with people at its core. A comprehensive combination of tools, policies and education.

Employees should be regularly trained on how to ensure they do not cause an unintentional threat to your organisation – covering topics such as password reuse, phishing and BEC. Beyond this, educate employees on how to spot unusual behaviour among colleagues and on the consequences of perpetrating or facilitating a malicious threat.

Ensure you have tools in place to monitor users' network activity – flagging up repeat or unusual requests for system access to spot potential privilege misuse. Limit the printing and copying of sensitive data and only allow access to 'need-to-know' information with a legitimate and documented reason.

Finally, implement and police policies regarding the use of email, acceptable use, external storage devices and BYOD. These policies must be agreed to by anyone with access to your systems – employees, vendors, contractors and any other third party.

Ultimately, while fending off insider threats can be challenging, it is not impossible. But transparency and vigilance are key.

It's vital that you know who has access to your data, and that you understand why and how they are accessing it. The greater your understanding, the easier it is to spot irregularities or changes in behaviour – and the faster you can nullify potential insider threats. □

Rob Bolton is Senior Director, EMEA and APJ, Insider Threat Management at Proofpoint.

For more information, please visit
www.proofpoint.com/uk

proofpoint.

The importance of creating a culture of cybersecurity

The importance of cybersecurity has raised its profile for sophisticated cyber-attacks.

Kevin Eley reports

Online financial services now represent a key driving force behind the wheels of the global economy, but the importance of the industry has raised its profile for sophisticated cyber-attacks.

To remain safe, there are important steps organisations can take that underpin an effective cybersecurity response. These steps must encompass people, process and technology, but also the right attitudes to create a culture of cybersecurity.

Creating an effective cybersecurity posture in the financial services world

A strong cybersecurity posture lies in a confluence of powerful technology solutions and a shift in how security is viewed within organisations. It is vital that innovation, diligence and flexibility are recognised and embraced within the field of cybersecurity, and that the cybersecurity organisation is valued, and their roles and stresses understood within the wider organisation.

Success in creating a culture of cybersecurity lies in communication and understanding. For example, does the executive leadership understand the unique stresses that business growth – in its varying forms – can bring upon security teams? Or can the CISO effectively communicate their achievements to the board and display a true return on investment? Beyond the executive level, this culture of cybersecurity must be fostered to permeate organisations, so that every employee fulfils their role with cybersecurity at the forefront of their minds.

In terms of the direct response, there are several key factors that represent a strong and mature cybersecurity model within an organisation. Of primary importance is a measurable reduction in the time taken to detect and respond to threats, the essential variable to damage mitigation. Tied to shortening the mean time to detect (MTTD) and mean time to respond (MTTR) is the ability to automate and expedite workflows, freeing up the valuable time of security teams. Visibility is also a key component of cybersecurity effectiveness, offline or online, and cybersecurity teams must be able to immediately see shifts in behaviour on the network to recognise imminent threats as they arise. If these traits are applied to an organisation's security model, then even the most sophisticated threats can be recognised and thwarted.

A CISO's perspective

The cybersecurity leader, most usually the CISO, is commander in chief of an organisation's security response and has the leading influence in defining a company's cybersecurity culture. Accordingly, it is also the CISO who is ultimately responsible for communication to the board how an organisation is meeting the inherent cybersecurity risks to the business, while also aligning security principles to business goals. In performing this task, clarity of message is crucial.

Having built or inherited a security operations centre (SOC), it is upon the CISO to demonstrate business benefit to the board with a clear plan for evolution such as a Security Operations Maturity Model (SOMM) – through which security maturity is measured.

It is within board meetings that the values of business and security are negotiated. One method that a CISO can use to create a high trust environment is through partnering a member of the board with the security team. This partner can field perspective to the team from a purely business context, allowing the team to produce intelligence to the overall board that exhibits the business value of the SOC's methods.

A collaborative approach will broaden the understanding technical security teams have for business goals and the board's understanding of security necessity. Board-level support is vital to promoting a culture of cybersecurity as it is the values of the leadership that define the operating principles of an organisation.

SOMM: how to measure maturity

To quantify the effectiveness of an organisation's security posture, it is essential that security teams communicate measured results to the board, and that the board understands SOMM metrics. SOMM is a means by which cybersecurity professionals assess their organisation's current level of security maturity and plan for making improvements over time, in order to reduce risk.

The model, developed by our team at LogRhythm, describes five levels of security operations maturity – blind, minimally compliant, securely compliant, vigilant, and resilient. Each level builds on the prior, adding additional technology and process

Though the importance of board-level and employee buy-in for fostering a culture of cybersecurity cannot be overstated, an effective security posture relies on people and technology being guided by sound processes.

improvements that strengthen the capabilities of an organisation's security operation toward MTTD and MTTR reductions. If in the early stages of developing a SOC for their organisation, a CISO must show how they aim to reach the resilient phase, as and when business needs dictate.

Business growth and the security team

At its fundamental level, a paradigm shift that results in a culture of cybersecurity must rely upon executives having a thorough understanding of how changing business circumstances represent different security climates for teams to navigate. This has been seen recently with the COVID-19 pandemic leading organisations to develop security within a mass work-from-home dynamic, in which cyber-attacks have reached a fever-pitch. However, security challenges can also arise while fortunes are soaring.

For example, while a CEO may be thrilled at the prospect of rapid business growth, the same event may leave the CISO in a cold sweat. Not only will the company's success raise its profile in the eyes of cybercriminals – who keep a keen eye on the markets – but it will increase exponentially the amount of data that needs to be monitored, while security budgets may remain static. This will leave CISOs with difficult choices of where and when to protect data.

To address unforeseen security circumstances, be it a global pandemic or robust business growth, a re-think of the payment models for security solutions is in order. The two most common pricing models used by security vendors are the capacity-based model and the user-based model. Neither of these models offer easy scalability without a crystal ball. Executives should instead look to subscription-based models that offer a fixed outlay regardless of the data processed. Knowing that the organisation has the means to scale security to business changes will alleviate stress placed upon the CISO and security teams.

SOAR: vital technological support

Though the importance of board-level and employee buy-in for fostering a culture of cybersecurity cannot be overstated, an effective security posture relies on people and technology being guided by sound processes. In terms of technology processes, for top-level security, businesses can look towards the resilient stage of the SOMM model by deploying fully featured security orchestration, automation, and response (SOAR) tools, alongside cloud-hosted security information and event management (SIEM).

SOAR is an umbrella term that captures a range of incident response, security automation, case management, and other tools that help SOCs deliver that extra level of efficiency that is so crucial in today's cyber-threat landscape. Most leading SIEM solutions now include embedded SOAR capabilities, and industry analysts predict these two markets will soon converge.

A SOAR approach automates the manual tasks usually handled by SOCs and improves reporting capabilities by consolidating intelligence from a range of sources, displaying them in a single pane of glass. This allows security professionals to concentrate on the far more important matter of remediating true threats. Remediation efforts can be bolstered by SOAR's customisable workflow and controls functionality, which removes the complexity from investigating threats that might endanger the corporate network. By boosting efficiencies, SOAR greatly saves the important time of security teams.

Innovative technological approaches do much to ease the work of SOCs and are integral to the culture of cybersecurity. After all, a team that can focus on thorough investigation opposed to mindless data-sifting is a happy and effective one, and more likely to attract and retain talent. Added to this, is the importance of board-level support and a scalable budget enabling the team to counter any circumstance. Through these criteria, a culture of cybersecurity can be achieved in the financial services sector, and companies that can maintain this will find themselves protected from the most sophisticated threat actors. □

Kevin Eley is Client Director at LogRhythm.

For more information, please visit **www.logrhythm.com**

LogRhythm