SECURING THE LAW FIRM

5th July 2022
London

@eCrime_Congress
#securingthelawfirm

#securingthelawfirm

Cybersecurity and privacy for virtual working processes

Forthcoming events

e-crime & cybersecurity CONGRESS

21st September 2022
Abu Dhabi

e-crime & cybersecurity SWITZERLAND

28th September 2022
Zurich

e-crime & cybersecurity MID-YEAR

19th October 2022
London

e-crime & cybersecurity NORDICS

1st November 2022
Copenhagen

e-crime & cybersecurity SPAIN

16th November 2022
Madrid

e-crime & cybersecurity BENELUX

8th December 2022
Amsterdam

For more information, please visit
akjassociates.com/contact-us

For legal firms, remote and hybrid working is here to stay. Are we really ready?

SECURING THE LAW FIRM

5th July 2022 | Park Plaza Victoria | London

Welcome back to a face-to-face version of Securing the Law Firm. It's great to be back.

In its annual top-100 survey of UK law firms, PwC said 90% were 'extremely or somewhat concerned' about the impact of cyber-threats on their ability to achieve their ambitions over the next 12 months, even though only 4% had experienced a ransomware attack – the commonest attack type – and none of the firms involved were in the top 50.

In three-quarters of cases, cyber-attacks were the result of 'unintentional actions taken by staff' rather than 'malicious actions by staff' (2%). In almost all the other cases, firms said they did not know what caused the attack.

Most law firms will have had some level of remote working before the pandemic, and many say that after the initial shock of extreme lockdowns the adaptations they required to security processes were reasonably straightforward and have been implemented. But as we move into a period in which a significant proportion of employees prefer to work at least partly at home, is it really true that inherent cybersecurity risk has stayed the same?

So, if law firms are avoiding material attacks with current levels of spending, what is the evidence that they need to do more?

This is just one of the many topics that we will be discussing today at Securing the Law Firm. In addition, we have sessions on behavioural analytics, cyber-insurance, CISO priorities for the rest of the year and vulnerability management in the real world.

But one of the main aims of our events is to facilitate conversation and dialogue. So please, enjoy your event, and take the opportunity to mingle with peers, colleagues and solution providers. If you have any questions, please do not hesitate to ask any member of the team.

Simon Brady
Editor

@eCrime_Congress #securingthelawfirm

Editor:
Simon Brady
e: simon.brady@akjassociates.com

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

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

Booklet printed by:
Method UK Ltd
Baird House
15–17 St Cross Street
London EC1N 8UN
e: hello@thisismethod.co.uk

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

SECURING
THE LAW FIRM

Cost of passwords: Resets, breaches, and more

Organisations are spending more than ever to protect themselves from cybercriminals.

A recent Deloitte study found that companies spend roughly $2,700 on each full-time employee for security each year. For companies with large workforces, that can add up to millions. But all the spending in the world won't matter if you're using passwords and the weak security they provide in your authentication processes.

Passwords are a massive security issue for organisations. Verizon's 2021 DBIR found that hacked and stolen passwords cause 89% of web application breaches, and these attacks can take months and millions of dollars to recover from.

To illustrate the costs of continuing to rely on the password, we've picked out a few statistics that show that passwords aren't only insecure but costing your organisation a lot of money.

The monetary cost of a breach

IBM's Cost of a Data Breach 2021 report found that the average cost of a data breach for an organisation was $4.24 million. Here's the breakdown of the average cost for different types of attacks:

- *Phishing:* $4.65 million
- *Malicious insiders:* $4.61 million
- *Social engineering:* $4.47 million
- *Compromised credentials:* $4.37 million

It's important to note that passwords play a critical role in all of these attacks. Phishing attacks are usually targeted at getting users to unwittingly give away passwords, social engineering uses fake authority figures to trick people into giving away passwords to 'verify' accounts, and insider attacks often rely on passwords not being updated and changed after employee turnover. The password remains the target for all of these attacks.

Breaches caused by compromised credentials took the longest to identify and contain. On average, the password-related attacks IBM studied took 250 days to identify and another 90 days to contain, totalling 341 days.

Remote work has made data breaches more costly. For organisations that have 81–100% of their workforce remote, the average cost of a breach was $5.54 million. Companies with less than 10% of employees working from home had data breaches that cost an average of $3.56 million, which is still a significant amount of money but a dramatic difference from the costs to more remote work organisations.

The costs are often much higher for companies with remote employees because they are accessing resources on many different devices where the company has no way of assessing the risk or security posture of the device. Users can just enter their username and password and access sensitive data on any malware-infested device and a hacker has their way into the network.

It also often takes longer to discover breaches when the workforce is remote, allowing malicious attackers to wreak havoc and drive up costs for the recovery process. Companies with more than 50% of employees working remotely took 316 days to identify and contain breaches while organisations with more in-office employees only took 258 days.

Breaches caused by compromised credentials took the longest to identify and contain. On average, the password-related attacks IBM studied took 250 days to identify and another 90 days to contain, totalling 341 days. An attack on New Years Day wouldn't be detected until sometime around Labor Day and likely not resolved until early December. That's nearly an entire year, and attackers can do a lot of damage in that time.

It only takes one compromised password from a phishing attack or a hacker to employ a successful credential stuffing attack to cause all these financial and productivity losses.

Password resets = lost productivity

While the previous study looked at passwords and the costs associated with password-related attacks, Forrester looked at the cost of passwords from a productivity aspect.

Passwords suck up our time in one of two ways: either through recalling and entering them or spending time resetting them. Forrester's

Beyond Identity reports

> Beyond Identity's platform offers an easy way for organisations to ditch passwords for good. Your customers are secured with our product by using immutable credentials backed by private keys that never leave the device.

researchers found that employees spend an average of 11 hours per year performing these two tasks. In a company of 15,000, an organisation would pay $5.2 million in wages just for employees to enter or reset their passwords!

Those employees aren't the only payroll costs associated with lost or forgotten passwords, however. Forrester also estimated that large organisations were spending an average of $1 million a year in help desk costs to assist employees with password-related issues.

Password issues hit e-commerce especially hard

In e-commerce, getting people to add items to their cart and successfully check out is the utmost priority for these websites. If customers encounter friction during shopping or checking out, it can easily lead them to abandon their carts. And often passwords are a big source of friction for customers.

Our research found that a quarter of those surveyed were willing to abandon a high-value cart ($100+) if a password reset was necessary. Password issues during the checkout process are disastrous.

We also found that one out of every eight shoppers will abandon their carts if you ask them to create an account before checking out. This is most likely due to the friction of having to create yet another username and password. In fact, we found that 84% of users are tired of remembering so many passwords.

It's already difficult enough to make a sale. The friction of passwords is making it even harder – and costing companies potential revenue.

Passwordless authentication pays for itself

Eliminating passwords doesn't just make good security sense – it makes equally good fiscal sense. Password-based attacks are often only discovered after the attacker has had months to scour your servers for high-value targets. Who knows what they might be able to find with that amount of time?

Secure Customers brings the convenience and security of passwordless authentication to your customers. Beyond Identity's platform offers an easy way for organisations to ditch passwords for good. Your customers are secured with our product by using immutable credentials backed by private keys that never leave the device.

Every time a customer logs in, you know they are who they say they are, and the device they're using is a known device to your network. Secure Work does the same thing for your workforce with passwordless multi-factor authentication (MFA) where only secure, phishing-resistant factors are used. Our product integrates with popular single-sign-ons and totally removes passwords from the authentication process and all the costs associated with them.

We'd love to show you how passwordless MFA can secure your network, streamline authentication, and save you money. Ask for a demo today. □

About Beyond Identity
Invisible multi-factor authentication
Eliminate ransomware and account takeovers.

Invisible strong authentication. Security without friction. No passwords, no one-time codes, no user actions or second devices required. Just three unphishable factors.

The most advanced MFA on the planet – only one device needed.

Beyond Identity verifies users by cryptographically binding identities to devices to provide the most secure and frictionless MFA experience ever.

Implement a state-of-the-art MFA solution or add frictionless security to your existing MFA in 30 minutes or less.

For more information, please visit
www.beyondidentity.com

BEYOND IDENTITY

Law firms must take security seriously as cyber-threats HEAT up

Law firms are increasingly attractive targets for threat actors.

Menlo Security reports

The legal industry is exemplary of the drive towards digitisation during the pandemic. Previously known for laborious paper-based processes and administrative practices, law firms have begun to shed their inefficiencies and evolve to thrive in a more technologically savvy world.

In truth, they have little choice. With increased competition, cost control and client expectations, it's become a case of sink or swim for many firms, with the need in many cases for an operational overhaul.

We found this out recently in our UK Legal Services Cybersecurity Survey Research Report published in May – a survey of 150 legal professionals. Here, almost half of respondents (47%) stated that they had introduced digital services.

Be it sophisticated search tools, digital case and document management, legal CRM, cloud billing and expenses systems, or online collaboration platforms, the adoption of new technologies and innovation of legal processes has brought about significant benefits to industry players.

However, there is a less positive side to this development.

With lawyers now spending much of their working day in the browser, often to leverage new applications and tools, organisations' digital footprints have expanded. But at the same time, cybercriminal activities have also increased both in volume and complexity.

Take HEAT (Highly Evasive Adaptive Threats) attacks, for example. Specifically designed to target web browsers as the attack vector, these attacks see threat actors using various techniques to evade multiple layers of detection in legacy security stacks and bypass common web security measures to deliver malware or compromise credentials.

> The pattern is clear: as legal professionals increasingly use their browsers as firms digitally transform, attackers adapt to target those users directly.

The pattern is clear: as legal professionals increasingly use their browsers as firms digitally transform, attackers adapt to target those users directly.

This makes law firms increasingly attractive targets for threat actors, especially with many legal documents now stored, collaborated on and shared online, and containing highly sensitive (or, in the eyes of threat actors, lucrative) data.

Law firms recognise the threats, but are not responding

It's no surprise that several high-profile data breaches and phishing scams hitting large law firms have come to light in recent times.

In response, legal industry bodies are working to address the threats. Both The Law Society and the Solicitors Regulation Authority (SRA) have published advice for law firms in developing cybersecurity policies and dealing with attacks, the latter having also opened a consultation with its law firms to ask for feedback on plans to clarify the scope of cover in professional indemnity policies when a firm is subject to a cyber-event.

At the same time, the Council for Licensed Conveyancers (CLC) has explored requiring law firms to purchase standalone cyber-insurance in a consultation paper in 2021 as 'evolving forms of cyber-risk' become more complex.

It is evident that many law firms recognise the growing number of cyber-threats facing them.

According to PWC's latest Annual Top 100 Law Firm Survey 4, published in October 2021, the top 100 UK law firms stated that cyber-attacks were the biggest threat to their ambitions, with nine in 10 concerned about the impact of cyber-threats to their business.

However, this concern is failing to result in any meaningful action.

When asked about the advice and guidance published by The Law Society and the SRA, our survey revealed that the majority of respondents were aware of them, but only a third had read them. Equally, little more than four in 10 had checked the consultation content from the SRA.

At a time where web traffic is expanding exponentially and the risks are heightening by the day, isolation allows law firms to secure all employee digital activities that may unknowingly result in catastrophic consequences.

What was also clear from our study was that a significant proportion of firms are failing to provide employees with adequate advice and direction on security best practice despite the threats. Around half of all respondents lack confidence in the cybersecurity training that they are currently receiving.

This failure feeds into other worrying statistics. Currently, around four in 10 legal professionals do not recognise that they have a responsibility to identify and report cyber-threats to their firms, while more than three in 10 do not know how to deal with phishing emails.

Sustaining the benefits of digital transformation while maximising security

While the legal sector has been quick to embrace new applications, solutions and technologies, security has slipped down the priority list. Just over half (58%) of law firms have changed their cybersecurity measures to deal with home working, while *less* than half (45%) have updated their cybersecurity training to address these new ways of working.

The fact that many companies have failed to implement any meaningful change suggests that they are likely using outdated solutions that simply were not designed for the hybrid or remote working models that have been adopted. It is perhaps no surprise then that almost half (48%) of respondents from our survey are not confident about their firm being well prepared to deal with an attack.

Such attitudes need to change of course, and security needs to be further up the priority ladder in the sector.

There are some simple steps that law firms can take to improve their defences. This starts with identifying gaps in the security stack and adopting internal policies and procedures suitable for remote and hybrid working environments to effectively address new attack vectors.

The Zero Trust principle

To further bolster browser security and mitigate the threat of HEAT attacks effectively, firms should also look to adopt the principles of Zero Trust. Traditional security models operate on the outdated assumption that everything inside an organisation's network should be trusted. Zero Trust turns this on its head, taking a default 'deny' approach that's rooted in the principle of continual verification.

It recognises trust as a vulnerability, and therefore ensures that all traffic – whether emails, websites, videos, or other documents – is verified.

One of the most effective ways of achieving Zero Trust in its truest sense is through the adoption of isolation-based technologies. It is a solution that shifts the point of execution for active content away from a user's browser and into a disposable, cloud-based virtual container.

In essence, this acts as a barrier, preventing any content – including potentially malicious payloads – from reaching the endpoint. It is not 'almost safe' like other security solutions. It can stop malware 100% of the time.

For law firms this is crucial. At a time where web traffic is expanding exponentially and the risks are heightening by the day, isolation allows law firms to secure all employee digital activities that may unknowingly result in catastrophic consequences.

For organisations looking to offer a safe online experience, empowering users to work without worry as they keep the business moving, isolation technology is the only answer. □

For more information, please visit
www.menlosecurity.com

MENLO SECURITY

Geopolitical cyber-warfare

Etienne is one of the early pioneers of the internet security. He has spent over 20 years promoting the innovative use of technology and building services to solve complex issues.

Etienne Greeff reports

As a security practitioner with a particular interest in the geopolitical aspects of cybersecurity, it is somewhat difficult for me to comment on the cyber-aspects of the military conflict in Ukraine. The war is a desperate situation with huge losses on both sides. It does behove me as a professional to give our customers advice on how to respond to these momentous events as they impact every single one of us.

In the day to day of any business we are always balancing the risks originating from state actors using cyber to project power, the structural forces affecting our businesses, which include the threats relating to how we put together our IT systems and lastly dealing with rapid technology changes. Generally, we attempt to observe geopolitical forces and structural factors so we can orient ourselves to be able to deal with the impact. We attempt to control and react to the rapid changes of technology within our organisations as we embrace new ways of working, accelerated by the pandemic.

When major geopolitical changes happen, as they have over the past weeks, some factors such as the effect of geopolitical actions increase the importance of the geopolitical driven threats.

One of the consequences of using the Internet is that it is a shared medium and all of us are often unwitting participants in situations of war.

In the case of the Russian invasion of Ukraine all businesses that rely on the Internet became unwitting participants in the conflict.

We have seen Western companies like Microsoft and Fortinet enter the fray. Microsoft to share intelligence to disrupt a large-scale malware attack targeting Ukraine. Fortinet to stop a large-scale distributed denial of service attack. We have also learned that the US Army's Cyber Command has worked with private companies to disable some malware which was designed to wipe computer systems within the Ukrainian train service, prior to the Russian invasion. If this malware was still present during the invasion it could have prevented the mass evacuation of civilians.

The reality is every single organisation should consider themselves a participant in the conflict. When state sponsored actors attack, the odds are stacked against any resource constrained organisation.

It is important to plan for the worst and balance spending across the ability to assess your weaknesses and detect attacks, deploying technology to protect your environments and ensuring you have an incident response plan in place to recover from an attack.

It is also true that even state-sponsored adversaries will exploit structural factors within business!

Our recommendations would be:

1. *Embed security into your digital transformation initiatives*
   - Think security 'of' the cloud versus security 'in' the cloud
     - Consider Cloud Security Posture Management services
     - Review the security of applications within the cloud
2. *Even state actors use legacy techniques* – be aware of common themes such as:
   - Spear phishing is the most common infection vector
   - Known vulnerabilities are exploited
   - Supply side attacks – Do your suppliers practice what they preach?
3. *Simulate a determined threat actor* – penetration testing
   - Use a CREST accredited firm knowing they use best practices
   - Be aware of poor-quality penetration testing that is fundamentally just a vulnerability scan with commentary
4. *Plan for the worst* by balancing spending across these areas:
   - Assessing risk
   - Detecting attacks
   - Protecting your assets
   - Responding to attacks
   - Recovering from attacks □

Etienne Greeff is CEO at Flow.

FLOW the smart choice

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

FLOW
the smart choice

Your digitial transformation partner

Areas of expertise

datacentre

Harness the best of the old and the new world to optimise performance and enhance capability.

networks

Through expert design, deployment and management we deliver real business outcomes.

security

Providing you best-of-breed solutions, expert advice and support for secure cloud transformation.

cloud

Built into the fabric of our solutions, enabling secure and confident business operations.

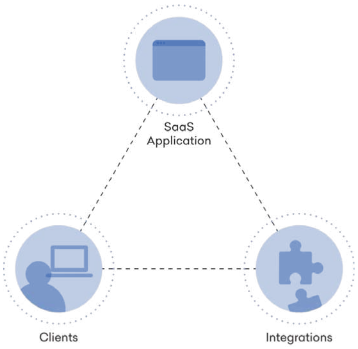
The smart choice for secure cloud transformation

Flow provide efficient and secure solutions to organisations allowing them to do business in confidence, with seamless transition and without fear of a cybersecurity attack.

T: (0) 1442 927 996
info@flowtransform.com
flowtransform.com

The components of a holistic SaaS security strategy

SaaS security: A changing model of cybersecurity.



Obsidian reports

Businesses today commonly employ hundreds of SaaS applications for a variety of functions, but the majority of sensitive data is typically entrusted to a small set of foundational enterprise applications. Security leaders are well aware that the transition to SaaS has prompted increased targeting by bad actors and recognise that SaaS cybersecurity is more important than ever – but the way teams are thinking about and equipped to protect SaaS needs a new approach.

For years, security teams focused on securing *things*: endpoints, servers, and networks. Accordingly, endpoint detection and response (EDR) solutions were used to monitor and mitigate threats residing on user devices and servers, while network detection and response (NDR) tools protected the network.

Although the transition to cloud-based applications has fundamentally changed the coverage model for application security, many teams are still intently focused on securing the clients and their connections while overlooking other critical components of SaaS. Better SaaS security requires a new approach and a different way of thinking uniquely designed around the architecture of cloud-based applications – a holistic solution that extends the principles of zero trust to SaaS.

The core components of SaaS

To better understand how to approach SaaS security, you should first consider three core components of SaaS application:

- The client connection to the application
- The SaaS application itself
- Other applications integrating with it

A holistic approach to SaaS cybersecurity recognises that each of these components can be a source of risk to the entire application, while the interconnected nature of these applications also means that a breach originating at any one of these points can threaten your wider SaaS environment.

Securing the client connection

Monitoring the client connections to your SaaS environment is essential. Your security team needs to understand the authentication, privileges, and actions of your users within and across business-critical applications to define the scope of each user's risk. This data needs to be aggregated and normalised from every application into a single, easily understood format in order to be readily accessible to your security team, extending the zero trust model of 'never trust, always verify' beyond identity providers and into the SaaS applications themselves.

Securing the application

The SaaS applications that are core to your business are inherently unique and complex, with the intricacies and functionality that one might expect from an operating system. Securing these applications requires a deep understanding of each platform, structural vulnerabilities, and issues specific to your own environment. Continuous monitoring of the application security posture is critical here – this includes both application configurations and the privileges granted to your users. Fully securing applications also means going beyond merely knowing the state of controls and privileges, but monitoring associated activities to detect lapses in security and utilising inter-application insight.

Securing the integrations

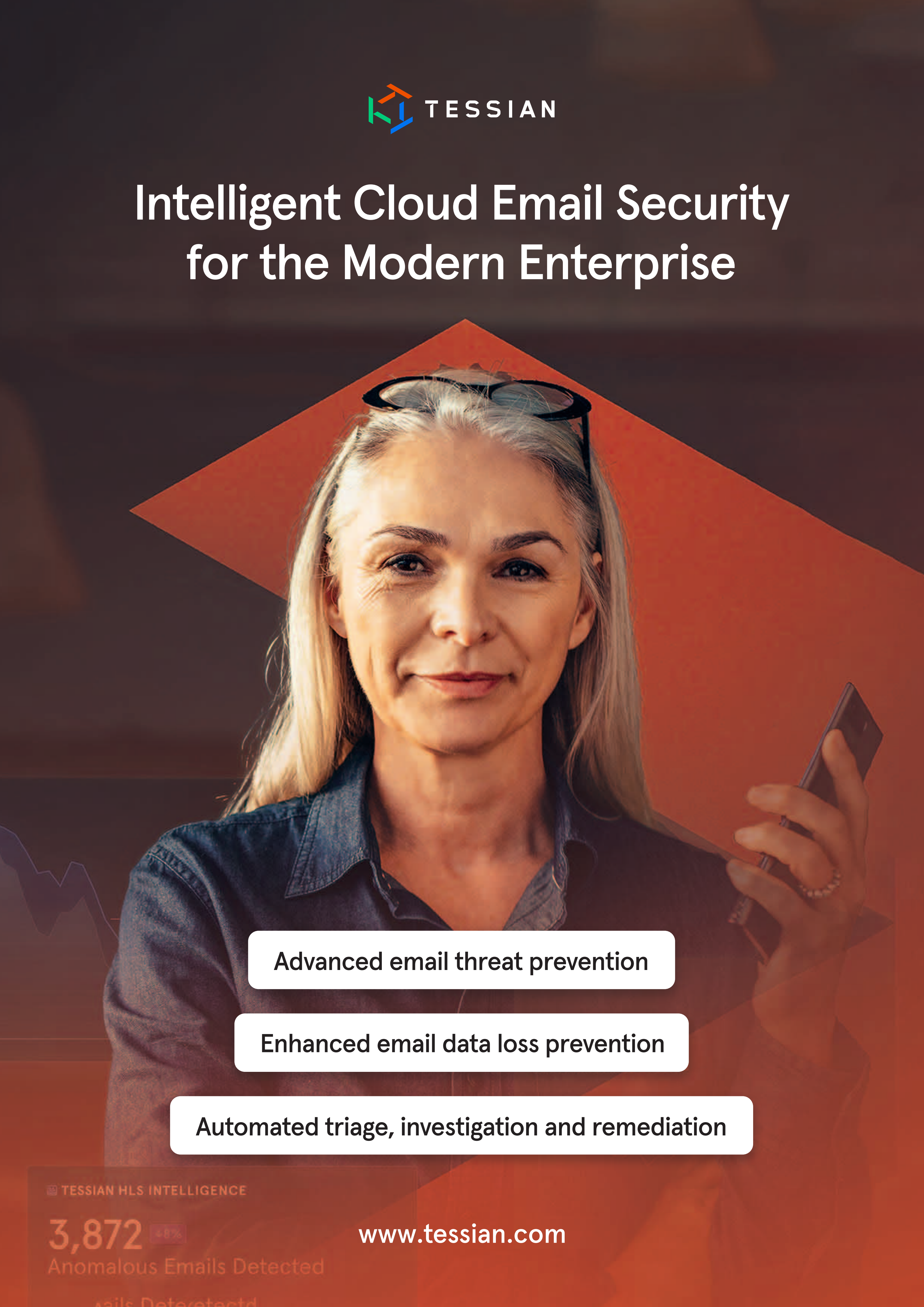
SaaS users and administrators integrate third-party applications into core applications in order to expand functionality, automate workflows, or even play their favourite games. Once authorised, these connections persist their permissions and access to the core application – a vulnerability which can present serious security risk if left unchecked. Even vetted third-party applications can be compromised by an attacker, providing a backdoor into core applications. Without continuous monitoring and threat detection to verify the integrations, they fall outside of the zero trust framework.

Obsidian's comprehensive approach

Obsidian Security offers the first truly comprehensive SaaS cybersecurity solution built with a deeper understanding of your business-critical applications. This understanding of the three core components of SaaS applications enables Obsidian to take zero trust beyond the identity provider and secure the business-critical data held in SaaS applications. □

For more information, please visit
www.obsidiansecurity.com

OBSIDIAN


TESSIAN HLS INTELLIGENCE
3,872
Anomalous Emails Detected

Phishing awareness training: How effective is security training?

Phishing awareness training is an essential part of any cybersecurity strategy. But is it enough on its own? This article will look at the pros and cons of phishing awareness training – and consider how you can make your security programme more effective.

Tessian reports

Pros of phishing awareness training

Employees learn how to spot phishing attacks

While people working in security, IT, or compliance are all too familiar with phishing, spear phishing, and social engineering, the average employee isn't. The reality is, they might not have even heard of these terms, let alone know how to identify them.

But, by showing employees examples of attacks – including the subject lines to watch out for, a high-level overview of domain impersonation, and the types of requests hackers will generally make – they'll immediately be better placed to identify what is and isn't a phishing attack.

It's a good chance to remind employees of existing policies and procedures

Enabling employees to identify phishing attacks is important. But you have to make sure they know what to do if and when they receive one, too. Training is the perfect opportunity to remind employees of existing policies and procedures. For example, who to report attacks to within the security or IT team.

Training should also reinforce the importance of other policies, specifically around creating strong passwords, storing them safely, and updating them frequently. After all, credentials are the number one 'type' of data hackers harvest in phishing attacks.

Security leaders can identify particularly risky and at-risk employees

By getting teams across departments together for training sessions and phishing simulations, security leaders will get a bird's eye view of employee behaviour. Are certain departments or individuals more likely to click a malicious link than others? Are senior executives skipping training sessions? Are new-starters struggling to pass post-training assessments?

These observations will help security leaders stay ahead of security incidents, can inform subsequent training sessions, and can help pinpoint gaps in the overall security strategy.

Training satisfies compliance standards

While you can read more about various compliance standards – including GDPR, CCPA, HIPAA, and GLBA – on our compliance hub, they all include a clause that outlines the importance of implementing proper data security practices.

What are 'proper data security practices?' This criterion has – for the most part – not been formally defined. But, phishing awareness training is certainly a step in the right direction and demonstrates a concerted effort to secure data company-wide.

It helps organisations foster a strong security culture

In the last several years (due in part to increased regulation) cybersecurity has become business-critical. But, it takes a village to keep systems and data safe, which means accountability is required from everyone to make policies, procedures, and tech solutions truly effective.

That's why creating and maintaining a strong security culture is so important. While this is easier said than done, training sessions can help encourage employees – whether in finance or sales – to become less passive in their roles as they relate to cybersecurity, especially when gamification is used to drive engagement.

Cons of phishing awareness training

Training alone can't prevent human error

People make mistakes. Even if you hold a three-hour-long cybersecurity training session every day of the week, you'll never be able to eliminate the possibility of human error. Don't believe us? Take it from the UK's National Cyber Security Centre (NCSC) "Spotting phishing emails is hard, and spear phishing is even harder to detect. Even experts from the NCSC struggle. The advice given in many training packages, based on standard warnings and signs, will help your users spot some phishing emails, but they cannot teach everyone to spot all phishing emails."

That's right, even the UK's top cybersecurity experts can't always spot a phishing scam. Social engineering incidents – attacks that play on people's emotions and undermine their trust – are becoming increasingly sophisticated.

For example, using Account Takeover techniques, cybercriminals can hack your vendors' email accounts and intercept email conversations with your employees. The signs of an account take-over attack, such as minor changes in the sender's writing style, are imperceptible to humans.

Phishing awareness training is always one step behind

Hackers think and move quickly and are constantly crafting more sophisticated attacks to evade detection. That means that training that was relevant three months ago may not be today. In the last year, we've seen bad actors leverage COVID-19, Tax Day, furlough schemes, unemployment checks, and the vaccine roll-out to trick unsuspecting targets. What could be next?

Training is expensive

According to Mark Logsdon, Head of Cyber Assurance and Oversight at Prudential, there are three fundamental flaws in training: it's boring, often irrelevant, and expensive. We'll cover the first two below but, for now, let's focus on the cost.

Needless to say, the cost of training and simulation software varies vendor-by-vendor. But, the solution itself is far from the only cost to consider. What about lost productivity?

Imagine you have a 1,000-person organisation and, as a part of an aggressive inbound strategy, you've opted to hold training every quarter. Training lasts, on average, three hours. That's 12,000 lost hours a year. While – yes – a successful attack would cost more, we can't forget that training alone doesn't work. *(See point 1: Phishing awareness training can't prevent human error.)*

Phishing awareness training isn't targeted (or engaging) enough

Going back to what Mark Logsdon said: Training is boring and often irrelevant. It's easy to see why. You can't apply one lesson to an entire organisation – whether it's 20 people or 20,0000 – and expect it to stick. It has to be targeted based on age, department, and tech-literacy. Age is especially important.

According to Tessian's latest research in the Psychology of Human Error Report, nearly three-quarters of respondents who admitted to clicking a phishing email were aged between 18–40 years old. In comparison, just 8% of people over 51 said they had done the same. However, the older generation was also the least likely to know what a phishing email was.

Jeff Hancock, the Harry and Norman Chandler Professor of Communication at Stanford University and expert in trust and deception, explained how tailored training programmes could help:

"A one-size-fits-all approach won't work. Different generations have grown up with tech in different ways, and security training needs to reflect this. That's not to say that we should think that people over 50 are tech-illiterate, though. Businesses need to consider what motivates each age group and tailor training accordingly. Being respected at work is incredibly important to an older generation, so telling them that they don't understand something isn't an effective way to educate them on the threats. Instead, businesses should engage them in a conversation, helping them to identify how their strengths and weaknesses could be used against them in an attack. Many younger employees, on the other hand, have never known a time without the internet and they don't want to be told how to use it. This generation has a thirst for knowledge, so teach them the techniques that hackers will use to target them. That way, when they see a scam, they'll be able to unpick it and recognise the tactics being used on them." Jeff Hancock – Harry and Norman Chandler Professor of Communication at Stanford University

Should I create a phishing awareness training programme?

The short answer: 'Yes'. These programmes can help teach employees what phishing is, how to spot phishing emails, what to do if they're targeted, and the implications of falling for an attack.

But, as we've said, training isn't a silver bullet. It will curb the problem, but it won't prevent mistakes from happening. That's why security leaders need to bolster training with technology that detects and prevents inbound threats. That way, employees aren't the last line of defence.

But, given the frequency of attacks year-on-year, it's clear that spam filters, antivirus software, and other legacy security solutions aren't enough. That's where Tessian comes in.

How does Tessian detect and prevent targeted phishing attacks?

Tessian fills a critical gap in security strategies that SEGs, spam filters, and training alone can't.

By learning from historical email data, Tessian's machine learning algorithms can understand specific user relationships and the context behind each email. This allows Tessian Defender to detect a wide range of impersonations, spanning more obvious, payload-based attacks to difficult-to-spot social-engineered ones like CEO Fraud and Business Email Compromise.

Once detected, real-time warnings are triggered and explain exactly why the email was flagged, including specific information from the email. Best of all? These warnings are written in plain, easy-to-understand language. These in-the-moment warnings reinforce training and policies and help employees improve their security reflexes over time. To learn more about how tools like Tessian Defender can prevent spear phishing attacks, speak to one of our experts and request a demo today. □

Sponsors and exhibitors

Beyond Identity | Strategic Sponsor

Organisations rely on Beyond Identity to secure identities on the internet. Beyond Identity secures access to SaaS applications and cloud resources to protect data and privacy. Breaking down the barriers between cybersecurity, identity, and device management, Beyond Identity provides the most secure authentication on the planet, and dramatically improves the way the world logs in.

With the Beyond Identity Passwordless Identity Platform, organisations can eliminate passwords, positively verify user identities, confirm device trust, and enforce risk-based access controls. Beyond Identity enables security teams to implement zero-trust so their organisations can safely and securely work in hybrid-work environments with increasingly cloud-centric IT. Organisations turn to Beyond Identity to stop cyber-attacks, protect their most critical data, and meet compliance requirements.

We offer SaaS, subscription-based software.

Founded in 2019, Beyond Identity is headquartered in NYC, and has offices in Boston, Dallas and London.

For more information, please visit www.beyondidentity.com

Flow | Strategic Sponsor

Flow is the smart choice for secure cloud transformation. The expert team provide secure and efficient datacentre, network and cloud native solutions to allow organisations to do business in confidence, with seamless transition and without fear of a cybersecurity attack.

We harness the best of the old and the new world through best-of-breed technology to help our customers transition in a secure fashion, optimise performance and enhance capability.

With over 12 years of experience at the highest level, we build trusted relationships with our customers supporting them wherever they are on their digital transformation journey. Cybersecurity is built into the fabric of our solutions, enabling organisations to operate securely and stay ahead of the modern threat landscape.

For more information, please visit www.flowtransform.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

Tessian | Strategic Sponsor

Tessian is a machine intelligent email security platform that automatically prevents security threats like misaddressed emails, unauthorised emails and non-compliance. Tessian uses machine learning to understand normal email communication patterns in order to automatically identify email security threats in real time, without the need for end user behaviour change or pre-defined rules and policies. Tessian makes email safe at some of the world's largest enterprises across the financial, legal and technology sectors.

To find out more, visit www.tessian.com

Abnormal Security | Education Seminar Sponsor

Abnormal Security provides a leading cloud-native email security platform that leverages AI-based behavioural data science to stop business email compromise (BEC) and never-seen-before attacks that evade traditional secure email gateways (SEGs). Abnormal delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including phishing, malware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The Abnormal platform delivers inbound email security, internal and external account takeover protection, and full SOC automation. Abnormal's API-based approach enables customers to get up and running in 15 minutes and can augment a SEG or be used standalone to enhance native Microsoft security protection. Abnormal Security is based in San Francisco, CA.

More information is available at abnormalsecurity.com

Ankura Consulting Group | Education Seminar Sponsor

Ankura Consulting Group, LLC is an independent global expert services and advisory firm that delivers services and end-to-end solutions to help clients at critical inflection points related to change, risk, disputes, finance, performance, distress, and transformation. The Ankura team consists of more than 1,700 professionals in more than 35 offices globally who are leaders in their respective fields and areas of expertise. Collaborative lateral thinking, hard-earned experience, expertise, and multidisciplinary capabilities drive results and Ankura is unrivaled in its ability to assist clients to Protect, Create, and Recover Value.

For more information, please visit www.ankura.com

Arctic Wolf | Education Seminar Sponsor

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organisations end cyber-risk by providing security operations as a concierge service. Arctic Wolf solutions include Arctic Wolf® Managed Detection and Response (MDR), Managed Risk, Managed Cloud Monitoring and Managed Security Awareness – each delivered by the industry's original Concierge Security® Team. Highly trained Concierge Security experts work as an extension of internal teams to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to give organisations the protection, resilience and guidance they need to defend against cyber-threats.

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

Egress | Education Seminar Sponsor

Egress makes digital communication safer for everyone. As advanced and persistent cybersecurity threats continue to evolve, we recognise that people get hacked, make mistakes, and break the rules. Egress's Intelligent Cloud Email Security suite uses patented self-learning technology to detect sophisticated inbound and outbound threats, protect against data loss, resulting in the reduction of human activated risk.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

For more information, please visit www.egress.com

Kocho | Education Seminar Sponsor

At Kocho, we believe greatness lies in everyone. That's why we exist, to help companies realise their potential. By combining the power of Microsoft cloud technology with world-class identity, cybersecurity and our team of brilliant people – we take our clients on a journey of secure transformation.

And we're with you every step of the way. Because the path to greatness isn't walked alone. We help you adopt and embrace the right tech solutions at the right time.

The result? Sustainable and secure growth that amplifies your business success.
Kocho. Become greater.

For more information, please visit kocho.co.uk

Obsidian Security | Education Seminar Sponsor

Obsidian Security is the first truly comprehensive threat and posture management solution built for SaaS. Our platform consolidates data across core applications to help your team optimise configurations, reduce over-privilege, and mitigate account compromise and insider threats. The company was founded in 2017 by industry experts from Carbon Black and Cylance including Ben Johnson, Glenn Chisholm and Matt Wolff. Notable Fortune 500 companies trust Obsidian Security to secure SaaS applications, like Salesforce, Workday, Microsoft 365, ServiceNow, Google Workspace and Github. Headquartered in Southern California, Obsidian Security is privately held and backed by Menlo Ventures, IVP, Greylock, GV, Norwest Venture Partners, and Wing.

For more information, visit www.obsidiansecurity.com

CyberGuard Technologies | Networking Sponsor

CyberGuard Technologies, the specialist CREST-accredited cybersecurity division within the OGL Group provides a full range of IT security services from its 24/7 UK Security Operations Centre.

The OGL Group is the preferred technology partner to over 1,300 UK businesses, including those in the legal and financial services sectors. We are accredited by the world's leading IT and cybersecurity vendors to deliver best-in-class managed IT services and cybersecurity solutions.

Our 45-year heritage has earned OGL Group an enviable reputation for delivering first-class service and tailored solutions built on our extensive knowledge and experience. We also pride ourselves on remaining at the forefront of emerging technologies to enable modern businesses to digitally transform their operations and protect themselves from the growing threat from cybercriminals.

For more information, please visit www.ogl.co.uk/cyber-security

Exabeam | Networking Sponsor

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimise false positives, and make security success the norm.

For more information, please visit www.exabeam.com

The Missing Link | Networking Sponsor

We provide a full range of IT consulting and professional IT support services to businesses in all industries and market sectors, both in Australia and in the UK. Our highly skilled team of IT specialists includes cybersecurity, IT infrastructure/Cloud and robotic process automation experts, with many years of experience and a commitment to delivering first-class solutions that exceed our customers' expectations.

For more information, please visit https://www.themissinglink.com.au/

5TH JULY 2022

SECURING THE LAW FIRM

AGENDA

08:00 Registration & networking

08:50 Chairman's welcome

09:00 **What has risk got to do with technology?**

Karen Jacks, CTO, Bird & Bird

- Buying technology platforms
- Managing the people
- The boring process bit

09:20 **Why attack surfaces heat up with remote work**

Amir Ben-Efraim, CEO, Menlo Security

- Why has the pivot to new working models increased cyber-risk?
- How are attackers leverage Highly Evasive Adaptive Threats (HEAT) to launch ransomware attacks?
- What can organisations do to avoid the next class of browser-based attacks?

09:40 **Staying ahead of cybersecurity threats in today's undeniably digital world**

Etienne Greeff, CEO, Flow

- Current geopolitical events together with the exponential increase of Ransomware means the risk for businesses has never been higher
- Identify and understand the current state of the cybersecurity threat landscape
- How businesses can securely harness the best of technology
- How we operate in a world with carrier grade adversaries

10:00 **Why do they do that? Harnessing psychology to inform information security in organisations**

Marco Cinnirella, Professor of Applied Social Psychology, Royal Holloway

- How to best leverage insights offered by psychology when investigating risky information security behaviours
- Understanding how risk perception is impacted by cognitive biases, culture, and the 'psychological work contract'
- Why a mixed methods approach to collecting data is vital
- How psychology can inform communication and education
- Why you can never completely 'design out' behavioural issues

10:20 **Education Seminars | Session 1** **See pages 21 and 22 for more details**

Abnormal Security	Egress
Key considerations for choosing the right email security platform	**The changing email threat landscape**
David Lomax, Systems Engineer, Abnormal Security	**Jack Chapman,** Vice President of Threat Intelligence, Egress

11:00 Networking break

11:30 **EXECUTIVE PANEL DISCUSSION** **The big risks**

Mark Jones, CISO, Allen & Overy (Moderator); **Valerie Jenkins,** CISO, Clyde & Co; **Steve Davies,** Head of Cyber Security, DLA Piper

- Combating ransomware in the legal sector
- Addressing supply chain risk in an effective way
- Cutting your cloth

12:00 **Why legacy MFA is not good enough for modern authentication requirements**

Chris Meidinger, Technical Director, Beyond Identity

- A brief history of MFA
- We look into why traditional MFA was appropriate at the time but has kept up with the progress of attackers
- We detail the dangers posed by passwords and traditional MFA that requires a second device and/or push notifications
- Finally we cover off the alternative which is unphisable passwordless MFA

12:20 **Navigating the dark corners of social engineering attacks**

James Alliband, Senior Product Strategy Manager, Tessian

- Attackers have successfully infiltrated organisations through advanced social engineering techniques that exploit people's behaviour and vulnerabilities
- The success rate of these attacks has led to some of the worst data breaches in history. Still today, the number one method for delivering socially engineered attacks is via email
- In this session, we will walk you through socially engineered attacks found by the Tessian Threat Intelligence Team and what you can do to prevent these attacks

12:40 **Education Seminars | Session 2** **See pages 21 and 22 for more details**

Ankura

Cyber-risk management in focus

Ryan Rubin, Senior Managing Director, Cybersecurity, Digital Forensics and Incident Response; **Tanya Gross,** Senior Managing Director, Cybersecurity, Data Analytics & eDiscovery; **Steve Sandford,** Senior Director, Cybersecurity, Digital Forensics and Incident Response; and **Ahsan Qureshi,** Senior Director, Cyber Security Risk Advisory, Ankura

Arctic Wolf

Security by chance or security by choice? The conundrum of security operations faced by law firms

Nick Dyer, Senior Systems Engineer, Arctic Wolf

13:20 Lunch break

14:30 **SENIOR LEADERSHIP PRIORITIES PANEL**

Steve Davies, Head of Cyber DLA Piper (Moderator); **Karen Jacks,** CTO, Bird & Bird; **Karl Knowles,** Head of Cyber, HFW; **Jonathan Freedman,** Head of Technology & Security, Howard Kennedy; **Annette Brown,** Head of IT, Milbank

- Data privacy or security? How will companies view 'security' in the post-pandemic world?
- Hybrid working: problem solved or problem postponed?
- The issue of 'basic' cyber-hygiene (or 'why can't we stop ransomware?')
- Is 2022 the year of Cloud? And have the security implications of Cloud been exaggerated?
- The future of the security stack: insource/outsource/reduce number of solutions/rely on large application and infrastructure providers more
- Reining in the costs of cybersecurity

15:00 **What should you have in your post-breach legal toolbox?**

Hans Allnutt, Partner & Cyber & Data Risk Practice Leader, DAC Beachcroft

This session will look at the current legal landscape for affirmative action following cyber-incidents and data breaches including:

- Actions against 'persons unknown': what benefits can suing an unknown hacker bring?
- Ransom payments: in what circumstances are they unlawful or illegal?
- Who is to blame when email breaches give rise to payment frauds?

15:20 **Education Seminars | Session 3** **See pages 21 and 22 for more details**

Kocho

The verdict is out! How to empower digital transformation without sacrificing security

David Guest, Solution Architect and Technology Evangelist, Kocho

Obsidian Security

Obsidian Security: Extending Zero Trust to SaaS

Chris Fuller, Principal Product and Solutions Architect, Obsidian Security

16:00 Networking break

16:30 **Vulnerability management in the real world**

Steve Davies, Head of Cyber, DLA Piper

- Vulnerability management, then and now
- Prioritisation and compliance (risks vs. patch all the things)
- The move to DevSecOps, quick wins = big wins

16:50 **Creative operational security dashboard**

Noha Amin, Head of Information and Cybersecurity, TLT LLP

- Key aspects of dashboards
- Types of dashboards
- How to improve security dashboard quality

17:10 **The cyber-insurance market – managing risk**

Will Slater, Technology and Cyber Practice Director, Gallagher

- State of the cyber-market
- The challenges (red flags)
- State of coverage
- The journey (risk management)

17:30 Drinks reception & 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: 10:20–11:00

Abnormal Security

SESSION 1
10:20–11:00

Key considerations for choosing the right email security platform

David Lomax, Systems Engineer, Abnormal Security

Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organisation – deploying malware, leaking valuable data, or stealing millions of dollars. Unfortunately, email threats are only growing in number. Business email compromise accounts for 44% of all losses to cybercrime, and the 2021 Verizon DBIR holds that phishing remains the top entry point for breaches – a position it has held for years.

Does that mean email is doomed, and we should give up? Quite the opposite – instead, we should look to newer technologies and an integrated security strategy that provides a modernised approach to email defence. In this webinar, we do just that.

Attend the Abnormal Security session for answers to your most pressing questions, including:

- What are modern email threats, and how are they different from legacy attacks?
- Which email threats are most concerning, and how can we defend against them?
- Which technical capabilities are required from modern email security providers?
- How do modern email security companies use AI, machine learning and data science to detect the most dangerous and costly attacks?

Egress

SESSION 1
10:20–11:00

The changing email threat landscape

Jack Chapman, Vice President of Threat Intelligence, Egress

Cybercriminals continue to launch increasingly sophisticated social engineering attacks. This is driven by crime as a service ecosystem, change in human behaviour and hardening of traditional routes into organisations. Because of these factors and more, it's no surprise that 85% of today's security breaches involve a human element.

Join this presentation to learn more about:

- Today's email security landscape and how the threats are evolving
- The behaviours behind email data breaches
- Why legacy approaches are no longer fit for purpose
- How to use behavioural science and zero trust to take back control over data loss
- How real-time teachable moments are more effective at changing human behaviour than traditional security awareness training

Session 2: 12:40–13:20

Ankura

SESSION 2
12:40–13:20

Cyber risk management in focus

Ryan Rubin, Senior Managing Director – Cybersecurity, Digital Forensics and Incident Response, **Tanya Gross,** Senior Managing Director – Cybersecurity, Data Analytics & eDiscovery, **Steve Sandford,** Senior Director – Cybersecurity, Digital Forensics and Incident Response, and **Ahsan Qureshi,** Senior Director – Cyber Security Risk Advisory, Ankura

Securing the law firm in 2022 remains a challenge. In 2021, we saw examples of how cyber-exposures have adversely impacted companies in the legal sector. Our threat analysis on a sample of the industry in 2022 generates further food for thought. The key question is what else can law firms be doing to reduce their cyber-risk exposure. Join Ankura experts in this presentation as we discuss several challenges facing law firms today and some practical strategies to get ahead of the risks and reduce the likelihood of common breach scenarios impacting the industry.

- Key threats facing law firms today
- Understanding law firm structural inherent risks

SECURING THE LAW FIRM

- Key risk reduction strategies
- Tactics, techniques and procedures to drive down impact from breaches
- Recent case studies and key lessons learnt

Arctic Wolf

SESSION 2
12:40–13:20

Security by chance or security by choice? The conundrum of security operations faced by law firms

Nick Dyer, Senior Systems Engineer, Arctic Wolf

- How can legal firms mitigate the growing alert & process fatigue whilst managing the increasing cyber-risk across an exploding multi-cloud attack surface?
- Why cyber-insurance premiums are on the rise, and proactive measures to ensure your business is covered
- We'll share our perspective running one of the world's largest security operations services, handling over 2 trillion security events per week
- How Arctic Wolf's Security Operations Cloud, and the Concierge Security Team, detected & remediated against ransomware for a customer.

Session 3: 15:20–16:00

Kocho

SESSION 3
15:20–16:00

The verdict is out! How to empower digital transformation without sacrificing security

David Guest, Solution Architect and Technology Evangelist, Kocho

Over the last 2 years, the way many law firms work has radically changed, with increases in virtual working, remote access, and cloud adoption. All of this is driving an explosion in apps, devices and users across an increasingly complex infrastructure.

As the barriers blur between who is in your network and out of it, organisations struggle to manage identities and secure access for not only their employees but external partners, suppliers, and even clients. Learn how Microsoft technologies can help you provide secure, seamless, and compliant access to your business apps and data whilst striking the perfect balance between productivity and security.

Join this seminar as we examine:

- *Exhibit A:* How to enable seamless and secure end-user authentication
- *Exhibit B:* How to protect critical resources with Conditional Access
- *Exhibit C:* Why you should put identities at the heart of your security framework
- *Exhibit D:* How to establish passwordless authentication in Azure AD

Obsidian Security

SESSION 3
15:20–16:00

Obsidian Security: Extending Zero Trust to SaaS

Chris Fuller, Principal Product and Solutions Architect, Obsidian Security

In a world where the natural evolution towards SaaS was accelerated by remote working during the pandemic, do the principles of Zero Trust still apply? SaaS currently makes up 75% of the cloud, yet SaaS security visibility is notoriously difficult for security teams to manage, given the expertise, visibility and control required to manage each disparate SaaS application.

Meanwhile, integrations between SaaS applications create a highly interconnected environment. With more sensitive business data entrusted to SaaS than ever before, it's time to consider how best we secure those applications.

In this session, we'll explore how the Zero Trust principles of continuous verification, breach impact limitation and facilitation of rapid incident response can be applied to SaaS applications.

- Review the guiding principles of Zero Trust
- Learn the inherent risks of SaaS usage and why securing SaaS applications goes beyond the identity provider
- Understand how the principles of Zero Trust can be applied to SaaS □

Speakers and panellists

Securing the Law Firm is delighted to welcome delegates, speakers and panellists. The event has attracted a large number of key names and decision-makers from Legal Services Firms and from a cross section of other industries.

James Alliband

Senior Product Strategy Manager, Tessian

James is a cybersecurity strategist, responsible for leading and defining product strategy at Tessian. With nearly 10 years experience in the security industry, James has successfully implemented tried-and-tested product strategy and frameworks in high growth organisations. Prior to joining Tessian, James held senior strategy roles at VMWare Carbon Black and CheckPoint Technologies.

Hans Allnutt

Partner & Cyber & Data Risk Practice Leader, DAC Beachcroft

Hans leads DAC Beachcroft's multi-award winning cyber risk and breach response team. He has responded to hundreds of breaches and cyber-incidents, helping clients of all sizes, from SME to global corporates across all sectors. He is a true specialist and trusted advisor, guiding clients through their crisis and defending any regulatory investigation and privacy litigation that follows. Hans has also advised on cyber and data protection compliance programmes, as well as responding to information rights requests (e.g. DSARs). As a litigator, Hans advises on disputes and injunctive relief. His practice includes national and international litigation, arbitration and other forms of dispute resolution.

Noha Amin

Head of Information and Cybersecurity, TLT LLP

Noha Amin acts as the central point of information security contact within law firm TLT whilst also managing its info sec team and the company-wide business continuity forum. Amin plans, manages and undertakes internal and third-party audits on IT governance, information security and controls. A strong advocate and representative voice for women in cybersecurity.

- Featured Top 30 Women in Tech in Manchester, by Manchester Evening News
- Featured Top 50 NW Technology Transformers, by BusinessCloud DTX
- Featured in 'One Golden Nugget' Wisdom Book UK
- Featured Cybersecurity SHE RealModel UK
- Multi Awards Winner (USA, Canada, UK, Middle East)
- Multi Awards Judge (Canada, and UK)
- Manchester Tech Trust Member
- Advisory Board Member for CISO Council–Middle East and Chairwoman for WLCS initiative (Women Leaders in Cybersecurity)
- Advisory Board Member for OWASP ME (Open Web Application Security Project – Middle East) – WICS initiative (Women in Cyber Security)
- Advisory Committee Member for Cybersecurity Resilience Conference, Abu Dhabi
- Podcaster, Speaker, Panellist (Live Conferences, Virtual Conferences, and Webinars) for Cybersecurity and Women empowerment conferences in the UK and the Middle East-Dubai

Amir Ben-Efraim

Co-founder and CEO, Menlo Security

Amir Ben-Efraim is Co-founder and CEO of Menlo Security. Previously, Amir was Vice President of cloud security at Juniper Networks where he helped define the company's strategy to secure the virtualised data centre, public and private clouds. He joined Juniper via its acquisition of Altor Networks, which he led as Founder and CEO. Prior to Altor, Amir was an executive at Check Point Software, a pioneer in internet security. He holds an MBA from UCLA, an MSEE from Stanford University and a BSEE from UC Berkeley.

Annette Brown

Head of IT, Milbank

As Head of IT for Milbank in Europe, Annette is responsible and accountable for the smooth running of the firm's information technology systems in the London, Frankfurt and Munich offices. Annette manages the IT team, who are responsible for delivering day to day IT/helpdesk support, IT training, system management and IT infrastructure & projects.

SECURING THE LAW FIRM

Jack Chapman

Vice President of Threat Intelligence, Egress

Jack Chapman joined Egress as part of their acquisition of Aquilai in June 2021. He co-founded Aquilai in 2018 and oversaw the development of its anti-phishing solution. Based on its technological excellence and vision, Aquilai was hand-selected by the National Cyber Security Centre (NCSC), the UK Government's intelligence and security agency, for its Accelerator program and benefitted from in-depth and strategic insights for product development.

Marco Cinnirella

Professor of Applied Social Psychology, Royal Holloway

Marco Cinnirella is a Professor of Applied Social Psychology at Royal Holloway, one of the UK's leading psychology departments. He has published widely in peer-reviewed scientific journals on a diverse range of topics such as attitudes, behaviour change, group dynamics and cyber-psychology, and uses a diverse range of qualitative and quantitative techniques in his research.

Marco's expertise in behaviour change has led him to advise a range of organisations on behavioural information security challenges, including large multi-nationals in the energy, oil and pharmaceutical sectors. His expertise in behavioural information security challenges has led to invited addresses at the United Nations and he has delivered keynote addresses on information security and psychology at various academic and industry conferences.

Steve Davies

Head of Cyber Security, DLA Piper

Transformational cybersecurity leader striving to be the nexus between risk and innovation. Demonstrable track record in delivering game changing improvements that allow organisations to move fast safely.

Nick Dyer

Senior Systems Engineer, Arctic Wolf

Nick serves as a Senior Systems Engineer at Arctic Wolf, and has spent the last 15+ years working for emerging enterprise IT technology companies delivering innovations such as server & network virtualisation, flash storage and cloud/AI/predictive analytics. Most recently following an acquisition by HPE, Nick served as a global Field CTO for storage, working with engineering & customers to introduce new products to market, and focusing on IT operational experience with predictive analytics and AI. In early 2021 Arctic Wolf and it's Security Operations Cloud entered EMEA in which Nick was the founding EMEA SE. Nick blogs occasionally at https://www.dyertribe.co.uk.

Jonathan Freedman

Head of Technology & Security, Howard Kennedy

Jonathan Freedman is the Head of Technology & Security at London law firm Howard Kennedy, with a background in enterprise architecture and systems engineering within the UK professional services sector spanning more than 18 years, now focusing on information and cybersecurity. Working closely with teams from across the firm, his role includes both the review, development and implementation of new technology within the firm and leading the firm's internal cybersecurity/cyber-awareness programmes. In addition, he holds multiple industry certifications including, Certified Ethical Hacker, CGEIT, CISSP, TOGAF, and ISO27001 with special interests in cybersecurity, ethical hacking & penetration testing, data protection, cryptography, secure systems design, mobile device security and technology innovation.

Chris Fuller

Principal Product and Solutions Architect, Obsidian Security

Chris Fuller is Principal Product and Solutions Architect at Obsidian Security. Chris works with leading enterprises across EMEA to uncover their

SaaS security challenges and help them rapidly deploy Obsidian's technology to safeguard the business-critical data held in SaaS apps like Microsoft365, Workday, Salesforce and more. Today, the Obsidian platform secures over 4 million unique SaaS users and thousands of interconnections between SaaS apps.

Chris has spent the last decade specialising in web and cybersecurity technologies, focusing on tuning and securing user experiences for major brands across Europe and the Middle East. Prior to Obsidian, Chris built the EMEA Sales Engineering team for Shape Security and managed that team following the $1bn acquisition by F5.

Etienne Greeff

CEO,
Flow

Etienne is one of the early pioneers of internet security. Etienne first got involved in cybersecurity in 1994, after he graduated university. He really has seen the development of the industry from the very beginning. He has spent over 20 years promoting the innovative use of technology and building services to solve complex issues. He has been involved in numerous general management roles during his career but has enjoyed staying close to the technology. He came aboard Flow as CEO in December 2020, leading the transformation of Flow becoming the smart choice for secure cloud transformation.

Tanya Gross

Senior Managing Director – Cybersecurity, Data Analytics & eDiscovery, Ankura

Tanya has spent the past decade managing investigations and disputes that involve data (unstructured, structured, and semi-structured formats). She has led large scale evidence and disclosure management exercises in the UK, France, Switzerland, Hong Kong, Japan, the Middle East, and the US. She leads the team's client delivery and practice development efforts across Europe, the Middle East and Africa (EMEA), and Asian Pacific (APAC), including e-discovery, digital forensics, information security, structured analytics, and custom solutions. As an accomplished practitioner, Tanya is able to convey the technical detail in a language her clients understand. Having worked in the industry for a long period, Tanya has a thorough understanding of the challenges involved in managing large scale data management exercises and has become a trusted advisor in her field. Her experience covers a wide variety of clients in both the private and public sector, including financial services, construction, retail, and manufacturing, and a wide variety of issues including arbitration, litigation, intellectual property, fraud, antitrust/competition, regulatory, and employment matters. Tanya was also recognised in the Who's Who Legal Consulting Experts list in 2019.

David Guest

Solution Architect and Technology Evangelist, Kocho

As Kocho's Solution Architect and Technology Evangelist, David is responsible for developing identity, Microsoft 365 security, and other cloud service solutions – and keeping our clients abreast of the latest technology trends. His 20+ years of experience across a wide range of identity and security technologies including Unix, Linux, IBM, and Novell, helps him design and implement great solutions on behalf of our clients. He is a regular presenter at our events and Microsoft roadshows, presenting to large and small audiences, and trying to turn technobabble into something resembling English.

Karen Jacks

CTO,
Bird & Bird

Karen is CTO at international law firm Bird & Bird providing strategic planning, delivery and support of IT solutions, information security and telecommunications to 30 offices in Europe, Middle East, US, Asia and Australia. Karen has overseen the rapid expansion of Bird & Bird and has built the international team and solutions to support this. She has led the Firm through a number of technology and business projects and is a regular and active contributor to articles and conferences particularly in legal IT, legaltech and emerging technologies. She is involved in a number of advisory boards including ILTA and a keen supporter of diversity in technology and part of the DELTAs driving forward diversity in IT and related topics.

Valerie Jenkins

Chief Information Security Officer, Clyde & Co LLP

Valerie has been part of the information security profession for more than 25 years. While working in UK Government, Valerie represented the UK at Western European Union security working group and has held information security leadership positions in several global companies in the automotive, financial services, and pharmaceutical sectors. Valerie's career has taken her to live in Switzerland, South Africa, returning to the UK to join a global insurance broker and is now with Clyde & Co as their first global CISO. Valerie is passionate about balancing cyber-protections with business strategy and bringing commercial understanding to cyber-strategy and solutions.

Mark Jones

CISO,
Allen & Overy

An award winning CISO and risk management and security professional operating at executive level for the last 10 years with experience of leading large teams on both a global and national basis to deliver and sustain:

- Cybersecurity for globally recognised high privacy brands and tier 1 CNI providers
- Regulatory compliance programmes in response to regulatory scrutiny
- Internal and external audit support (analysis and programme delivery)
- Business and service continuity
- Information security across all industry verticals

Experience includes leading both end user, IT service provider and management consulting teams and encompasses leadership of the global cybersecurity & IT compliance business for Atos Group, development and deployment of the cybersecurity strategy for BAA/Heathrow Group as an end user CISO and the leadership of the Global Information Security agenda as CISO for Allen & Overy.

Karl Knowles

Head of Cyber and Service Delivery, HFW

A well-established security leader with extensive experience and views on cybersecurity. Karl has presented thought provoking and meaningful content to a wide range of different audiences. After a long career, with a multitude of experience, he is very well respected in the industry. Karl began his career as a Communications Engineer in the British Army. In the second half of his career, he was employed within multiple information security roles, advising senior military leadership on the global deployment of information and communications systems. He then built upon this successful 25-year military career moving to consultancy at BSI and then, Deloitte LLP. It was during this time that Karl quickly established himself as a subject matter expert, advising private and public clients towards the development of improved cyber and privacy strategies. He is a champion of veteran's employment, a full member of the Chartered Institute of Information Security and a Fellow of the Chartered Management Institute.

David Lomax

Systems Engineer,
Abnormal Security

David Lomax is an experienced Systems Engineer with over 18 years' experience in the cybersecurity landscape, working across email, network, data and applications. He is also seasoned in cloud-based threat detection and response. His knowledge extends to multiple industry sectors including banking, manufacturing, legal, pharma and critical national infrastructure.

Chris Meidinger

Technical Director,
Beyond Identity

Over the past 20 years, Chris has driven revenue via both pre-sales and post-sales with IT security and communications solutions. His initial career was spent with VARs, architecting and deploying custom solutions to meet specific business requirements. For the last decade, he's been in sales engineering at emerging, venture-backed security companies. He specialises in bringing value to customers by synthesising complex technical concepts into simple business value propositions and presenting tailored, data-driven investment proposals to senior executives to earn their business.

Ahsan Qureshi

Senior Director – Cyber Security Risk Advisory, Ankura

Ahsan Qureshi is a Senior Director at Ankura's global cybersecurity practice and focuses on proactive cybersecurity services in the EMEA region. Ahsan holds an MSc and has over 15 years' experience of Big 4 and industry in helping organisations establish robust cybersecurity environments, strategies and security transformation programmes. Ahsan has worked across industries including a number of law firms. He led a large back to compliance programme for a global law firm.

Ryan Rubin

Senior Managing Director, Cybersecurity, Digital Forensics and Incident Response, Ankura

Ryan brings over 23 years of global Big 4 and boutique experience to help clients holistically manage complex cyber and tech challenges from the boardroom to the network. He has a passion for helping others reduce their risks and is curious about making the digital and physical world safer to live in. Ryan has partnered with many global information security, risk, internal audit and general councils throughout his career. He has led specialist proactive and event-driven matters covering cybersecurity strategy and execution, governance, e-crime investigations, compliance, data and technology advisory and assurance, IT resilience, incident response, data privacy, due diligence, e-discovery and regulatory compliance. Before Ankura, Ryan set up Cyberian Defense, supporting virtual CISO, breach response and non-exec board positions; as well as partnering with Accenture on cyber-insurance pre and post breach services. Prior to Cyberian Defense, he was an EY equity assurance partner, leading EMEA cybercrime, DFIR services and responsible for UK cyber-services in TMT. Specific engagements include cybercrime investigations, cryptocurrency frauds, ransomware, BEC, breaches, software and shadow audits, insider threat programmes, strategy reviews, cybersecurity audits, due diligence, and blockchain security.

Steve Sandford

Senior Director – Cybersecurity, Digital Forensics and Incident Response, Ankura

Steve is a knowledgeable cybersecurity professional with more than 12 years' experience from within law enforcement as well as in the private sector. Steve has experience in the investigation of cybersecurity incidents as well as assessing organisations readiness for such incidents. He has helped large, medium, and small corporate organisations with digital forensics and cyber-investigations, and has also assisted with workflow development, policy and procedure writing, and the implementation of in-house capabilities for multi-national organisations. The types of investigations with which Steve has assisted clients with include business email compromise, ransomware, malware, network intrusions, PCI investigations, insider threat and breach of internal usage policies. Steve has prepared hundreds of expert witness level reports and witness statements for use in criminal and civil courts, as well as tribunals, and has experience presenting evidence in criminal and civil courts on many occasions. He has given evidence in the Central Criminal Court of England and Wales, the Old Bailey, on a case where the victim was defrauded of over €2.5m. After being cross-examined by two defence barristers, Steve's testimony helped convict both defendants.

Will Slater

Technology and Cyber Practice Director, Gallagher

Will is a Director in the Technology & Cyber Practice, where he leads the team focusing on large complex global clients in placing and mitigating their cyber-risk. Sample clients include international law firms, major global retailers and complex manufacturers, including those that have suffered 8 figure ransomware losses. Prior to Gallagher, Will worked for the specialist London wholesale broker Miller. □

Cyber-risk management still in focus

Get back to basics and get ahead of the breach before it is too late.

Ryan Rubin, Tanya Gross, Steve Sandford and Ahsan Qureshi report

Law firms and the legal services sector continue to be prime targets for cyber-threats due to the nature of sensitive information and data they hold. Information may include commercial information about M&A activity, private client or employee data, confidential client disclosure material relating to disputes or litigation and financial data. A successful cybersecurity incident not only poses a serious threat to the law firms, but also to the companies and individuals they represent. In addition to the reputational damage and financial loss, in some cases cyber-exposure even threatens the very existence of the company. For example, in 2016 MOSSACK FONSECA had to close its doors, after suffering a devastating data leak.

The risk of cyber-threat continues to grow and jolt the industry. Recently, one of the Top 100 law firms, Ward Hadaway was blackmailed and asked for £4.75 million after confidential documents were stolen in a cyber-attack.[1] Another example is the resurgence of the DeathStalker APT group. First emerging in 2018 and threatening the legal sector, DeathStalker have continued to update its toolset to make its attacks more efficient. They also use online platforms, such as YouTube, Google+, and WordPress, to execute stealthy command and control mechanisms to conduct cyber-attacks quickly and effectively.

A recent UK legal services cybersecurity survey by Menlo reported that over 92% of respondents identified a cyber-attack as being very damaging to their business. 90% of respondents were also concerned about data loss and an inability to operate. The report also stated that despite 77% of respondents switching to home working during the pandemic, less than 60% had changed their cybersecurity measures to address home working. Also, almost 47% of respondents introduced digital services and only 52% felt that their organisations are prepared to deal with a cyber-attack.[2] This correlates with Ankura IR case trends that the root causes of ransomware attacks often relate to phishing attacks targeting users and poor patching of external remote access/VPN infrastructure. This combination, when found in companies with inadequate planning, poor endpoint control, poor data governance and use of insecure remote access, often led to costly breaches.

> Financial gain and other motivations are driving cybercriminals and other threat actors to rapidly evolve their techniques. This is exacerbated by the digitisation, reliance on cloud technologies and increase in home working.

Financial gain and other motivations are driving cybercriminals and other threat actors to rapidly evolve their techniques. This is exacerbated by the digitisation, reliance on cloud technologies and increase in home working. Other factors leading to the legal industry being under-prepared for the cyber-threats include people, process, and technology aspects:

- Law firm partners tend to manage their own engagements as practitioners and make decisions on third-party tool adoption without seeking independent advice.
- Many law firms fully outsource IT operations and lack dedicated IT security owners.
- There is often a lack of security investment, governance, and management oversight due to cybersecurity being treated as an IT issue, rather than a business risk.
- There are often manual processes such as over reliance on e-mail to share sensitive information internally and with clients.
- Disparate systems, common applications used across the industry and custom solutions expose the industry to wide-spread supply chain attacks.
- Legal teams often support the M&A deal lifecycle leading to multiple IT environments and systems being used. Often, there is a lack of control and ownership of where data for these solutions are hosted.
- Evolving cyber-threat landscape, and the threat actors are getting more resourceful.
- Increased outsourcing and dependence on third parties as well as remote/home working and bring your own devices further expanding the attack surface.
- There is a general lack of security awareness among staff.

Law firms require a more active cybersecurity risk management to get ahead of cyber-threats. Key actions to reduce the impact of cyber-attacks include:

- Have an agreed set of technology providers minimises the risk of tracking where client data and matter data are hosted.

It is clear with the emerging landscape of threats that face the legal industry that more can always be done to be better prepared and resilient to withstand cyber-attacks.

- Ensure cybersecurity ownership, oversight, and reporting are established and align accountability to skilled individuals and/or credible external providers.
- Understand threat landscape, key threats, and cybersecurity risks and priorities.
- Align with industry good practice standards to develop a security baseline.
- Set a security budget and develop a security plan aligned with business risk appetite.
- Develop cyber-policies and procedures, along with a security awareness programme to promote security culture and socialise across the business and key suppliers.
- Ensure security hygiene across the IT environment including use of critical cyber-technologies e.g. antivirus, endpoint detection and response tools to help prevent, detect, and mitigate/contain malware and other cyber-threats.
- Monitor and assess third-party risk on a continuous basis. Identify stakeholders who are responsible for onboarding and are key relationship stakeholders.
- Implement a proactive incident response plan and know recovery capability and options in an event of an incident e.g. IR retainer service, self vs external insurance.

It is clear with the emerging landscape of threats that face the legal industry that more can always be done to be better prepared and resilient to withstand cyber-attacks. Recent breaches have drawn attention to clients and regulators who will be expecting more from their legal advisors in future. Get back to basics as outlined in this article and get ahead of the breach before it is too late. □

[1] https://www.lawgazette.co.uk/news/ward-hadaway-blackmailed-after-cyber-attack/5112294.article

[2] https://info.menlosecurity.com/rs/281-OWV-899/images/IRN-Menlo-Cybersecurity-Legal-Research%20Report-May-22.pdf

For more information, please visit
www.ankura.com

At Ankura we are committed To Help Law Firms Mitigate Risk

We tailor our services to support our clients' requirements across a variety of event driven scenarios. Our specialist team of experts advise clients on proactive measures to increase information security, data security and privacy through best practices.

We are also able to rapidly respond in the event of an incident or data breach drawing upon a truly global team with the technical expertise to remediate the crisis quickly and provide decisive strategic and tactical advice on improvements to cyber and privacy programmes.

PROTECT, CREATE, AND RECOVER VALUE

ankura™

IS A LEADING BUSINESS ADVISORY AND EXPERT SERVICES FIRM.

1,700+ PROFESSIONALS
serving
3,000+ CLIENTS
doing business in
55 COUNTRIES

| Cybersecurity & Data Privacy
| E-Discovery & Digital Forensics
| Data Analytics, Strategy & Governance
| Litigation, Arbitration & Disputes
| Expert Witness

Contact Us
ankuracyber@ankura.com
EMEA Incident Response Hotline: +44 (0) 207 015 8811 | incident@ankura.com

ankura.com

Survey reveals UK cybersecurity professionals overworked and lack confidence to stop cyber

A few highlighted takeaways of a survey of 300 security and IT workers in the UK.

Arctic Wolf reports

In April and May of this year, we commissioned a survey of 300 security and IT workers in the United Kingdom, and today we are publishing the results. They reveal the attitudes and beliefs that cybersecurity practitioners have about their day-to-day working experience. Here are a few highlighted takeaways.

Front-line cybersecurity experts lack confidence to protect UK organisations

With cybersecurity being a top-of-mind concern for executives and boards of directors, over a quarter (27%) of front-line cybersecurity personnel do not feel knowledgeable enough as an individual to spot a cyber-threat. Additional insights from the survey include:

- Nearly one-third (30%) of those working in cybersecurity claim they do not know how to use their organisation's security tools effectively
- Only 19% of cybersecurity practitioners feel that the team they work on is effective at stopping cyber-attacks
- 35% of cybersecurity professionals claim they have forgotten what they have learned because training happens too infrequently

UK cybersecurity professionals are struggling to find a work-life balance

With the volume of threats increasing each year, and organisations being susceptible to an attack around the clock, cybersecurity professionals in the UK are overwhelmed by work, with half of them claiming to be regularly working over 40 hours per week. Other work-life imbalance findings include:

- More than a quarter (26%) of cybersecurity workers claim their job has a negative impact on their mental health
- 56% of practitioners believe they would be blamed by management if their organisation experienced a breach
- 25% of those working in cybersecurity were unable to use all of their holiday entitlement last year

Cybersecurity practitioners are in high demand and actively looking for new opportunities

There is a global cybersecurity skills shortage and UK-based practitioners are increasingly aware of the value their skills have on the open market, with nearly half (44%) of survey respondents saying they have recruiters contacting them about new job opportunities multiple times per month. Other insights include:

> Cybersecurity professionals in the UK are overwhelmed by work, with half of them claiming to be regularly working over 40 hours per week.

- 79% of practitioners received a pay increase below the rate of inflation last year
- More than a third (34%) of cybersecurity workers say they are thinking about changing jobs in 2022
- 39% of practitioners believe they would be able to find a job in their field in under a month

Female security professionals remain the minority; diversifying hires offers upside for all

Cybersecurity practitioners in the UK remain overwhelmingly male, with only a third of survey respondents identifying as female. Employers would be wise to further diversify their cybersecurity hiring, not only to bring additional perspectives to their IT and security teams, but also because female practitioners are more likely to stay with their current employer for a longer period, with the survey revealing:

- Less than a quarter (23%) of female practitioners are thinking of changing jobs this year, compared to 40% of their male counterparts
- Over two-thirds (68%) of women cybersecurity professionals believe they can advance their cybersecurity career at their current employer □

Learn more at **arcticwolf.com/uk**

ARCTIC WOLF

Four reasons to outsource your managed security service

An outsourced MSSP can provide a higher-quality and more cost-effective option than building an in-house security function.

Anna Webb reports

Too often, organisations get hung up on cost when considering outsourced security. While getting value for money is important, it's worth prioritising some other important advantages of using a managed security service.

If you're considering how to improve the security posture of your financial services company, an outsourced managed security services provider (MSSP) can provide a higher-quality and more cost-effective option than building an in-house security function.

Using an MSSP can help you:

1. Overcome the skills gap

There's no shortage of headlines about the cybersecurity skills gap, but there is a shortage of people to fill it. Many smaller businesses have only one employee responsible for cybersecurity and they're often a general 'IT person' rather than a cyber-specialist. Large organisations tend to be better resourced with four to five people in cyber-roles, but still struggle to attract and retain talent.

This means they often don't have enough resources to implement essential cybersecurity practices such as firewalls, anti-malware, and data encryption.

Working with an MSSP means savings on recruitment, salaries, bonuses, benefits, and training – plus, your security partner will help establish the optimal security system configurations.

2. Ensure security at all times

Security incidents aren't known for their convenience – they'll happen when you least expect. Even a minor breach can lead to system downtime and delays in service delivery. These can vary from the mildly frustrating to business-critical – particularly in a heavily regulated industry such as the financial services sector.

An outsourced MSSP provides you with consistent and undisrupted monitoring, through both technology and human expertise. By establishing better threat monitoring and security reporting, you also get actionable insight to further improve your security posture.

> More tools isn't always the answer, it's about getting the *right* tools and having the *right* people set-them up correctly and manage them on an ongoing basis.

3. Access the latest technology

The sheer amount of security solutions on the market is intimidating, with updates and new technology appearing all the time. But more tools isn't always the answer, it's about getting the *right* tools and having the *right* people set-them up correctly and manage them on an ongoing basis.

By working with an MSSP, they can guide you to security solutions with the optimal price-to-value ratio – and then implement, integrate, and scale selected technologies within your existing infrastructure.

4. ...and, of course, save money

Cybersecurity can be an expensive function to establish in-house. Setting up an in-house SOC for an organisation with up to 1,000 users can cost up to £1,033,500 over three years in CAPEX and OPEX costs. That's often unrealistic for small- and medium-sized companies.

Partnering with an MSSP, however, could save you over £893,500 in the same time frame. These savings come from not having security staff on the payroll and not having to invest in constant upskilling and training.

Any MSSP worth their salt will ensure the right tool selection and optimise your costs. This ensures that you're spending what you need to secure your operations, vs. going for the vendor-recommended (but not the most cost-effective) technology. □

Anna Webb is Head of Security Operations at Kocho, a leading provider of cybersecurity, identity, and Cloud IT services.

For more information, please visit **kocho.co.uk**

Kocho

The psychology of social engineering and phishing

What specific psychological tricks do cybercriminals use? And how can we use that knowledge against them?

Egress reports

There's a reason phishing attacks are known as *social* engineering. They're human-activated, and simply don't work unless someone takes the figurative bait. That's why even though phishing originates externally, it falls under the umbrella of insider threat – someone internal needs to make a mistake.

Phishing is ultimately an emotional attack. It plays on our emotions and tricks us into doing something we wouldn't normally do when we're concentrating at our best. So what specific psychological tricks do cybercriminals use? And how can we use that knowledge against them?

Why do we still fall for phishing?

Many people think they would never fall for a phishing attack (or scams in general) because they're educated, experienced professionals. They may even have gone through rigorous cybersecurity training. However, this overconfidence can lead to complacency, which is exploited by criminals.

In fairness, most people with even basic cybersecurity training *do* know the warning signs of phishing. They're diligent at work, and they don't act recklessly. The truth though, is there are times when any of us can become stressed, tired, or forced to rush. It's in those mindsets where we're most error-prone, and far better targets for phishing.

For that exact reason, cybercriminals have been quick to pounce on the fallout of the COVID-19 pandemic. Our research shows only 28% of remote workers have access to a solo office, while 46% feel pressured to use email outside of office hours (often from mobile devices). Among others, these factors have made it even easier for hackers to press on the psychological triggers that make phishing so effective.

> There are times when any of us can become stressed, tired, or forced to rush. It's in those mindsets where we're most error-prone, and far better targets for phishing.

Psychological triggers in phishing

The purpose of a phishing attack is to pull us out of our mindset of questioning the validity and security of communications. Consider the hallmarks of the most common form of social engineering – email phishing. These are just some of the psychological triggers scammers use to make us think emotionally, rather than logically.

- *Urgency:* a phishing email usually wants something done *right now,* as the longer you have to think, the more you may question whether it's legit
- *Plausibility:* the days of foreign princes offering a share of their fortune have gone… modern phishing attempts will be based on real-life, often mundane scenarios
- *Familiarity:* there's been a marked rise in spear phishing, where the attack is at least partially tailored to an individual – often claiming to be from an authority figure such as their CEO or head of security
- *Confidentiality:* the action required is specific to you and needs to be done by you alone, as getting someone else involved increases the chances of the scam being spotted

It's also common for criminals to target people who have just moved to new companies (info that often can be easily found on social media), as fear and anxiety are powerful motivators. These people are more likely to be anxious to impress a new boss and unaware of the subtle signs that something is amiss with their communication style. If you've worked under a CEO for many years, you'll most likely see the signs of a scam email. On your first day of work? Perhaps not.

Can we use psychology to protect ourselves?

According to Dr Jessica Barker in a recent Egress webinar, the key to stopping phishing could lie in behavioural economics. We process information in two ways: the calm, collected way where we analyse problems in a measured, thoughtful manner. Like doing a difficult maths sum. And then the second, more impulsive way, where we act almost on autopilot – such as driving a car on an empty road.

Phishing attacks use psychological triggers to push us away from the first frame of mind and into the

Egress Defend uses machine learning to analyse the content and context of emails in the background, offering people gentle traffic-light warning prompts when the signs of phishing emerge.

second. They wants us to act quickly, clicking and responding in autopilot rather than in a slow, analytical manner. That's why urgency is so key in phishing – if we came back to the email later in the day, we might not fall for it on closer inspection.

It's for this exact reason that so many people have an 'oh no…' reaction almost immediately after they've fallen for a phishing scam. We see the same thing with misdirected email. As soon as our brain slows down again, we begin to question what we just did. The training is remembered and the warning signs of a mistake start to creep in.

The problem businesses have is that it's all very well understanding these psychological nuances – but how can they help people in practice? How can we get employees to think that split-second earlier? The good news is we can, with a little help from technology.

Evening the odds with human layer security

Cybercriminals aren't looking for technological gaps to exploit when it comes to phishing – they're trying to find cracks in the human layer. That's also why the answer to phishing isn't ever going to be technology alone. It's about empowering people to become an integral part of an organisation's defence, rather than seeing them simply as a security problem to be mitigated.

Human layer security tools such as Egress Defend are able to give people a nudge back towards their calmer, more collected way of thinking. Because as we noted before, most of the time people can be trusted to do the right thing. Egress Defend uses machine learning to analyse the content and context of emails in the background, offering people gentle traffic-light warning prompts when the signs of phishing emerge.

Some phishing emails will always slip through the defences, so we need to tap into psychology to beat them. Criminals use psychological triggers to turn people into security risks – so we provide the tools to even up the odds and turn people into security assets. Most employees know the right thing to do, and it's about offering a technological guardrail that can nudge them back towards the place where they make smart security decisions.

For more information, please visit
www.egress.com

The rise of social engineering success: What CISOs need to know

Targeted attacks have greater potential to cause disastrous consequences for your company, despite the fact that you receive far fewer of them.

Mike Britton reports

While traditional email security tools may be able to prevent the overwhelming majority of spam messages, phishing attempts, and other deceptive emails from ever reaching your inbox, these aren't the only types of threats you need to worry about.

The truth is, targeted attacks – like business email compromise, supply chain fraud, ransomware, and account takeover – have greater potential to cause disastrous consequences for your company, despite the fact that you receive far fewer of them. And because they have few traditional indicators of compromise (like a malicious attachment or suspicious link), they also have a higher likelihood of being safely delivered.

Email is still the primary attack vector

Although real-time collaboration tools like Slack and Microsoft Teams have skyrocketed in popularity over the past two years, email remains the go-to channel for asynchronous communication. And because our universal dependence on email is unlikely to end anytime soon, it will continue to be an attractive vehicle for cyber-attacks.

Because they provide access to individuals at companies anywhere in the world, email attacks are highly lucrative. The recent FBI IC3 report has shown that loss from business email compromise continues to increase, costing organisations $2.4 billion last year, and our research shows that the average supply chain compromise attack costs an organisation more than $180,000.

In addition, cybercriminals are successful in their account compromise attempts 12% of the time, enabling them to access and use real user accounts to run their attacks. These stats indicate the severity of the problem and showcase the fact that it isn't going away anytime soon.

Modern cybercriminals have learned how to hack the human, rendering the tools that look only for traditional indicators of compromise nearly obsolete.

Traditional indicators of compromise are becoming obsolete

Unlike attacks of the past, modern cybercriminals don't have to compromise their victims' existing infrastructure to execute their attacks. Instead, they have the resources to build their own infrastructure, which is more reliable than a hijacked system and can support attacks that bypass the secure email gateway. These infrastructures can even be quickly adapted to attack certain targets.

Further, while business email compromise may appear to be less sophisticated than designing and installing malicious software, it's often a more effective approach because the technology wasn't developed to stop these kinds of attacks. By removing malicious attachments and suspicious links and instead relying entirely on text-based communication, it's easier for threat actors to circumvent conventional security measures.

In essence, modern cybercriminals have learned how to hack the human, rendering the tools that look only for traditional indicators of compromise nearly obsolete.

Modern tactics focus on compromising people, not just hardware

Threat actors have started to move away from tricking targets into downloading infected attachments or clicking on malicious links. Rather, they're focusing on triggering an emotional response – most often urgency or worry – via social engineering.

Recently, we've seen a resurgence of conversation hijacking, a type of attack that is less of an all-out assault and more of a slow play. Threat actors will first gain access to an employee's credentials through a credential phishing attack and then enter their inbox and browse through their messages until they find the right opportunity to 'take over' an existing conversation. Once they've found that opportunity, they then reply to a thread with a request for sensitive data or payment for a nonexistent invoice.

Conversation hijacking capitalises on our innate desire to be cooperative and assume positive intent. When we receive an email from a colleague or partner asking for assistance of some kind, generally

Any moderately-sized organisation will have to endure at least one (if not multiple) attacks per day. What sets the victims apart from the companies who simply experience intrusions, however, is that the latter are actively searching for fraudulent activity.

our first instinct is to be helpful, not suspicious – exactly what attackers are banking on. Consequently, understanding when an account has been compromised and then blocking these attacks before your employees can respond to them is fundamental to minimising your organisation's risk.

Social engineering attacks can be exceptionally costly

What makes account takeovers particularly pernicious is that once a cybercriminal manages to get through the door, they can fly under the radar for months. Sitting in the background undetected, they can obtain untold volumes of valuable data about the company and its customers, which they can then sell or leverage for future attacks.

Or, in the case of vendor fraud, the perpetrators can take advantage of recurring payments to collect considerable sums of money. A colleague of mine shared the story of one retailer who paid millions of dollars worth of fraudulent invoices after an attacker created a fake supplier profile in the retailer's inventory management system. For more than six months, the cybercriminals successfully received payment for fake orders until the company finally realised what was happening.

What's worse is that in some cases, the fraudsters don't even have to access the account, instead relying on domain spoofing or display name deception to run their scams.

Threat monitoring and quick responses are essential

Unfortunately, when it comes to mitigating attacks, the odds are stacked against the average business. A cybercriminal only has to succeed once to cause long-term damage, which is incredibly scary given the fact that large enterprises can have hundreds of millions of email accounts.

While organisations should have a layered approach to stopping these attacks, attempting to eliminate all fraudulent activity is an exercise in futility.

Any moderately-sized organisation will have to endure at least one (if not multiple) attacks per day. What sets the victims apart from the companies who simply experience intrusions, however, is that the latter are actively searching for fraudulent activity.

They understand that the be-all, end-all of information security isn't only to keep the bad actors out, but to be able to respond quickly and quash any threats once they've been identified, should they bypass security infrastructure.

CISOs at these organisations prioritise both the prevention of successful attacks, as well as the identification and immediate remediation of intrusions. Their systems focus on responding quickly to contain the issue and minimise any losses. And they recognise that people are the last line of defence, ensuring that they understand the risk through security awareness training.

Protect your organisation by modernising your email security

The vast majority of cybercrime today is successful because it hijacks the people behind the keyboard. The best thing you can do is to stop these attacks before they reach them, and the most effective way to do that is to use a behavioural-based approach that evaluates identity, context, and content to establish known good and block the messages that deviate from it.

Abnormal Security helps you keep your business safe by preventing high-impact targeted attacks. Check out our Gartner Peer Reviews to see why organisations worldwide trust our cloud-native email security platform to protect them from the attacks that matter most.

Mike Britton is CISO at Abnormal.

For more information, please visit **abnormalsecurity.com**

Abnormal

e-Crime & Cybersecurity Mid-Year Summit 2022

e-crime & cybersecurity MID-YEAR

19th October 2022
London

“ Insightful, relevant and thought provoking; no hard sells, sensible practical approaches to current day cybersecurity challenges. ”

Head of Information and Cyber Security, McArthurGlen Group

“ Thanks, very enjoyable. Look forward to my invitation to the March event. Thanks to everyone making this possible in these difficult times. I actually spent the whole day on it! ”

Director of Global Security, American Express

“ Thank you for the update and the invitation to join yesterday’s session. I found the conference to be very informative (as always) and covered the threat landscape in a timely manner. The presenters were excellent and the introduction/ continuity was executed to perfection. The content was superb [...]Thank you for the invitation again and I hope to catch up with you in person at the March 2022 event. ”

Information Security, AIB Group Technology Services

“ It’s been a wonderful experience to attend this virtual conference. Many thanks for organising the event. ”

Information Security Officer/ Data Protection Manager, Jein Solicitors

2021 sponsors included:

Principal Sponsor

F-Secure.

Strategic Sponsors

BeyondTrust

DARKTRACE

MENLO SECURITY

okta

proofpoint.

Recorded Future®

SentinelOne™

Education Seminar Sponsors

appgate

axis security

bitglass

corelight

CybelAngel

CyGlass by NOMINET

DEVO

CISCO KENNA Security

onelogin

PICUS

RANGEFORCE

RED SIFT

For more information, please visit
akjassociates.com/contact-us

Thank you to all our sponsors

Strategic Sponsors

BEYOND IDENTITY

FLOW the smart choice

MENLO SECURITY

TESSIAN

Education Seminar Sponsors

Abnormal

ankura

ARCTIC WOLF

egress

Kocho

OBSIDIAN

Networking Sponsors

CyberGuard Technologies

exabeam

themissinglink
Australia • United Kingdom