Post event report

Strategic Sponsors

BeyondTrust
CROWDSTRIKE
DARKTRACE
Menlo Security
proofpoint.
RANGEFORCE
SentinelOne

Education Seminar Sponsors

bitglass
Centrify ZERO TRUST PRIVILEGE
corelight
Google Cloud
INTSIGHTS Defend Forward
KENNA Security
MORPHISEC Moving Target Defense
netwrix
okta
Recorded Future
Synack
TERRANOVA SECURITY
yubico

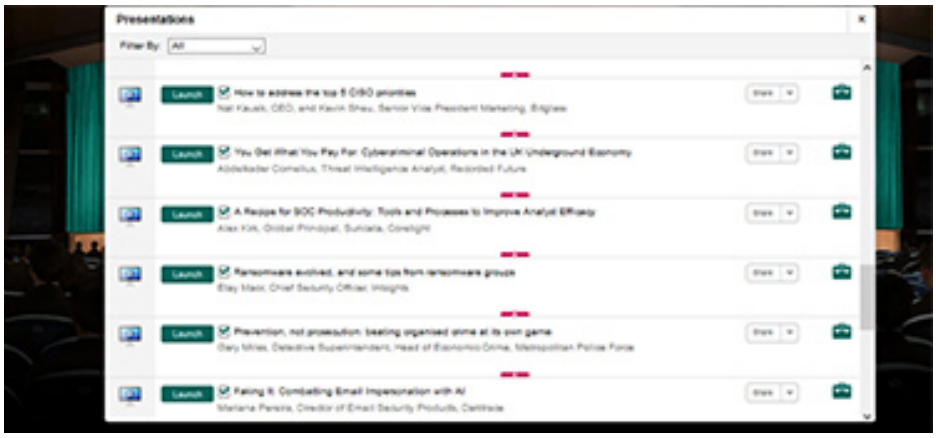
“ Thanks, very enjoyable. Look forward to my invitation to the March event. Thanks to everyone making this possible in these difficult times. I actually spent the whole day on it! ”

Director of Global Security, American Express

“ 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

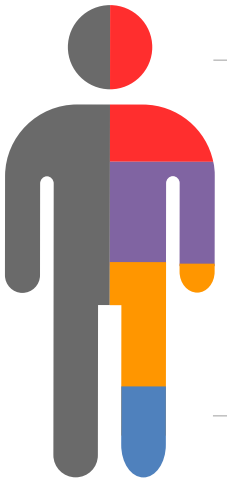
Inside this report:



Key themes

- Cybersecurity for business resilience
- Securing and protecting remote employees
- Protection versus business needs
- Rethinking identity and access management
- Cybersecurity by remote control
- Securing the workplace revolution
- Building in security: easier said than done?
- Securing the customer – are your websites up to it?
- Stuck in the Cloud

Who attended?



Cyber-security
We have a 15-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Benjamin Bell, Senior Security Specialist, Google Cloud Security

Simon Brady, Managing Editor, AKJ Associates Ltd

Dan Burns, Head of Cybersecurity, NEXT

Kevin Butler, CISSP Regional Principal Solutions Engineer, Okta

Rupert Collier, Director of Sales – EMEA and APAC, RangeForce

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

Richard Davis, International Cybersecurity Strategist, Proofpoint

Jonathan Freedman, Chief Technology and Information Security Officer, Howard Kennedy

Deborah Haworth, CISO, Penguin Random House

Luke Hebbes, Head of Cyber Security and Risk, HSBC

Alex Kirk, Global Principal, Suricata, Corelight

Daniel Klatt, Director of IT Risk, Commerzbank

Karl Lankford, Director Solutions Engineering, BeyondTrust

Craig McEwen, Global Head of Cyber Operations, Anglo American

James Mckinlay, Group Information Security Officer, Barbican Insurance

Tom McVey, Solutions Architect, Menlo Security

Raif Mehmet, AVP of EMEA, Bitglass

Milen Mihnev, Head of Technology risk and control, M&G

Gary Miles, Detective Superintendent, Head of Economic Crime, Metropolitan Police Force

Diana Moldovan, UK Cyber Intelligence Lead, Aviva

Chris Owen, Director of Product Management, Centrify

Mariana Pereira, Director of Email Security Products, Darktrace

Ronald Pool, Senior Solutions Engineer, CrowdStrike

Stephen Roostan, VP EMEA, Kenna Security

Eyal Rozen, Director of Sales EMEA & APAC, Morphisec

Justin Shaw-Gray, Account Director, Synack Inc

Ashish Shrestha, Director of Information Security, Clear Channel International

Ilia Sotnikov, Vice President of Product Management, Netwrix Corporation

Jan Tietze, Director Security Strategy EMEA, SentinelOne

Nick Truman, CSO, JATO Dynamics

Ste Watts, Head of Security Operations, Aldemore Bank

Mark Walmsley, CISO, Freshfields Bruckhaus Deringer

Neil Webster, Solutions Engineer, Yubico

Theo Zafirakos, CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

Agenda

08:00 Login and networking

08:55 Chairman's welcome

09:00 **Alienated from the mothership: reorienting a business and human focussed security policy in an alien landscape**

Nick Truman, CSO, JATO Dynamics

- COVID-19 frustration: how security policy is destabilised without a physical space to operate in. Audits cannot be conducted, standards cannot be verified, awareness cannot be guaranteed
- JATO's journey: how to go from having no security framework to a security framework funded by the board, intertwined into the business and considered critical by stakeholders
- How to reorient a business focused security programme: access management, education and control
- Understanding your assets and why you might be hacked. A proxy attack is still an attack

09:20 **Reducing time to containment: THE security priority**

Jan Tietze, Director Security Strategy EMEA, SentinelOne

With limited resources, an ever-growing skills gap and an escalating volume of security alerts, organisations are left vulnerable to what is perceived to be unavoidable risk. This environment is demanding more of already resource-constrained CISOs. In this keynote we will be discussing how automation can help to:

- Drastically reduce the amount of uninvestigated and unresolved alerts
- Automate time-consuming investigations and remediate well-known threats
- Act as a force multiplier for resource-constrained security teams

09:40 **UPM: Empowering a remote workforce and improving your security posture with Universal Privilege Management**

Karl Lankford, Director Solutions Engineering, BeyondTrust

The new normal of a remote workforce has changed the threat model of the organisation overnight. Join this session and learn:

- Considerations for a secure remote working environment
- How to balance remote workers security and productivity
- Recommendations to support a remote workforce with a PAM solution

10:00 **EXECUTIVE PANEL DISCUSSION** **Resilience, risk and innovation in the financial services**

It is no secret that when it comes to the maturity of security frameworks, the financial services lead the way. Heavy regulation, plentiful resources and technological maturity drive large financial institutions towards investment in tooling and staff to prevent incidents and ward off the cybercriminals who are attracted by the large amount of cash at stake. However, like all other organisations there have been paradigm shifts for security practitioners in the financial services as a result of C19 and the subsequent overdrive towards digitisation. Cybersecurity has been proven to be central to operational resilience, but does this mean that all digitised functions in the financial services are safe?

Luke Hebbes, Head of Cyber Security and Risk, HSBC
Milen Mihnev, Head of Technology risk and control, M&G
Daniel Klatt, Director of IT Risk, Commerzbank

10:20 **Education Seminars | Session 1**

Centrify	Google Cloud Security	Okta	Synack	Terranova Security
Identity-centric privilege management for cloud	**Transform your security strategy with data-driven detection**	**Zero trust in practice: why identity drives next-gen access**	**Next generation defence: using hackers to beat hackers**	**How security awareness training can protect your hybrid workforce against increasing cyber-threats**
Chris Owen, Director of Product Management, Centrify	**Benjamin Bell,** Senior Security Specialist, Google Cloud Security	**Kevin Butler,** CISSP Regional Principal Solutions Engineer, Okta	**Justin Shaw-Gray,** Account Director, Synack Inc, and **Mark Walmsley,** CISO, Freshfields Bruckhaus Deringer	**Theo Zafirakos,** CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

10:50 Networking break

11:20 **EXECUTIVE PANEL DISCUSSION** **Updating security culture and governance in the era of remote work**

The human element of cyber-risk has always been a major bugbear for CISOs. With workforces spread out and dispersed, how can controls be put in place to raise security awareness in a moment characterised by uncertainty and a high volume of cybercrime. Furthermore, how can the corporate governance model be dynamically adapted to the domestic workspace, and how can issues such as hardware, communication and strategy be effectively addressed.

Jonathan Freedman, Chief Technology and Information Security Officer, Howard Kennedy
Ashish Shrestha, Director of Information Security, Clear Channel International
Deborah Haworth, CISO, Penguin Random House
Craig McEwen, Global Head of Cyber Operations, Anglo American

11:50 **Hacking exposed: Tales from the front line**

Ronald Pool, Senior Solutions Engineer, CrowdStrike

- New attack techniques uncovered by CrowdStrike's threat hunting and incident response teams including: initial attack vectors and persistence, lateral movement and data exfiltration techniques
- Ransomware: Pay or cure. Is not having the intention to pay ransomware realistic? Can you handle an incident or intrusion alone or do you need specialist help? What are the hidden costs even if you do pay?
- Time to respond: Learn why security hygiene matters and how partnering can help solve the skills shortage in your security team. We will present new tips & tricks to improve your organisation's time to respond

Agenda

12:10 **Navigating a new normal: People are your most attacked asset and your most likely source of data loss – learn how to measure and reduce your people-based risk?**

Richard Davis, International Cybersecurity Strategist, Proofpoint

For the last few years people have been the most attacked asset and your most likely source of data loss. This risk has only increased over the last few months as organisations have adapted to a new way of working, often putting business continuity ahead of security and risk concerns. Join this session and learn:

- How to gain visibility into who your very attacked people are, what threats you face as an organisation and how to mitigate this risk through:
  - The latest detection and protection solutions
  - Deploying a meaningful security awareness training programme that drives behavioural change of your people
  - Changes to business processes that have the biggest impact to reduce risk
- How to gain visibility into where your sensitive data now resides and how to prevent both inadvertent and malicious data loss across
- Why the world's largest organisations are adopting our People Centric Security Framework

12:30 **Zero trust principles with internet isolation**

Tom McVey, Solutions Architect, Menlo Security

- The concept of zero trust holds that no actor, whether inside or outside the network, should be trusted to access information by default
- Internet isolation extends the idea of zero trust by assuming that all web traffic should not be inherently trusted
- Discover the benefits of isolation and how they increase at scale
- Learn how forward-leaning security professionals consider internet isolation as a vital element to achieving zero trust goals

12:50 **Education Seminars | Session 2**

Bitglass	Corelight	IntSights	Kenna Security	Recorded Future
How to adopt your cybersecurity strategy in the fast-changing age of digital transformation	**A recipe for SOC productivity: tools and process to improve analyst efficacy**	**Ransomware evolved – and some tips from ransomware groups**	**Rethinking & solving the patching problem: a new approach**	**You get what you pay for – cybercriminal operations in the UK underground economy**
Raif Mehmet, AVP of EMEA, Bitglass	**Alex Kirk,** Global Principal, Suricata, Corelight	**Etay Maor,** Chief Security Officer, IntSights	**Stephen Roostan,** VP EMEA, Kenna Security, and **Dan Burns,** Head of Cyber Security Operations, Next	**Abdelkader Cornelius,** Threat Intelligence Analyst, Recorded Future

13:20 Lunch and networking break

14:10 **Prevention, not prosecution: beating organised crime at its own game**

Fireside Chat with **Gary Miles,** Detective Superintendent, Head of Economic Crime, Metropolitan Police Force

- Cybercrime has increased in volume across 2020, as organised crime syndicates adopt a strategy of toss out the net and see what is caught. Cyber awareness has never been more important
- Companies who never thought they would have to seriously address the cybersecurity question have been forced to digitise and operate remotely. How they choose to move forward now may make or break their futures
- The Metropolitan Police Force understands that it is prevention and not a focus on prosecuting criminals that yields results
- Effective management of risks and vulnerabilities must characterise how businesses approach cybercrime. Together with law enforcement, a standard of proactive security must be the aim

14:40 **Faking it: Combatting email impersonation with AI**

Mariana Pereira, Director of Email Security Products, Darktrace

- Today, 94% of cyber-threats still originate in the inbox. 'Impersonation attacks' are on the rise, as AI is increasingly being used to automatically generate spear-phishing emails, or 'digital fakes' that expertly mimic the writing style of trusted contacts and colleagues
- Humans can no longer distinguish real from fake on their own, so businesses are increasingly turning to AI to distinguish friend from foe and fight back with autonomous response
- In an era when thousands of documents can be encrypted in minutes, learn how 'immune system' technology can take action in seconds and stop cyber-threats before damage is done

15:00 **Welcome to the future of cybersecurity training!**

Rupert Collier, Director of Sales – EMEA and APAC, RangeForce

- No more 5 day long, death by PowerPoint, classroom-based courses held in windowless basements in soulless hotels
- No more courses cancelled last minute and no unnecessary travel requirements
- Welcome to on-demand preparation for the real world, using real live VMs simulating real cyber-breach scenarios on a cloud-based platform
- Welcome to selecting your own missions, tailored to you, any time of day or night, learning at your own pace, from the comfort of your own browser

15:20 **Education Seminars | Session 3**

Morphisec	Netwrix	Yubico
Introduction to proactive prevention	**Calculating ROI for security: Why this is so difficult? Do you need it?**	**How secure are your shared workstations & mobile restricted environments?**
Eyal Rozen, Director of Sales EMEA & APAC, Morphisec	**Ilia Sotnikov,** Vice President of Product Management, Netwrix Corporation	**Neil Webster,** Solutions Engineer, Yubico

15:50 Networking break

16:20 **EXECUTIVE PANEL DISCUSSION** **Threat prevention, detection and response in the transformed enterprise**

The world has changed for business leaders and security practitioners. CISOs have had to deal with a large volume of attacks across a year characterised by uncertainty, and address issues from afar. But to what extent have the nature of threats changed? Sophisticated ransomware strains break headlines while spear phishing campaigns have increased in volume. Vulnerabilities must be addressed, and it is important for security leaders to pool together insights concerning the common threat landscape.

Diana Moldovan, UK Cyber Intelligence Lead, Aviva
Dan Burns, Head of Cybersecurity, NEXT
Ste Watts, Head of Security Operations, Aldemore Bank
James Mckinlay, Group Information Security Officer, Barbican Insurance

16:40 **Cybersecurity in the age of disorder**

Simon Brady, Managing Editor, AKJ Associates Ltd

Pandemic, digitalisation, climate change, the collapse of Chimerica, Brexit – the list goes on. In all this chaos, cybersecurity, like everything else, has to change. But how? In this session, AKJ's Managing Editor, Simon Brady, gives his take on where CISOs should be looking in 2021.
Stop talking about 'the business' and start understanding it

- From facilities management to strategic advisory, or….?
- Cyber ROI is dead, good riddance to bad rubbish?
- Making use of enforced transparency: a new solution paradigm

17:00 Networking **17:30** Conference close

Education Seminars

Bitglass

How to adopt your cybersecurity strategy in the fast-changing age of digital transformation

Raif Mehmet, AVP EMEA, Bitglass

Given the global pandemic and the sudden shift in how the workforce operates, the CISO community has faced an unprecedented set of challenges and questions. Several months into the transition, new struggles continue to arise, while many of the original ones remain unanswered.

Join Raif Mehmet as he shares best practices from our CISO community and provide recommendations for how to address challenges associated with new age of digital transformation

What attendees will learn:

- *Addressing and assessing current risks:* How to identify which assets are more vulnerable now than they were at the beginning of 2020
- *Optimising costs:* How to justify the spend that is necessary to secure the remote workforce today while preparing for tomorrow's 'new normal'
- *Quantifying ROI:* How to balance spending at a time when the business may be contracting
- *Business agility:* With resource and budget constraints, how to balance the growing demands on IT from remote work while protecting sensitive data

Centrify

Identity-centric privilege management for cloud

Chris Owen, Director of Product Management, Centrify

According to recent research by the Identity-Defined Security Alliance (IDSA), 59% of organisations say that cloud applications are driving a 5x increase in the number of identities over the past 10 years. And, over the past two years, 79% have had an identity-related breach. Digital transformation has massively expanded the threatscape, as modern technologies like cloud, DevOps, containers, microservices and more are creating an explosion in the number of machine identities in the IT estate. Now more than ever, it's vital to take an identity-centric approach to securing privileged access to resources in on-premises, hybrid, and multi-cloud environments.

Join us in this session where we will cover the following:

- How organisations have evolved their use of cloud
- How PAM solutions have transformed to support new methodologies and tooling
- The difference between a vault-centric and identity-centric approach to Privileged Access Management (PAM)
- 6 key challenges organisations face for DevSecOps when it comes to cloud, and how to solve them

Corelight

A recipe for SOC productivity: tools and process to improve analyst efficacy

Alex Kirk, Global Principal, Suricata, Corelight

Despite spending years building SOCs filled with millions worth of security tooling and SIEMs stuffed with all the data analysts could supposedly ever need, alert fatigue continues to be a serious problem for the majority of enterprise organisations. Time to resolve incidents remains considerably higher than the speed at which new events are pouring in. This talk will investigate why SOCs remain so inefficient in their investigations, and will propose a different method for collecting and operationalising security data that will both simplify process and dramatically speed investigations.

- Weaknesses of the current SIEM data collection model – operational and structural
- A clear alternative to the existing process that speaks to the specific problems outlined
- Walkthrough of freely available playbooks that make use of this new data paradigm in a SOAR for maximum analyst efficiency

Education Seminars

Google Cloud Security

Transform your security strategy with data-driven detection

Benjamin Bell, Senior Security Specialist, Google Cloud Security

Ever feel like your security team is overly reliant on vendor-created threat detection? There are nuances to your environment that often require a more customised approach to identifying potential TTPs. Furthermore, advanced threat actors may use methods, techniques and malware that are custom-made for your organisation. The art of detection is evolving as more investments are made into SOC analysts, threat responders, and hunters – and as part of this movement, data driven detection is emerging as the most accurate way to craft enterprise-specific detections.

Attend this session to learn how you can intelligently transform your security strategy by authoring detections, treating them as code, and putting best practices in place to use, store, share and maintain your custom detections.

- Learn how to get started with a custom detection security strategy
- Experience how the custom detection lifecycle provides insight into attacker behaviour
- Understand the core components of authoring detections
- See how you can incorporate security frameworks into your detections
- Learn how a data-driven approach to detection writing detections captures lessons learned and sustains institutional knowledge

IntSights

Ransomware evolved – and some tips from ransomware groups

Etay Maor, Chief Security Officer, IntSights

Ransomware attacks have become an everyday event, from sporadic attacks targeting individuals to targeted attacks against organizations. In this session we will not only review the ransomware attacks methodology and monetization but also look at what enables these attacks in the first place as well as get tips for avoiding these threats FROM THE CREATORS THEMSELVES! In addition we will review how operationalizing threat intelligence and preparedness can help mitigate such threats.

- Get tips from ransomware creators on how to avoid attacks
- Learn about ransomware groups, their tactics and techniques
- See how MITRE can be used to operationalize ransomware threat intel

Kenna Security

Rethinking & solving the patching problem: a new approach

Stephen Roostan, VP EMEA, Kenna Security, and **Dan Burns,** Head of Cyber Security Operations, Next plc

In the last six months there has been more pressure than ever on IT security functions to squeeze out as much value as possible from their budgets. In this session, Stephen and Dan look at why the area of vulnerability management offers an untapped opportunity to measurably decrease risk and deliver operational cost savings.

- Strategic and tactical benefits of designing a new framework
- Changing the patching mindset across all stakeholders
- Leveraging existing investments with future-proof, flexible tools
- Defining – and achieving – the right success metrics for your business

Morphisec

Introduction to proactive prevention

Eyal Rozen, Director of Sales EMEA & APAC, Morphisec

Despite continued infosec investments, data breaches continue while companies contend with complicated security architectures composed of disconnected technologies that produce mountains of non-actionable data. Security architecture can be broken down into three main elements: prevention, detection and remediation. A renewed focus on prevention may hold the answer.

In this session we will explain:

- How prevention should be considered the most strategically important defence element, as by default good true time zero prevention dramatically reduces latency, risks and operational costs of the security structure as a whole.
- How as advanced threats evolve and data centre transformation forces enterprise teams to consolidate security, the need for faster, easier and more deterministic threat prevention is essential
- How corporations need to consider a purpose-built stack of true prevention capabilities, that isn't available in a singular off-the-shelf solution, and add detection-based tools, which by definition have a huge latency, false alerts and are cost prohibitive, where and when appropriate, but not as a prevention tool.

Education Seminars

Netrix

Calculating ROI for security: Why this is so difficult? Do you need it?

Ilia Sotnikov, Vice President of Product Management, Netwrix Corporation

The ongoing stream of data leaks and other breaches of consumer trust is a top concern for executives at organisations around the world. To make sound decisions about cybersecurity strategy, especially during challenging times like these, when budgets are tight, they need accurate assessments of the effectiveness of proposed security investments. However, providing those estimates of ROI can be extremely difficult for CISOs, who often struggle to quantify the expected impact of security measures.

Join us for this educational session and learn:

- What the 4 key benefits of a security investment are
- How to effectively communicate the value of cybersecurity investment to senior decision makers
- How to convince executives to make data security investments right now

Okta

Zero trust in practice: Why identity drives next-gen access

Kevin Butler, CISSP Regional Principal Solutions Engineer, Okta

As organisations move the mobile and cloud-based Wi services, there is a move away from traditional perimeter-focused approaches to security. Instead resources are focused on enabling access for all users (employees, contractors, partners, etc.) regardless of their location, device or network and zero trust is quickly becoming the dominant security model for the cloud, shifting the perimeter from the network to the people and devices that make up a modern workforce. As a model with many moving parts, the immediate question is where to start? This discussion will focus on: the full zero trust reference architecture and steps to get there, Why identity is the foundational layer to build contextual access controls from.

- The traditional four walls that protected an organisation's data no longer exist: the rise of mobile and cloud adoption has led to more people, accessing more resources, and from more locations, than ever before
- In order to enable these mobile and cloud experiences without compromising on security, organisations are moving away from the network perimeter-centric view of security and instead focusing on access – and identity – as the new security control point
- This means that instead of viewing user security as two separate groups – trusted individuals, able to access everything inside an organisation, and untrusted individuals, kept on the outside – organisations now are taking a zero trust approach that assumes no one is inherently trusted, requiring verification for access
- This shift requires organisations to focus resources on securely enabling access for all of the various users (employees, partners, contractors, etc.) regardless of their location, device, or network.

Recorded Future

You get what you pay for – cybercriminal operations in the UK underground economy

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

In our digital age, companies that transact business online find their data targeted by various forms of cyber-fraud. These cyber-fraud products and access broker services can be bought and rented freely on the dark web with ease. This is fuelling sophisticated payment systems on the underground economy in the UK.

During this session, we will cover:

- Exclusive access to live threat intelligence feeds from the region
- A detailed review of some of the methods being used in the underground economy
- How to use security intelligence to defend your organisation

Synack

Next generation defence: using hackers to beat hackers

Justin Shaw-Gray, Account Director, Synack Inc., and **Mark Walmsley,** CISO, Freshfields Bruckhaus Deringer

There are many dilemmas in today's complex cybersecurity world. Year on year increases in cyber-attacks, an increase in the sophistication of these attacks, a widening cybersecurity talent gap – not to mention IT security budgets that haven't kept up with growing demands. In this session, Synack's Justin Shaw-Gray will host an open conversation with Mark Walmsley, CISO, Freshfields Bruckhaus Deringer LLP. Justin and Mark will discuss Synack's innovative crowdsourced security model and how Freshfields has ultimately made their platform a more secure place.

Attendees will learn how Freshfields Bruckhaus Deringer LLP:

- Is using an army of ethical hackers to harden corporate assets
- Has transformed and simplified security operations
- Reduced the costs of legacy testing programmes
- And is now quickly deploying safer applications

Education Seminars	
Terranova Security **How security awareness training can protect your hybrid workforce against increasing cyber-threats** **Theo Zafirakos,** CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security	Cybersecurity risks increase when companies adopt work from home practices or a hybrid work model with little time to prepare and inform their users of the associated risks. While some employees may still work from home, others may be back in the office. For many users, this is a completely new work situation. Cybercriminals know that many people are adapting to a new normal, which makes it easy to fool them with email, phone and text messages. Cyber-attackers are leveraging new techniques to trick unwary users. In this session, learn why it's so important to maintain cybersecurity awareness training and how to mitigate these hybrid workforce-related cyber-risks and more specifically: • What are the cybersecurity risks associated with the human factor when employees work remotely? • How can users defend themselves and their organisation against the increase in cyber-attacks? • Adopting a people-centric approach: how can cybersecurity awareness create a first line of defence? • How can security awareness leaders create a culture of security with a hybrid work model?
Yubico **How secure are your shared workstations & mobile restricted environments?** **Neil Webster,** Solutions Engineer, Yubico	Best practices for a secure and efficient user experience. The shared workstation or mobile restricted environment scenario is one that can be found across a variety of industries – from manufacturing to critical infrastructure to financial services to healthcare to retail. In these scenarios, multiple employees may be sharing more than their workstations. They may also be sharing passwords and access to sensitive information or protected data. These environments may also restrict mobile use, which nullifies common MFA methods such as SMS, mobile authenticator apps, or mobile push. Attend this session to learn about: • The challenges faced in shared device environments • Common shared device scenarios including shared kiosk, mobile restricted, grab and go, and POS • Customer case studies to address user experience and enable stronger security • Modern authentication for modern devices