WHITE PAPER

The Cybersecurity Landscape

2017 AND BEYOND: A REPORT

CompTIA

Introduction

In June 2017, CompTIA brought the cybersecurity community together at a roundtable discussion at the Churchill War Rooms in London, inviting representatives from different areas of the industry to share their insights on the state of the sector. The group discussed the most pressing current threats, what future threats could look like and what we can do to mitigate them.

Cybersecurity has never been a higher priority, with recent attacks such as the WannaCry ransomware attack bringing down dozens of National Health Service Trusts in May 2017, the Yahoo breach that saw one billion accounts compromised in December 2016, and the Dyn attack, which saw IoT devices turned into a huge botnet that brought down several online services. Cyber-attacks are increasing in scale and severity, and organisations are starting to recognise that they are now a matter of when, not if.

The borderless and seemingly indiscriminate nature of cyber-attacks mean it is of vital importance that industry share their insights and work together to protect themselves and the wider population.

In today's connected world, a breach on one organisation can compromise an entire supply chain. It can spell disaster for businesses, eroding public trust and perceptions, whilst leaving them in financial ruin, particularly when the General Data Protection Regulation (GDPR) comes into force. It is up to the legitimate security community to learn from each other and share what works and what does not. Most importantly, it's vital for us all to identify where we can improve and ensure we leave no one behind.

As the world's largest association of IT professionals with members all over the globe, CompTIA understands the industry's need to advance as a collective, especially in the midst of a skills gap, which is leaving organisations without enough staff to meet today's threats. At a time when we need to 'do more with less' every company can learn from the different approaches and cybersecurity practices of others and share best practice in the cybersecurity space.

This whitepaper has been produced as a result of the discussions that took place at the CompTIA-hosted roundtable. Executives from large and small businesses, technology vendors, cybersecurity training providers and security consultancies participated. Here, we offer a snapshot into the state of modern cyberthreats, and the group's key strategic recommendations for how all organisations can protect themselves against current and emerging threats.

Why do cyber-attacks occur?

The participants discussed a number of reasons why attacks are happening and how they are constantly morphing. While this list is by no means extensive, the group collectively agreed on the below crucial reasons behind the rise in cyber-attacks across all organisations.

1 THE CHANGING ATTACK SURFACE

The past five years alone have seen a drastic change in the number of ways hackers can get into an organisation. There used to be a clear distinction between the inside and outside of an organisation and infrastructures had clearly defined boundaries; an office with computers and on-site servers meant that data never left the company. This ultimately equated to a physical firewall. However, now, with the rise of mobile working, the Internet of Things (IoT) and cloud services, that end-point has expanded and there is no clear, easily protected line that can keep data in and attackers out. Many organisations still have a legacy perspective of the perimeter.

This is problematic for security teams, who have to fight on an ever-expanding frontline. Mobile devices, particularly employee owned, spurred by the BYOD trend that was in vogue five years ago, are relatively easily hacked because they often lack basic security software and yet they are connected to a company's server. While seemingly insignificant in the singular, when multiplied by thousands of employees, there is a huge surface for attack; every person's computer is an entry point for a hacker. This is then compounded by the fact that employees expect convenience. They expect to bring their data with them and use free and popular services that are notoriously insecure or email documents to private accounts. The result is that data is now leaving the perimeter at an unprecedented scale.

Now that IoT has been adopted and has entered the mainstream, the perimeter and number of vulnerabilities are set to expand yet again. With the IoT industry estimated to reach $276 billion by 2020, and potentially 75.4 billion devices by 2025, the attack surface will expand exponentially. The issue lies in the fact that security is rarely built into the design of these devices and their software, leaving them open to attack.

Members of the roundtable pointed out that we have all experienced the ramifications of this, as recently as late 2016. The Mirai attack, which saw the exploitation of hard-coded credentials of IoT devices, such as camera devices, exploited to create a botnet that took down a number of significant services, affecting business functions worldwide. This one instance demonstrates that in many cases, security teams are constantly trying to fix a ship with thousands of holes, as it were. Without proper implementation of IoT, data leaks out and hackers get in each time a new IoT device enters the public space.

2 INSTANT DEMAND CULTURE

We have also seen the proliferation of a culture of convenience among consumers, in addition to within businesses. They have a 'vending machine mentality', where they expect to have services immediately, on demand, without thinking about how it works or interacts with other services behind the scenes.

Authentication is a common problem that has been caused by this type of culture. Users expect to be able to login as quickly

and effortlessly as possible, but such convenience is often at odds with security. Despite education from security teams to employ complex passwords with special characters that require a reset every few months, users continue to set common passwords, such as 'password' or '12345678' across all their accounts, which are easy to guess and highly insecure. This is particularly frustrating as McKinsey found that "when consumers find the authentication process easy, they use digital services 10 to 20 percent more than customers who are frustrated by authentication."

One attendee noted that even the most basic security measures are seen as inconvenient, and, importantly, that they are perceived as getting in the way of doing business. He quoted an example of where a customer's employees complained bitterly that their screensavers automatically locked them out after just five minutes. The employees saw this as annoying and unacceptable. Why? Because they did not want to have to log in so often. Clearly, we have yet to find the balance between security, convenience and perception.

3 INCREASINGLY COMPETITIVE BUSINESS ARENA

This instant demand culture echoes in the business space. Businesses need to be more agile than ever before to improve the time to value. This often means that security, although applied, is relaxed in favour of the customer experience. Online startups have exploded in number in recent years (one now starts up every three seconds), all driven to get to market as quickly as possible. Many of these businesses consider security, but not as a priority. They therefore tend to use insecure software services, such as improperly updated checkout cart/ ecommerce systems, which makes them an easy target for hackers. Updates to software can 'break' code and interrupt business, and as a result, security updates are often not conducted properly.

If this mindset is allowed to continue, it could lead to an attitude of seeing cybersecurity as a mere 'checkbox' on the project or list of things to do. It is very important to implement security frameworks thoroughly, and with a commitment to solve security problems, rather than simply tick a box. For example, ISO/IEC 27001 is typically regarded as a good measure of cybersecurity, which it undoubtedly is. However, many organisations tend to relax after implementing this standard believing they are safe, when the truth is they have only just begun. If we are to move out of the checkbox world, we need to start to measure how well we perform or carry out the mandates of this standard and, of course, other best practice frameworks. To do anything else will lead to complacency.

The group also agreed that many organisations are becoming too relaxed in their attitude to cybersecurity, that hacking and being hacked or compromised is becoming a part of the landscape – something we have to live with. This was exemplified by one delegate who noted a chilling fact that some organisations have started to hold bitcoin reserves to pay off ransomware attacks as quickly as possible (in order to continue running). This is dangerous territory: treating the symptom, but not the cause, can mask as business resiliency, but the reality is, the problems are still there and will get bigger and ultimately more costly.

4 HUMAN ERROR

According to the Information Commissioner's Office (ICO), human error is the number one cause of data breaches, such as sending the wrong document to the wrong person, leaving a computer unlocked or falling for a phishing email. There is a general lack of public awareness around basic secure behaviour, such as spotting fraudulent links and phishing emails or plugging in unidentified USB sticks.

There are two sides to the human error issue. Firstly, the organisations employees and customers (end users) have become the primary targets of cyber-attacks. End users are now targeted because their behaviours are relatively easy to exploit. Hackers now conduct reconnaissance on end users, observing behaviour and then finding a way to exploit it. This is called "passive attacking," because the hacker simply watches the behaviour. Passive attacks occur because despite the heightened risk around more end devices than ever before, there is a still a lack of education about the threats and a lack of truly secure solutions.

End users are attractive targets because, simultaneously, they have become less aware of security, while the devices they are using have become infinitely more powerful. Security as a behaviour has simply not been taught: it is a societal problem, and a major concern for all organisations, which are potential targets of a passive threat or attack. Yet security teams (not skilled in marketing) often do not communicate this or the whole security policy to staff very effectively – help is needed. In addition, devices rarely include enhanced security, such as multifactor authentication (MFA), that can prevent the vast majority of data breaches by stopping unauthorised users from accessing a company device. This all leads to the end user becoming the weakest link.

The second aspect is human error on the part of IT and security administrators. Managing the increased complexity of IT infrastructures now means there are more disparate security tools than ever before, including network monitoring, intrusion detection, encryption and security information and event management tools (SIEMs). The issue is that while there are more tools at the disposal of IT administrators, all of them need to be correctly aligned and/or integrated to provide effective security.

What unfortunately happens in reality is that many of the tools are implemented with the default configuration settings. This can mean, for example, that the detection tool starts returning far too much data, which often ends up being ignored. Another example is when a tool detects a truly dangerous cyber-attack, which gets lost in the "noise of data". Security teams need to set their baselines and thresholds according to the needs of the organisation, but as this process often takes a number of months, it is often omitted. Another truth that compounds these issues is that comparatively few individuals have received the correct level of training with respect to the products they are using and also a lack of experience to create proper baselines. This is a primary example of the competency and skills gap that CompTIA and others have been working to close over the years.

Undoubtedly, cybersecurity has dramatically changed. A ballooning attack surface, combined with ill-informed and improper consequential end-user behaviour that is being ignored by some organisations that refuse to take security seriously is stretching the capability of cybersecurity teams way past their limits. Surprisingly, however, the group agreed that we have yet to experience the "watershed moment" that will force or cause businesses to take security seriously. WannaCry came close, and although a new hack is in the news every day, security has yet to be truly adopted or even capture the businesses' imagination.

Future Threats: What Could We See If We Fail to Act Now?

We can all agree that the threat landscape is constantly evolving. The past five years have seen a huge change, and the next five will probably herald even more. The group then discussed what they considered to be the most worrying future threats.

1 ORGANISED CYBERCRIME

Less of a future threat and more of an emerging threat, organised cybercrime is the next trend that cybersecurity teams will have to combat. Until now, many incidents have been one-off attacks, motivated probably more by malice rather than financial gain. However, that is changing.

In early 2017, Europol's Serious Organised Crime Threat Assessment found that gangs – highly skilled and well-funded groups around the world – have officially added cybercrime to their repertoires, now that data has become as much of a commodity as money is. These gangs are usually motivated by financial gain, though some have ideological motivations. Attack patterns often follow 'Crime as a Service', models, often found on the dark web, where gangs hire hackers to carry out cyber-attacks.

It is thought that many of the recent ransomware attacks were highly organised and irrespective of whether they were state-sponsored or the work of gangs. In 2016, Intel Security logged 124 separate variants of ransomware, some of which were directly attributed as being controlled by gangs. Meanwhile a South Korean firm recently disclosed the largest ransomware payment ever recorded ($1 million) showing just how lucrative these attacks can be. It is, therefore, not a surprise for the criminal community to start to focus their attention in this area.

The group also discussed how organised cybercrime might evolve. One participant raised the possibility of hackers cloning or outright stealing entire business infrastructures, citing how relatively easy it is to infiltrate and remain undetected on an organisation's network, implying that there is scope to do far more damage. Today's coordinated ransomware attacks may even take the shape of something far more sinister in the future.

2 CYBER-TERROR

Building on the points above, a particularly disturbing form of attack could emerge as the physical and digital worlds become ever more closely intertwined. The close timeline between the NHS ransomware attack and the London Bridge–related terror attacks highlight how combined attacks could have disastrous consequences.

The WannaCry attack disrupted around 50 trusts and prevented them from treating patients; fortunately, there was no loss of life. However, if this attack had been combined with a high-scale terror attack, the effect could have been catastrophic, with nearby hospitals unable to treat terror victims. If organised criminal gangs are able to harness the power of cybercrime for financial gain, it would be naïve to think that a terrorist group would not want to avail themselves of similar powers.

3 INTERSTITIAL ATTACKS

From the roundtable discussion, another form of vulnerability emerged that is likely to increase as we use more technology systems in combination with one another. An interstitial attack is a vulnerability that

arises in the gap between two different systems or technologies. The most common interstice is between humans and computers that gives rise to the aforementioned human error vulnerability. However, these also exist between systems, which should be cause for concern.

For example, a few years ago, some online social networks would offer a forgotten password request via SMS. SMS technology is unencrypted and does not use strong authentication, which meant that it was very easy for hackers to listen in and acquire a huge number of passwords. Another example is the interaction between a website and database technologies.

The group believed that interstitial attacks will become more of an issue as the need to implement and integrate different systems gathers pace. Organisations are already opting for more and more cloud-based services, which directly interact with their local enterprise systems. Another example is IoT devices that interact with email systems. All these interstices, and many more, are, in fact, vulnerabilities that hackers could exploit. This number will only increase as these kinds of services become more popular.

Recommendations on How to Secure Organisations

After covering the key and emerging threats, the group turned their attention to how businesses can improve the cybersecurity stances.

1 RESHAPING SECURITY TEAMS

All attendees unanimously agreed on the key point that we must reshape our cybersecurity teams. Security is not just a part of IT – it's part of the entire business. Security has, for too long, been seen as a subset of IT, which has seen chief security officers (CSOs) or chief information security officers (CISOs) reporting to chief information officers (CIOs) and lacking any direct connection or influence over business operations. This is apparent in EY's Global Information Security Survey, which shows that only 22 percent of global executives, CIOs and CISOs believe that their businesses have 'fully considered the information security implications of their organisation's current strategy and plans.' This is despite the fact that three out of four organisations have experienced a data breach in the past year, as CompTIA found in our 2016 International Trends in Cybersecurity Report.

However, as cybersecurity grows in importance and starts affecting business operations, security teams have to become integral to the overall business strategy, no longer just a subset of the IT department. This could happen in a number of ways, as described below.

a) The Boardroom

Businesses need to bring CISOs into the boardroom and give them a voice equal to that of any board member. Security is a functional and integral part of the organisation and, as such, should be represented as an equal partner, as should the CIO or chief technology officer (CTO) representing IT. Security needs to be viewed not as an add-on to IT, but as a critical part of the organisation. CISOs at the board level can provide tremendous value, contextualising threats in a way that the board can understand, translating security threats into business risk and providing context for the business in its future planning.

For too long the IT and the businesses have been stuck in a situation where IT departments are responsible for rolling out IT services and securing them at the same time. This is a classic conflict of interest. Each time a conflict of interest occurs between implementing a new solution and securing it, the business service – usually seen as the implementation – often wins at the expense of security because of the pressure to keep the business moving forward as quickly as possible. In many organisations, security is not as seen as important as keeping things working. This, the group concluded, needs to change. There is a need to segregate IT from security and the CIO from the CISO. However, both need an equal voice with that of the business, as explained above.

Ultimately, the role of the modern CISO is to understand what the business is trying to achieve and how security can contribute to its functions. This way, security is not seen as an add on, or adjunct. Instead, it is seen as a fundamental pillar of how a business operates. We need to move away from the 'security for security's sake' mindset that many businesses currently have and intertwine it throughout. They have to understand the impact of cyber-threats and contextualise it in terms of business risk.

This will be particularly important when GDPR come into force in May 2018. The law will compel businesses to comply with strict guidelines around the safeguarding of customer data. Companies found not to be in compliance would face fines of up to 5 percent of their turnover, and increased fines for repeat offences. This can be disastrous for businesses' bottom lines; it is simply a business issue.

CISOs will have to play a crucial role in the implementation of GDPR:

- At the forefront of assessing and evaluating the security around currently stored customer data and establishing any improvements or changes
- Instrumental in understanding how these safeguards will need to adapt in line with emerging technologies, such as IoT, Industry 4.0 (automation) and big data
- Work out how and where GDPR needs to be addressed across each IT service, especially where data is being passed from end to end with multiple suppliers in the value chain
- Provide awareness of potential threats, how these may manifest themselves and how employees can protect both themselves and the organisation

Adhering to GDPR will not be a one-off task. Compliance will require constant, project-based work to ensure that any changes to the business will become – and remain – compliant. New technology will herald new security risks, and it will be the CISO's job to make the transition to new technology compliant with these laws.

b) The Security Industry's Communications Problem

We have established that security is often perceived as a hindrance to employees and executive management. It is also seen as something that obstructs usability and prevents end users from 'getting the job done.' This often leads to employees using insecure workarounds, such as passwords on Post-it Notes or using weak encryption and single-factor authentication with external cloud services. This combined with a lack of education and awareness to demonstrate how insecure their actions are and why humans are cumulatively the number one cause of data breaches.

Employees need to take security more seriously. Part of the lack of regard for cybersecurity is the fact that people see security as the 'department of the no.' Some even regard security teams as some form of 'secret police,' ready to swoop down and punish the end user. As a result, security workers are often perceived as some unseen force until the point where something goes wrong. Then the team penalises users for making mistakes and restricts them from working in the way they want to.

Arguably, this communication problem is analogous to the communications gap between the board and CISO. There is rarely a line of communication from security to the staff that explains what they are doing, what is expected of them and why certain behaviour is insecure.

The roundtable members felt that the best way to address this is to have security teams work closely with a marketing or communications team to effectively communicate what the security team is doing in a way that the whole business understands. In this way, the security team should be encouraged to adopt elements of the Computer Security Incident Response Team (CSIRT), which includes technical and non-technical members, including public relations individuals.

By communicating in a way that is relevant to employees, members of the security and public relations team will encourage everyone to practice good cybersecurity and let them know why certain policies are in place. Technical terms that are assumed knowledge in security, such as phishing, could be translated to relatable terms, like scam email. Why not, for example, create a dictionary of terms? Remember that biometrics were established years ago but not very popular until Apple decided to use this technology on its phones — a good example of the effect marketing and communications can have.

If the security communicator can change the perception of security in the workplace and make employees more security aware, we may see a trickledown effect throughout society. If staff are cybersecurity conscious by default, their best practices could filter down to their family and friends, contributing to a more security-aware society.

2 EMPLOYEE TRAINING – ADDING VALUE TO YOUR COMPANY

Businesses will also need to put training and education measures in place to raise the overall level of security awareness. This should include more than just the IT department. Corroborating research in CompTIA's International Trends in Cybersecurity report revealed that 52 percent of data breaches are caused by human error, with actions including falling for phishing emails, sharing passwords or connecting to public Wi-Fi. The fact that around 45 percent of employees do not receive any form of training or education, no doubt, fosters the general lack of cybersecurity awareness that leads to these actions. It is vital for employers to understand that as they invest in training, they are increasing the value of their company.

However, the best way to upskill employees remains up for debate. Attendees at the roundtable agreed that gamification is a very good way of teaching security best practices in an engaging way that sticks with the individual by rewarding good behaviour. One attendee cited an example of a lock-screen league at their workplace to teach staff to lock their computers when they leave their desks. The security team set up a league table, and users scored points if they managed to send an email from someone's unlocked computer to the security team. Users who left their computers unlocked were docked points. The attendee said this proved very effective at encouraging people to lock their computers, and at the same time raised awareness of why it is important.

Other examples include PwC's Game of Threats, which gamifies cybersecurity for board members. It puts them in the situation of attackers and defenders and demonstrates how different decisions have different outcomes. Digital Guardian's DG Data Defender game rewards good behaviour that prevents data loss through badges and prizes.

We still have a long way to go, however. One attendee said that during a routine social engineering exercise, one-third of employees fell for a phishing email. However, by rewarding good behaviour, organisations can bolster the 'human firewall,' making them less of a target for hackers. The nuance lies in using the carrot, not the stick, when it comes to training. Security teams, whether they

use gamification techniques or not, must not make their employees feel threatened, or they risk facing resistance.

CompTIA has incorporated a number of these approaches into its own training programmes to address employee awareness of cybersecurity. In 2015, CompTIA launched CompTIA CyberSecure™, a self-paced online training course, to give employees practical cybersecurity awareness tips around their everyday lives and during work. It incorporates results-driven training to keep trainees engaged and demonstrates that employees' actions are the crucial first line of defence in protecting their organisation against data breaches and other threats. CyberSecure's content is based on findings and experiences of its IT Security Community, ensuring that the latest knowledge from the frontline of the industry is transferred to businesses' employees. This includes fundamentals on email policies, using USB drives and other basic security principles.

Training must to be implemented to change the organisational mindset from the ground up. Human resources teams should be incorporating cybersecurity training into their employee on-boarding processes, as well as developing programmes to cultivate a secure environment that is currently lacking at this present time.

3 CERTIFICATIONS – PROOF OF VALUE

One of the best ways to prove that you have properly invested in your employees is to certify them. Training and certification is incredibly important in ensuring cybersecurity staff have the technical skills required to protect against breaches. It also helps prove to management, board members and others that you are applying metrics to your employees, and are tracking the return on investment (ROI) in regard to security. All members of the roundtable agreed that ROI is increasingly a major issue in regard to security. Few, if any, organisations wish to simply spend lavishly on security unless they have a very clear understanding of the benefits of that spending.

Therefore, training alone is not enough; certifications validate the skills of a business' workforce, ensuring that individuals are ready to apply best practices and properly use today's technologies. Certification helps ensure that employees are ready to meet the demands of cybersecurity today and confirm that they have retained knowledge. Businesses need to be sure that their cybersecurity teams have the capability to both protect against the modern and emerging threats using the most current tools, as well as the ability to deal with and remediate a data breach should one occur.

Businesses should consider certifications as a way of upskilling their workforces and ensuring that their knowledge remains as up to date and advanced as possible. CompTIA's certifications for example, are based on job requirements that are drawn up by specialist subject matter experts from renowned organisations in the industry. This guarantees that the learning outcomes are based on real-life scenarios and can be applied immediately in the workplace, providing maximum value to the employer.

The critical element to training and certification is linking it to a strong ROI. Certifications are important from both an employee and business point of view. Not only are certification holders more employable and credible, 89 percent of employers agree that certified professionals perform better than non-certified professionals in similar IT roles. This means that organisations that are looking for the best skills possible naturally gravitate toward certified individuals. In any conversation about skills, certifications must be considered.

Furthermore, CompTIA has listened carefully to the IT industry about how many of their cybersecurity workers have serious knowledge gaps. To help address this issue, CompTIA has focused on emphasising the cybersecurity pathway. The IT industry has been suffering from a significant skills gap for some time and has responded very positively to our approach of creating an industry-based pathway. For example, Microsoft's veteran's program, the Microsoft Software and Systems Academy, has recently adopted key elements of the cybersecurity pathway. It adopted CompTIA Network+ and Security+ because it recognised that individuals must first obtain essential industry-based knowledge before moving on to vendor-specific training and certification.

The IT industry has asked us to create additional pathways. Therefore, we have focused on the following tracks of instruction:

- Infrastructure: A+, Network+ and Security+
- Advanced infrastructure: Linux+, Server+ and Cloud+
- Cybersecurity: Security+, CSA+ and CASP.

These offerings allow trainers to address essential skills gaps.

4 EMERGING TECHNOLOGY

Emerging technologies, such as the latest IoT devices, will continue to profoundly affect businesses and consumers alike. However, with these opportunities come many threats. As we have discussed earlier, IoT expands the attack surface of an organisation exponentially, with each device becoming a new endpoint that hackers can exploit.

At the present, this kind of threat is not widely understood, although we are already seeing its effects, with hackers exploiting IoT device vulnerabilities. This is why we believe that one of the biggest threats is that of the innovator. New devices are created with no security built in. This leads to simple vulnerabilities like hard-coded credentials being exploited. The net effect is millions of IoT devices flooding the market with inherent vulnerabilities, which is akin to a car manufacturer rolling out a new fleet with faulty seatbelts.

In the same way that there is a trade-off between security and convenience, there must be a balance between innovation and security. Innovators are rapidly developing new technology, which has to be retroactively secured. The roundtable group posed two potential solutions to this.

1. By taking a more considered approach, developers could create technologies with cybersecurity in mind to prevent repeats of the Dyn DDoS attack. This applies for IoT devices, but also for new apps and startup businesses.

2. Establishing more regulation around these technologies. One attendee explained that certain industries are capable of good self-regulation, such as scuba diving, because the risks are apparent but can be managed. The technology sector and IoT, in particular, is not like this, as the security dangers are not as obvious to many company executives. Therefore, regulatory bodies may need to step in to ensure that developers create technology in a safe way. Groups like the Internet of Things Security Foundation are stepping in, but industry needs to do more to raise awareness. All in all, the roundtable agreed that the key is for the industry to adopt a proper software development lifecycle that takes security into account from the ground up.

Where to Next?

The roundtable emphasised the need for the industry to focus on best practices and the issues explored throughout the day. Attendees also emphasised that there is no silver bullet to resolve cybersecurity issues. The above points are by no means an exhaustive list. They do form a very valid beginning, to resolving the many issues that face us with respect to cybersecurity. Each point demonstrates how much we still have to learn. The sector is rapidly evolving and changes every day, which makes it an incredibly exciting sector, but not one without danger (the biggest being complacency).

Businesses must learn that cybersecurity involves the practice of identifying and managing risk. It is not simply an activity confined to the uber geeks in the IT department. Security has an impact on every aspect of business operations and involves every employee across an organisation. It is intertwined with emerging technology today that will be standard in the future.

CompTIA recognises that creating a cybersecurity-conscious culture within an organisation requires a concerted effort, from the board of directors on down to each and every company employee. This is why we brought our membership together to discuss their most pressing issues. It is up to us to share insights with each other so we can move forward as a collective. Every company, large or small, is in the same boat; we all work on the same internet together, and it is up to every company to work together to solve the cybersecurity problem. We need that open forum to progress the industry and protect ourselves from the threats of today and in the future.

If you would like any more information, please contact CompTIA.

CompTIA UK
11th Floor, Citypoint
1 Ropemaker St,
London
EC2Y 9HT

0207 3306060

CompTIA.org