TELSTRA

European Regional Summary 2019

Telstra Security Report 2019

Contents

Executive Summary

Today, the reality of security threats to businesses, communities and individuals is being felt right across Europe. This has been reflected in the implementation of national and pan-European security initiatives and legislation, increased cooperation within sectors and supply chains, and new investments by organisations and security service providers in strengthening their levels of defence. Our 2019 Security Report provides an in depth analysis of the challenges organisations around the world are experiencing in terms of security threats and attacks. Further, we explore their cyber and electronic security preparedness. In our 2019 European Regional Report, we examine the challenge of cyber and electronic defence across this region specifically, including the experience of businesses and public sector organisations in the past 12 months and their plans for the future.

Human error was identified as the greatest security risk in our recent report findings, consistent with our 2018 Security Report. In general, there are three forms of insider threats. They range from a malicious insider intent on, for example, stealing corporate data or causing a company damage; to an employee who has been targeted by an external advisory such as a social engineering attack; to an accidental insider who might not adhere to basic precautions or due to IT systems or business processes, is unable to complete their job securely. Most European respondents reported experiencing all types of insider threats, with human error reported as the highest concern for European respondents at 26 per cent. This is also forcing the issue of end-user awareness and training onto the agenda as part of the cyber preparedness agenda.

Among the European respondents, 38 per cent currently have formal education programs for security awareness training. Many of these programs are helping employees to understand the threats and in reducing the number of security incidents. Our research found that 26 per cent of European organisations surveyed cited skills shortage as a challenge. The International Information System Security Certification Consortium (ISC)[2] reports a current shortage of 142,000 qualified cyber security workers across Europe, the Middle East, and Africa, will reach 350,000 by 2022.[1] Some 34 per cent of the respondents also highlighted challenges with training their staff, and keeping up-to-date with the latest security technologies.

Significant external threats are also contributing to the increase in security investments. These include theft of data and credentials from outsider attacks; damage to digital systems through hacktivism or cyber vandalism; and financial loss from extortion (e.g. ransomware), crypto-related crime, and the impact on productivity from major malware attacks and data breaches. A recent Carbon Black research study that surveyed incident response professionals noted that attacks are becoming more complex. In nearly half the cases (46 per cent) the attackers engaged in 'counter incident response' to conceal their activities. 'Island hopping' was another trend identified in 36 per cent of reported cases.[2] This is where the attacker first targets an organisation's affiliates, such as customers, suppliers, or partners that have a weaker security posture, before working its way through the supply chain to the primary target.

One result of digital transformation is the increasingly connected world of IoT. Information technology (IT), including systems for data-centric computing, is increasingly becoming integrated with operational technology (OT), which includes systems used to monitor events, devices and processes. In this environment, an attacker can gain access to connected devices, such as an IP surveillance camera, through simple-to-crack default passwords. Once password protocols are bypassed, cyber criminals can exploit access to thousands of other units with relatively minimal effort. Mirai was an example of one of the largest distributed denial of service (DDoS) attacks of this kind, peaking at 990 Gbps[3], and has led to other strains, such as Brickerbot, Hajime, and Persai.[4]

[1] (ISC)² (2018). Cybersecurity Workforce Study, 2018. Retrieved from *https://www.isc2.org/Research/Workforce-Study*
[2] Carbon Black (2018). China, Russia & North Korea Launching Sophisticated, Espionage-Focused Cyberattacks Massachusetts, USA: Author. Retrieved from *https://www.carbonblack.com/company/news/article/china-russia-north-korea-launching-sophisticated-espionage-focused-cyberattacks-2/*
[3] Holmes, D. (2016, October 27). Making Sense of the Last Month of DDoS Attacks. F5. Retrieved from *https://f5.com/Portals/1/Cache/Pdfs/5041/making-sense-of-the-last-month-of-ddos-attacks.pdf*
[4] Cisco (2018). Cisco 2018 Annual Cybersecurity Report.

A 2018 Cisco report found that 31 per cent of security professionals reported their organisations had already experienced cyber-attacks on OT infrastructure.[5] Our research found 71 per cent of European organisations 'now have' or 'plan to have' a combined budget for cyber and electronic security. It makes sense, given the rise of smart factories and the rapid increase in the number of connected objects in the enterprise from manufacturing to logistics. In the future, it will be necessary to for companies to use an integrated approach when it comes to using and securing IT and OT systems.

One issue organisations have become used to grappling with over the last two years is compliance, given the introduction of the General Data Protection Regulation (GDPR) coming into effect in May 2018 and preparations leading up to it. GDPR and other data protection regulations have a direct impact on departments responsible for cyber and electronic security. Indeed, nearly two-thirds (63 per cent) of European respondents in our survey believe their organisation has received fines for being in breach of legislation enacted in the past two years. This is a stark reminder about the ramifications of being unprepared, as organisations pay the cost not only for actual breaches but for failing to demonstrate readiness to protect data in the first place.

[5] Cisco (2018). Cisco 2018 Annual Cybersecurity Report.

Methodology

The Telstra Security Report 2019 provides research-based insights into the current security landscape to support you in mitigating and managing security risk. Whether you are a senior security professional in a large multinational organisation, or an IT Manager in a 50-person domestic business, this report is designed to assist you in understanding current security trends and framing strategies for preparedness and incident response.

We engaged research and analysis firm GlobalData to interview professionals responsible for making IT security decisions within their organisation to obtain a number of key insights on a range of security topics. Our report also draws on the analysis of security information and data gathered from our infrastructure and security solutions, plus that of over 15 third-party providers, including our security partners.

With continued convergence within the security field, this year we once again examine cyber security and have expanded our research even further into electronic security. For the purposes of this report, electronic security refers to connected devices such as IP surveillance systems, through to building access and management systems, including industrial control systems.

Sample Size and Geography

GlobalData's online research in November and December 2018 provided 1,298 responses across 13 countries in total. Sixty one per cent of the surveys were conducted in APAC and 39 per cent in Europe. There were a total of 503 interviews completed in Europe, and these responses are the focus of this European regional summary of our 2019 Security Report. These respondents were from Germany, France, the UK, Belgium, Netherlands, and Luxembourg. The UK had the largest number of respondents in this subset, representing 31 per cent of all European respondents. The respondents reported knowing their organisation's annual security budget and having either some influence or complete control over the security investment.

Australia	320	25%
New Zealand	68	5%
Hong Kong	72	6%
Singapore	76	6%
United Kingdom	154	12%
Germany	129	10%
France	129	10%
Taiwan	86	7%
Philippines	82	6%
Indonesia	91	7%
BENELUX Region (Belgium, Netherlands, and Luxembourg)	91	7%
Total	1298	100%

Business Types

European respondents represented businesses of all sizes – 50 employees to as large as 5,000-plus across 15 industry verticals. These verticals include banking, financial services, and insurance (BFSI), retail, IT and technology, government and public sector.

Position Titles

European respondents included C-suite executives such as CEO, CFO, CIO, COO, CTO, CISO and CSO. These accounted for 19 per cent of the respondents with the remaining 81 per cent from IT and security management roles. The largest persona to participate in our survey was IT Manager at 38 per cent, with IT and security management representing 15 per cent of the sample.

Location of Respondents

1,298
Respondents

13
Countries

15
Industries

Europe
France, Germany, United Kingdom, Belgium, Luxembourg, Netherlands

Asia Pacific
Australia, New Zealand, Singapore, Hong Kong, Indonesia, Philippines, Taiwan

Australia

The European Cyber and Electronic Security Environment

Despite the ongoing challenges surrounding Brexit, and other regional, political, and economic uncertainties, Europe remains strongly interconnected and integrated from the perspective of technology, business, and many aspects of consumer markets. Security threats are global in scope and universally important. The European cooperation around data security and privacy means there is a shared defence - or at a minimum, level of acceptable preparedness. The institutions of the European Union (EU), including the European Commission (EC), and the many pan-European associations and agencies that support its member states all contribute to that effort.

European Cyber Security Month (ECSM) is an EU awareness campaign that promotes cyber security among citizens and organisations. It showcases the importance of information security and highlights the simple steps that can be taken to protect their data, whether personal, financial and/or professional. Held every October since 2012, the ECSM campaign strives to raise awareness, change behaviour, and provide resources to individuals about how to protect themselves online. Private sector participation and countries involved in the ECSM has grown annually, whilst also helping to jumpstart similar initiatives in the United States and Australia. Whether it has succeeded in changing behaviour enough to keep up with the increases in volume and complexity of cyber threats is an open question that its sponsors (the EU Agency for Network and Information Security and the European Commission Directorate-General for Communications Networks, Content, and Technology) must confront.[6]

Security awareness will become increasingly important as businesses look to use new technologies, such as IoT, to drive more efficiency and tackle new business models. The attack surface for many organisations will also increase. Electronic and cyber security have common threat vectors, such as malware and DDoS. Education and awareness thorough institutions and member states is an important way to help manage security risk across Europe.

[6] European Cyber Security Awareness. ENISA (2019). Retrieved from *https://cybersecuritymonth.eu/*

Regulation

In the EU, the General Data Protection Regulation (GDPR) came into effect in May of 2018, establishing new requirements for protecting data belonging to EU citizens. In the case of the GDPR, organisations that fail to comply with the regulation requirements could be penalised up to €20 million in fines, or up to four per cent of their total worldwide annual turnover.[7]

There is increasing acceptance in Europe of the widespread need for cyber security. This is due to newly open discussion about the inevitability of data leaks and breaches and growing public awareness of individual data privacy rights. Sixty three per cent of European respondents in our survey noted their organisation has received a fine for being in breach of any new legislation enacted in the past two years. As businesses strive to comply with regulations and avoid incurring significant fines, the risks of using digital services for both consumers and businesses became increasingly apparent to employees and end users. These new realities continue to make security a board-level issue. The C-suite continues to be more involved in security matters, holding regular briefings on the topic and being more accountable than in previous years. Some 46 per cent of European respondents report that the CEO and/or board of directors level of involvement on either cyber or electronic security matters as high or very high. Further, 46 per cent of respondents indicate the level of concern from their customers on data privacy has increased over the past year.

Legislation

Legislation is also moving forward to help boost the overall level of cyber security in the EU. The Network of Information Systems (NIS) directive was adopted by the European Parliament and put into force in 2016. It required member states to incorporate this legislation into their national laws and to identify operators of essential services by the end of 2018. The directive required each country to have a computer security incident response team (CSIRT) and a competent national NIS authority in order to cooperate with other member states on information exchange, strategy, and incident response; and to enforce stricter requirements on businesses in key sectors (including essential services like energy, finance, and healthcare, as well as digital service providers like search engines and cloud hosts).

In December 2018, the major EU legislative bodies reached an agreement on a new Cybersecurity Act which reinforces the mandate of the EU Agency for Network and Information Security (ENISA). This act will better support member states with tackling cyber security threats and attacks. The Act also establishes an EU framework for cyber security certification, boosting the cyber security of online services and consumer devices. The new rules are designed to help people trust their every-day devices. It is also intended to enable consumers to choose between products, like IoT devices, that are certified within the framework to be cyber secure. Organisations will benefit, as having a single EU certification regime will remove potential market entry barriers such as having to apply separately in each country. The EU believes that companies will be incentivised to invest in the cyber security of their products by turning it into a competitive advantage.

[7] European Commission (2018). Reform of EU data protection rules. Retrieved from *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*

Industry Initiatives

The European Commission is also examining how to strengthen cyber security cooperation across different sectors of the economy, establishing a forum called the contractual Public-Private Partnership (cPPP) on cyber security in 2016. The pan-European cyber security membership organisation has brought together large companies, industry associations, small and medium-sized businesses (SMEs), research institutions, and public sector organisations to collaborate in a pan-European ecosystem on strategic research and innovation. At the sector level, organisations, their suppliers and partners are coming together to consider their common supply chain security requirements. Our research found 30 per cent of European respondents have already implemented supply chain risk assessments, another 61 per cent are either rolling out or trialling capabilities, or are considering doing so within the next 12-24 months.

The AeroSpace and Defence Industries Association of Europe (ASD) participates in the cPPP to collaborate on civil-military security issues.[8] Meanwhile, the healthcare, energy and financial services sectors are working to bring their cyber security controls up to meet compliance requirements. For example, the Council of European Energy Regulators (CEER) recently published their cyber security report on Europe's electricity and gas sectors. They called for coordinated security planning and implementation for critical infrastructure across the sectors internationally, with close cooperation between national regulatory authorities.[9] Such initiatives are inevitable. Almost every industry sector progresses with digital transformation, often exposing the shared risks and threats of their ecosystems. New opportunities to share in mutual cyber and electronic security strategies are emerging as a result of these commonly felt threats.

[8] ASD (2018). Defence. Retrieved from *https://www.asd-europe.org/defence*
[9] CEER (October 2018). Cybersecurity Report on Europe's Electricity and Gas Sectors. Retrieved from *https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124*

Security Incidents and Breaches

Our 2019 Security Report is based on an extensive survey on the experience of private and public sector organisations regarding security during the last year. The results provided in this report provide timely intelligence on the frequency of security incidents and attacks by type of incident and means of attack.

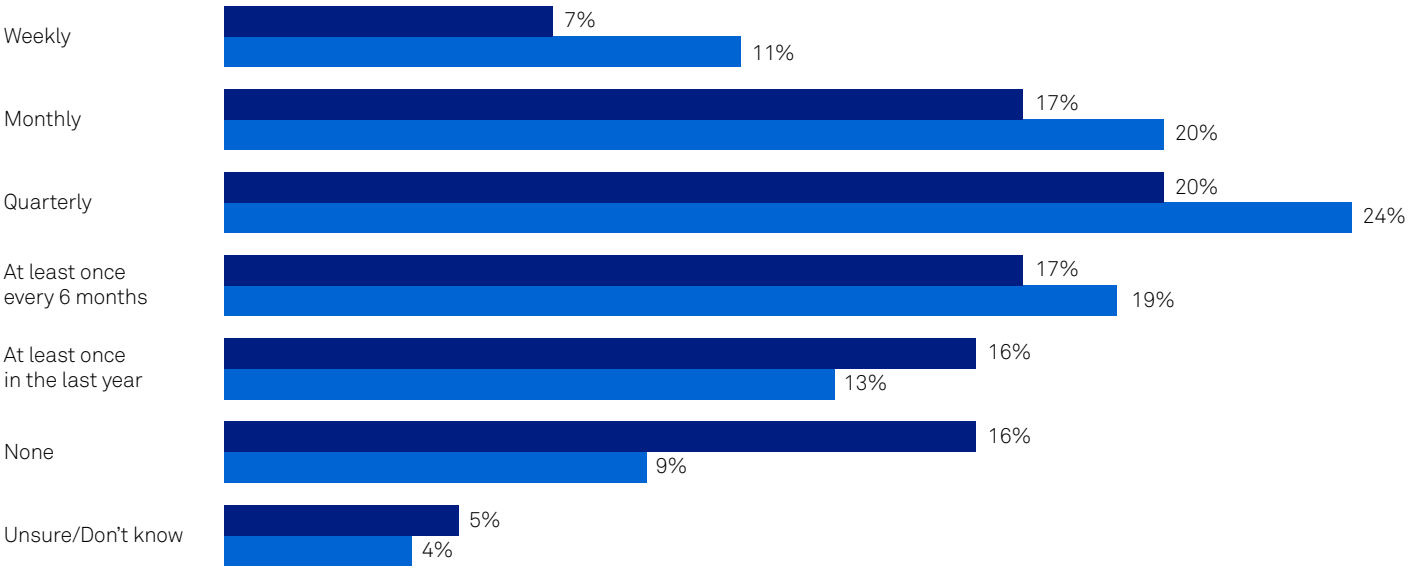
Malware, APTs and Other Attacks

At the global level, a similar volume of ransomware incidents were reported in our 2019 Security Report compared to our previous year, when WannaCry and NotPetya wreaked havoc. In September 2018, Europol named ransomware as the leading malware threat in its fifth annual Internet Organised Crime Threat Assessment (IOCTA) report.[10] The report identified the most commonly reported ransomware families were: Cerber, Cryptolocker, Crysis, Curve-Tor-Bitcoin Locker (CTBLocker), Dharma and Locky. In terms of frequency, European respondents that had experienced business interruption due to a security breach, 78 per cent of this subset experienced at least one ransomware incident within the last year, with 44 per cent of organisations experiencing at least one per quarter. Weekly ransomware incidents were experienced by seven per cent of European respondents.

[10] Europol (2018). Internet Organized Crime Threat Assessment (IOCTA). Retrieved from *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*

Q: How frequently has your organisation experienced the following security incidents in the past year?

A subset of European organisations that have experienced ransomware and other malware in last 12 months



Europe results, n=322 (subset)

Ransomware Other Malware

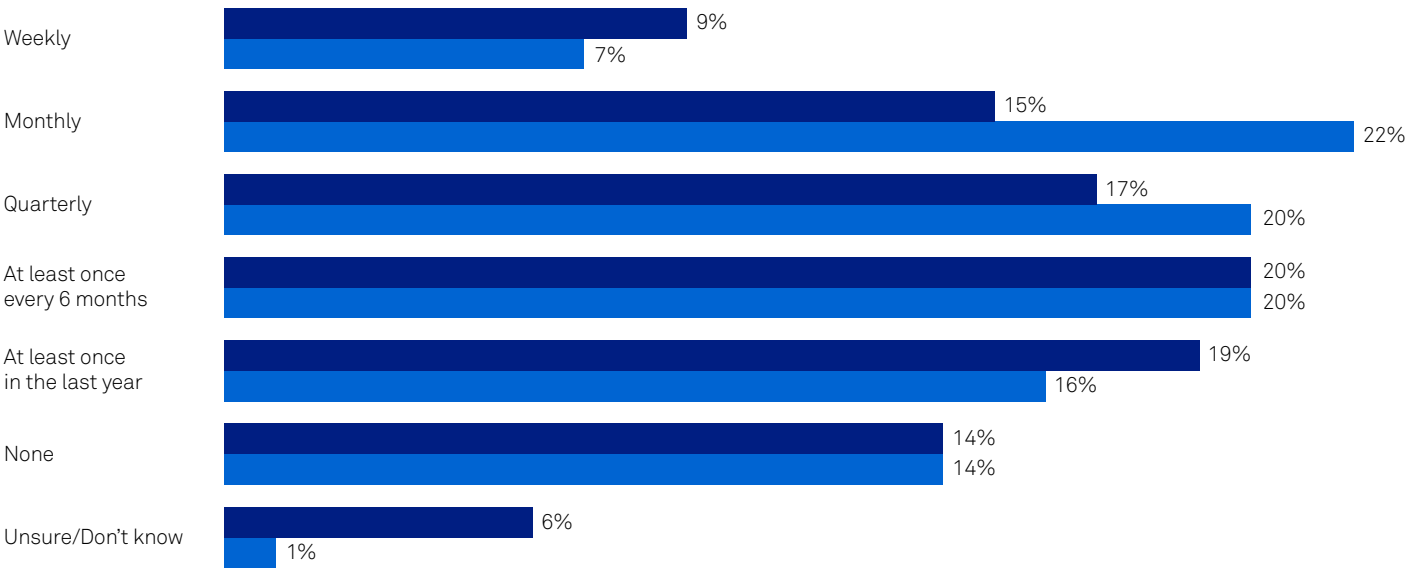
When it comes to other malware, including phishing, spyware, downloader, and adminware, organisations frequently experience incidents (87 per cent). Fifty five per cent of European respondents reported experiencing such incidents at least quarterly and 11 per cent reported experiencing incidents on a weekly basis. Europol's 2018 report identified that the number of banking trojans and other financial malware remains comparatively low. Yet malware such as Carbanak, Dridex, Emotet, Tinba, and Trickbot are enough to demonstrate ongoing challenges faced by the financial services sector.[11] The data cited in Europol's 2018 report is based on incidents reported to law enforcement and it is likely that some organisations did not report some incidents to authorities in order to protect their reputation. Since the implementation of the GDPR, the reporting of data breaches is now a legal requirement across the EU.

DDoS attacks remain one of the most frequent attacks experienced in Europe, with 49 per cent of European respondents reporting at least quarterly incidents (this was 60 per cent among public sector organisations). The largest known DDoS attack was recorded in 2018, peaking at 1.35 Tbps.[12] Botnets attacking IoT deployments has become a significant threat. According to reports monitored by Europol, a DDoS attack on two Swedish ISPs crippled train networks in there, and shut down communications on the Finnish Åland Islands after a telecom provider was attacked.[13]

[11] Europol (2018). Internet Organized Crime Threat Assessment (IOCTA). Retrieved from *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*
[12] Newman, L. (2018, March 1). Github Survived the Biggest DDoS Attack Recoded. Retrieved from *https://www.wired.com/story/github-ddos-memcached/*
[13] Europol (2018). Internet Organized Crime Threat Assessment (IOCTA). Retrieved from *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*

Q. How frequently has your organisation experienced the following security incidents in the past year?

A subset of European organisations that have experienced APT and DDoS in last 12 months



Europe results, n=322 (subset)

APT DDoS

Many malware incidents are suspected to originate from acts of advanced persistent threat (APT) groups associated with nation states, as opposed to financially motivated criminals. Twenty four per cent of European respondents reported experiencing APT attacks on a weekly or monthly basis, 13 per cent think the greatest risk of IT security is most likely to be the result of external hackers motivated by espionage, including state-assisted hackers. Europol's 2018 report suggests that many attacks on key industries and critical infrastructures tended to be part of APT activity.[14] These include the health services, telecommunications, transport, manufacturing and financial services industries, often with attacks leveraging one or more of the National Security Agency (NSA) exploits. Leaked by the Shadow Brokers group in April 2017 and incorporating self-replicating worm functionality, this accounted for the speed and spread of the infections.[15]

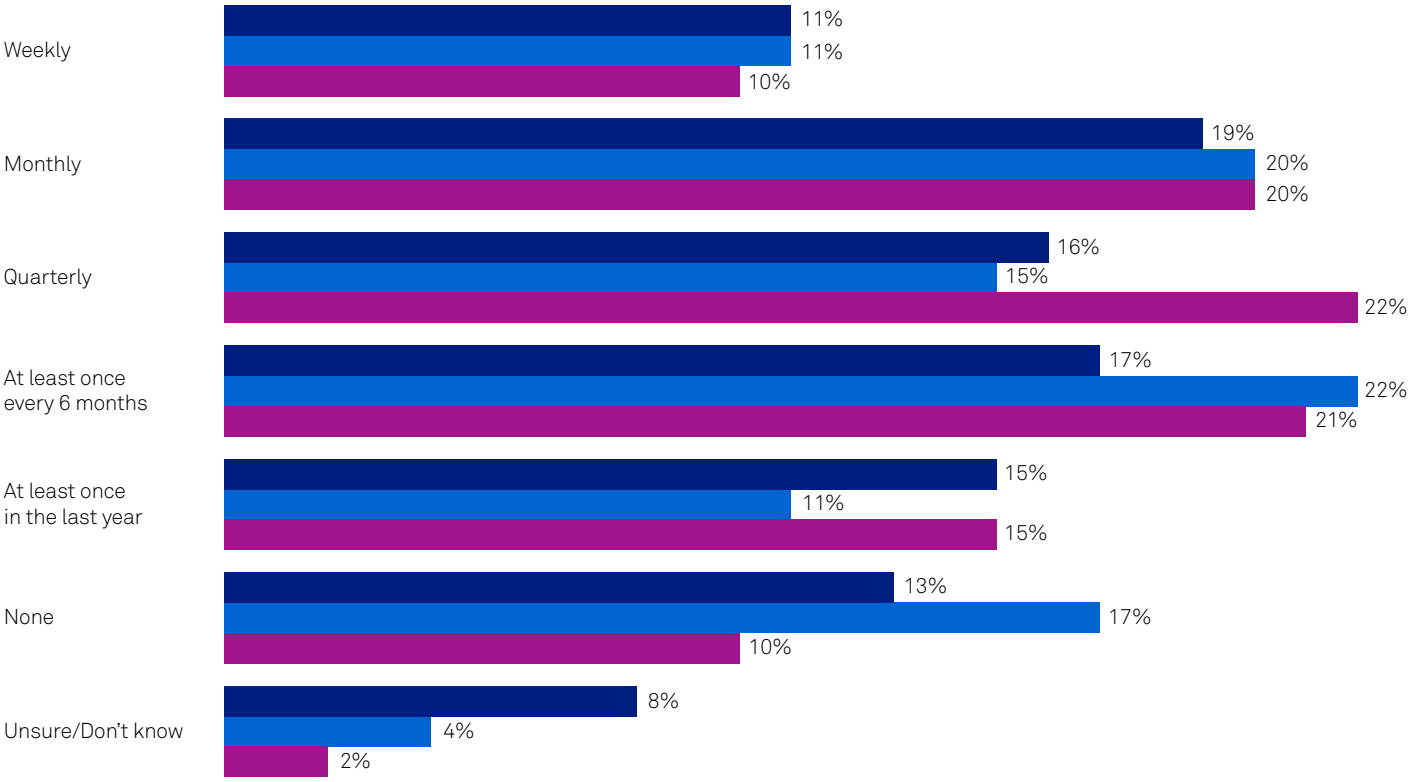
[14] Europol (2018). Internet Organized Crime Threat Assessment (IOCTA). Retrieved from *https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018*
[15] Ibid.

Human Behaviour Incidents

More 'traditional' security incidents that rely less on automation and more on human behaviour, such as hacking, are experienced even more by organisations in Europe than malware, DDoS, and APT incidents. At least 30 per cent of European respondents reported monthly or weekly brute force hacking, malicious insider and employee human error incidents during 2018. The latter type was most prevalent overall, with 88 per cent of European respondents reporting experiencing these incidents at least once in the last 12 months.

Q. How frequently has your organisation experienced the following security incidents in the past year?

A subset of European organisations that have experienced hacking, malicious insider, and human error in last 12 months



Europe results, n=322 (subset)

While the data does not differ too much between the type of organisations surveyed, it is notable that malicious insider incidents occurred (at least once) in fewer organisations within the local/national private sector (74 per cent) than the other organisation types, while hacking incidents occurred in fewer public sector organisations (77 per cent) than the others.

Other Incidents

Malware, DDoS and APTs are only some of the incidents routinely experienced by organisations in Europe and around the world. There are also incidents where employees fall victim to an attack, such as a business email compromise (BEC) event. In this exploit, the attacker typically uses the identity of an employee to trick the target into sending money to the attacker's account. The FBI reported BEC scams have cost victims more than US$12.5 billion dollars in the last five years.[16]

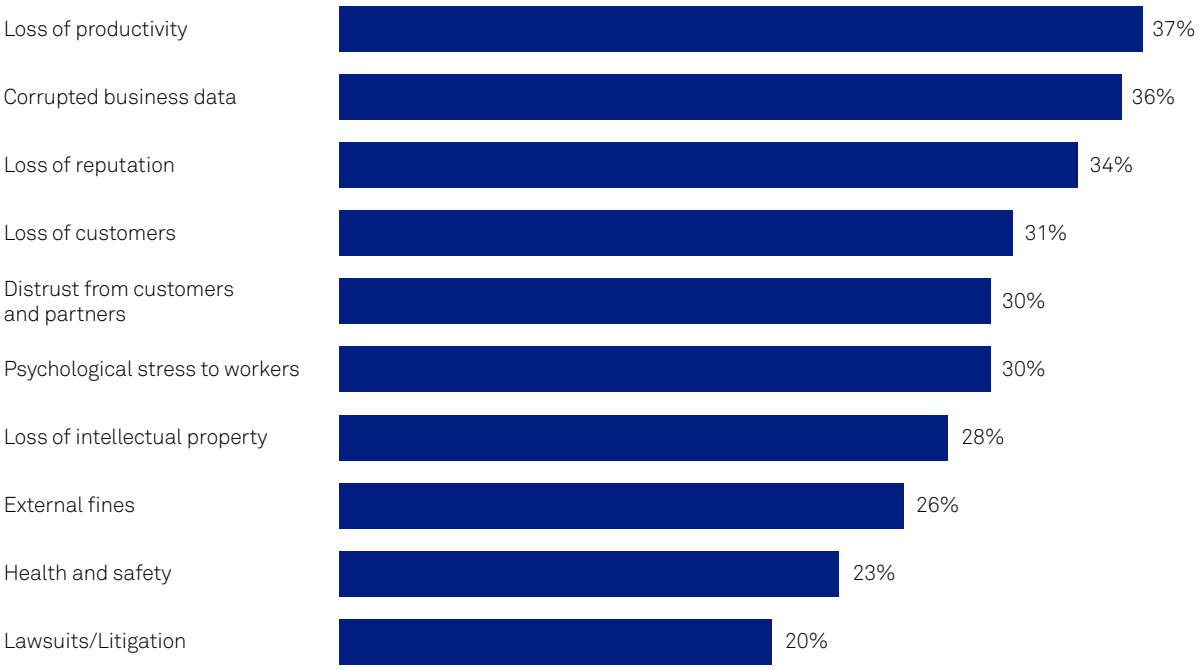
In our research, 49 per cent, within the subset of European respondents reporting a security attack, experienced BEC on a weekly, monthly or quarterly basis. Our European respondents reported identity theft and phishing incidents occurred at a similar rate. Attacks on OT processes (56 per cent) and systems/devices (54 per cent) occurred in even more organisations at least quarterly. These attacks impacted industrial control system processes and events such as supervisory control and data acquisition or SCADA, and also hardware ranging from video cameras to heating, ventilation, and air conditioning systems (HVACs).

[16] Federal Bureau of Investigation (2018, July 12). Public service announcement. Business E-mail Compromise The 12 Billion Dollar Scam. Retrieved from *https://www.ic3.gov/media/2018/180712.aspx*

Impacts of Cyber Crime

Cybercrime can impact an organisation in various ways. When asked about the potential impacts resulting from a major security breach in their organisation most of our European respondents identified loss of productivity (37 per cent). This was especially true in the local/national private sector (42 per cent) and MNC (37 per cent) organisations. Public sector organisations on the other hand most frequently cited the impact of corrupted business data (46 per cent), with loss of productivity coming in fourth at 26 per cent behind psychological stress to workers (36 per cent), and loss of reputation (31 per cent). These differences may reflect higher private sector organisation confidence in their data backup processes, in addition to the inherently high value they place on productivity.

Q: What are the more concerning potential impacts of a major security breach in your organisation?



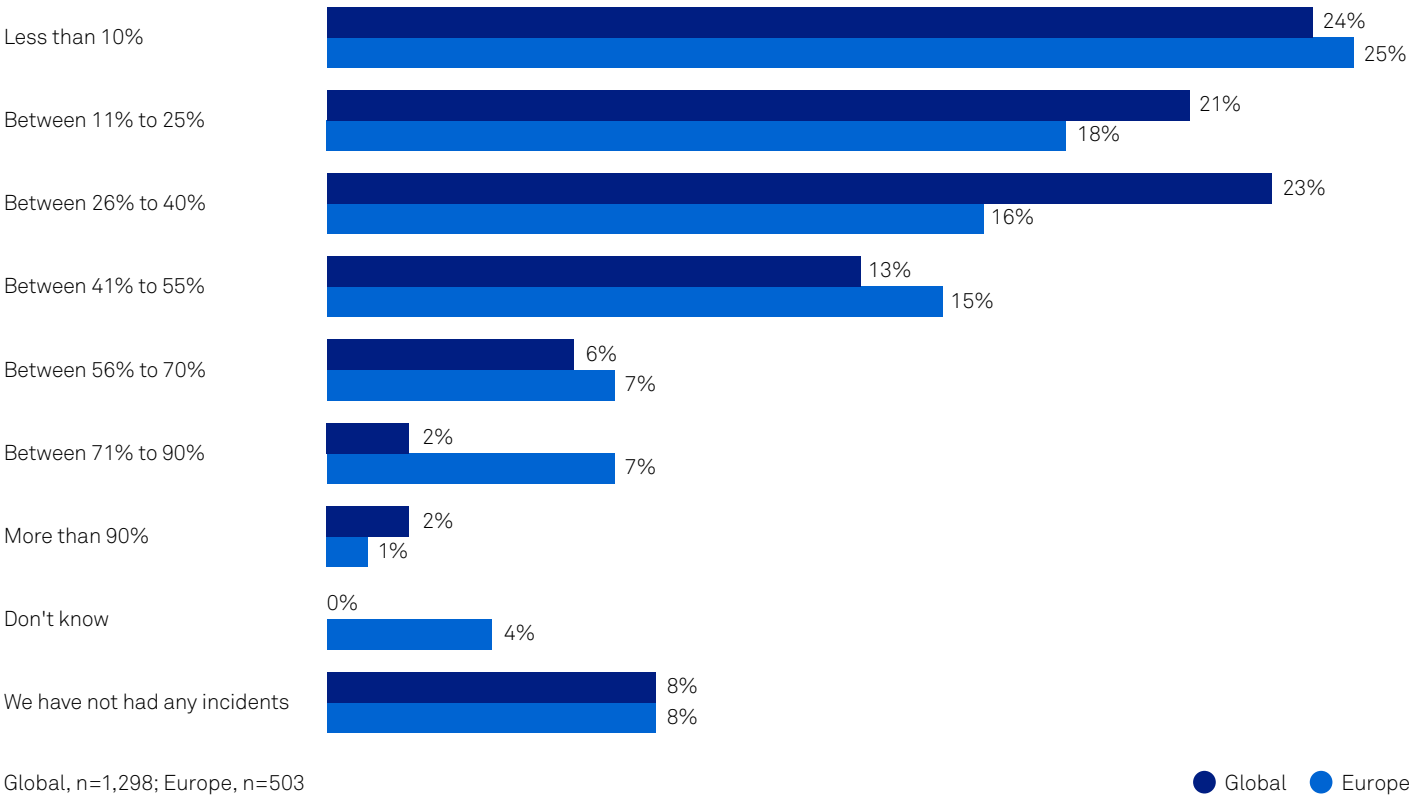
Europe results, n=322 (subset)

In addition to potential impacts of a breach, we also asked respondents about the actual impacts they experienced – whether caused by a major breach or common incident – in the last year. In terms of outright security attacks, 52 per cent of organisations reported experiencing at least one during the past year. Loss of productivity from a security breach is a common concern, but a business interruption due to a breach is even more serious. European respondents reported experiencing business interruption from a breach due to an attack or otherwise, (64 per cent) within the past year. MNCs are most likely to have suffered a business interruption at least once per quarter (23 per cent). When it comes to local/national private sector enterprises, 10 per cent of European respondents reported suffering from business interruptions due to security breaches with staggering frequency (i.e. on a weekly basis).

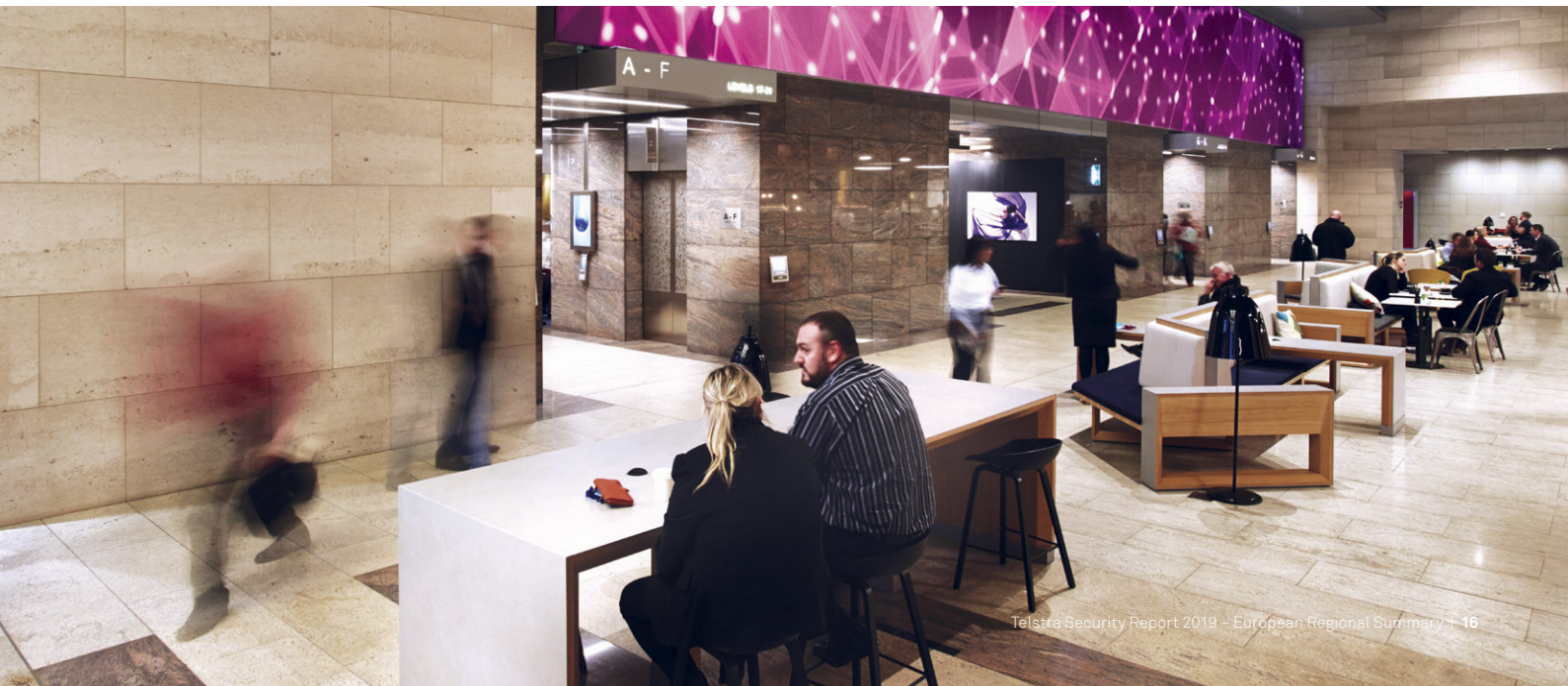
Undetected Breaches

The impact of detectable attacks, discussed previously, are easy to measure but frustrating to endure. What aren't as easy to measure are breaches that go undetected (whether for a short period of time, or even indefinitely). When we asked respondents what percentage of data breaches went undetected in the past year, a quarter of respondents reported that less than 10 per cent of breaches were undetected. Nearly a third of organisations (30 per cent) estimate that breaches occur completely under the radar over 40 per cent of the time.

Q: In your best estimate, what percentage of data breaches have gone undetected in the past year?



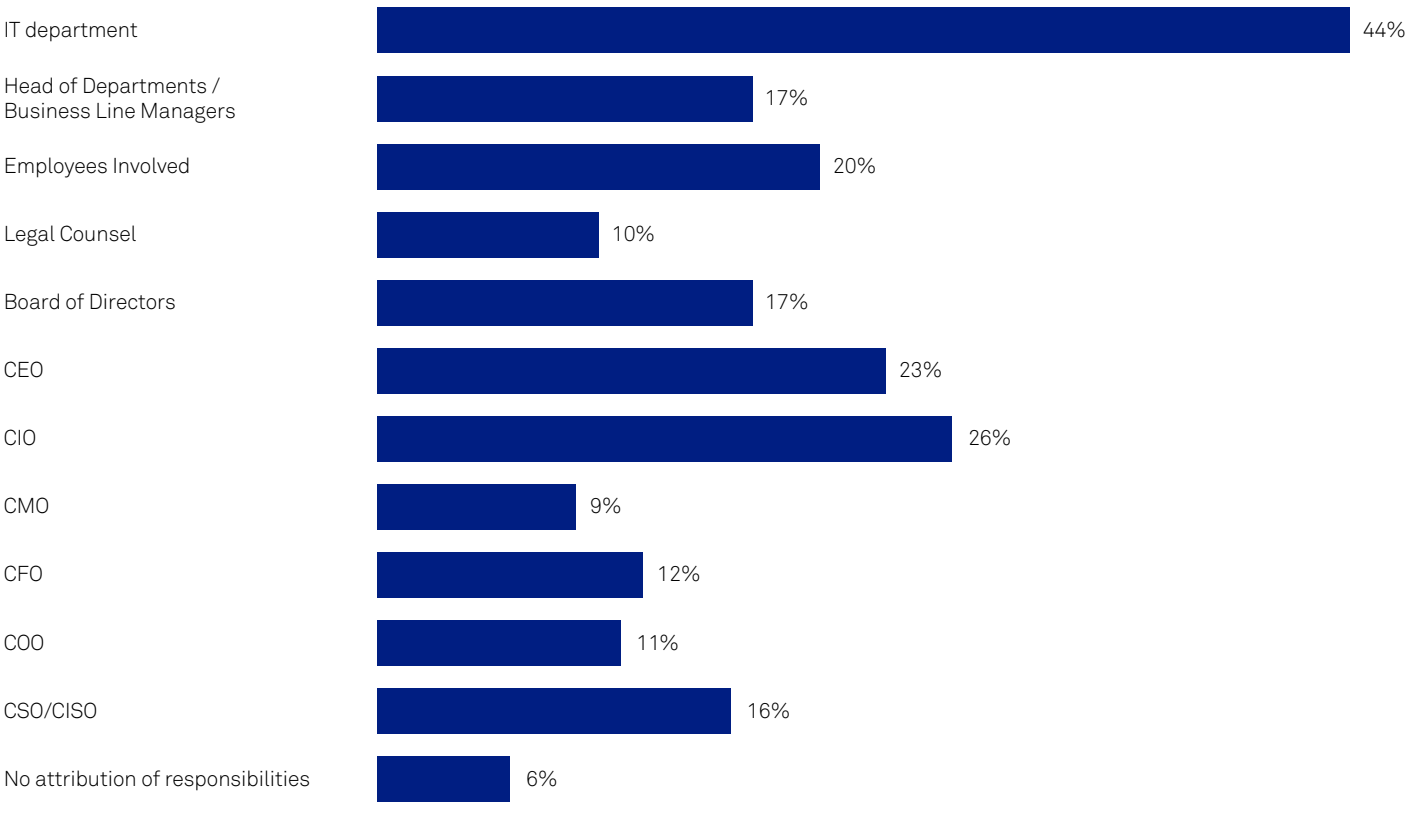
Global, n=1,298; Europe, n=503



Cyber Preparation and Incident Response

Most organisations understand that cyber and electronic security requires continuous investment and not just ad hoc attention. For this reason, European respondents reported significant security budgets, ongoing evaluation and deployment of multiple security technologies and services, and regular executive and board oversight of security policies and operations. Still, it is telling that when it comes to who in their organisation is ultimately responsible for cyber security incidents, just 16 per cent of organisations cite an actual chief security officer (CSO/CISO). In modern European organisations, the IT department owns security issues more than any other group or executive (44 per cent).

Q: In the event of a cyber security incident, who is ultimately held responsible?



Europe results, n=503

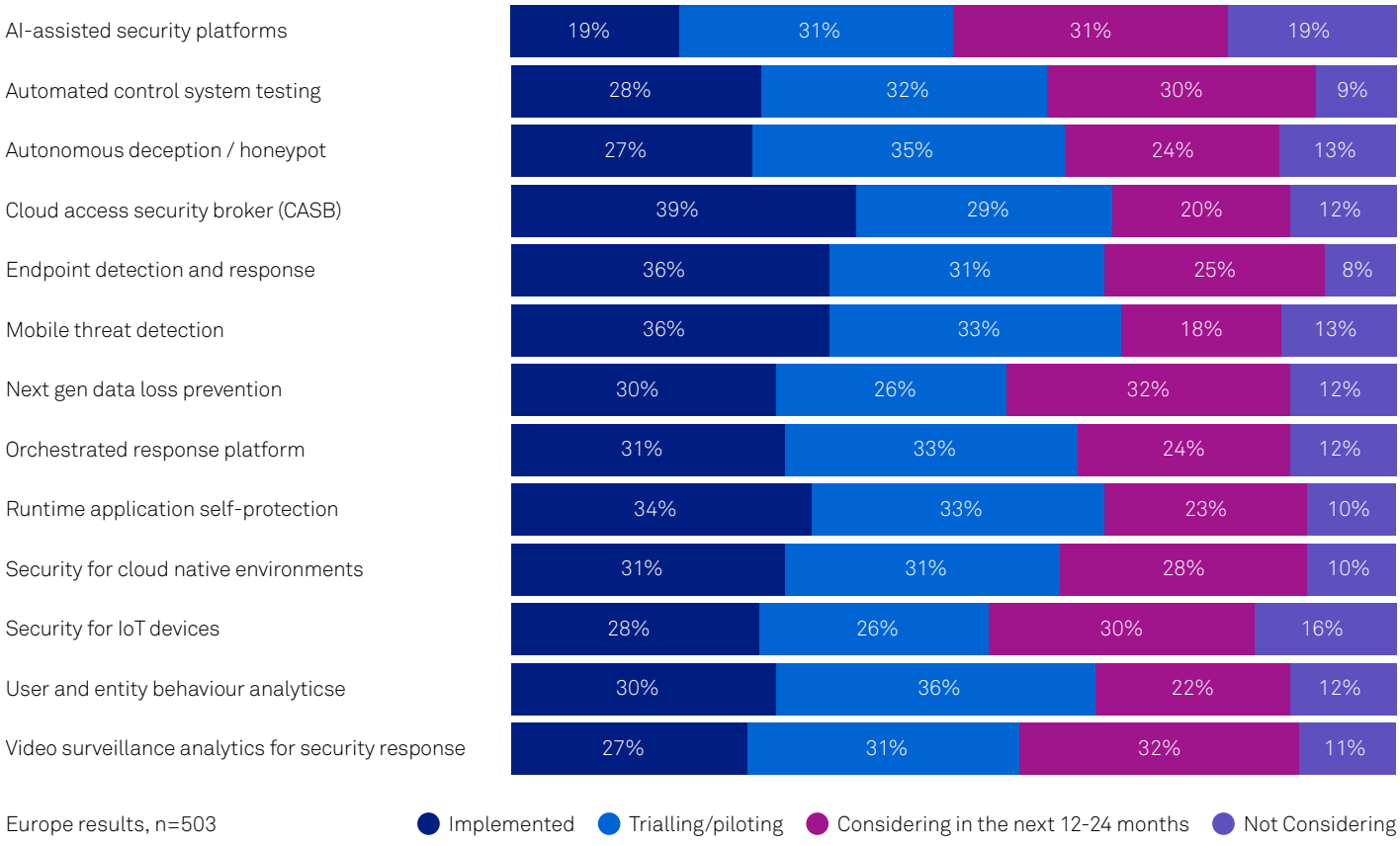
The IT department is not the only interested party when it comes to organisational security. This is reflected in the broad range of executives and departments routinely notified when breaches occur. Our European respondents reported that CEOs and boards of directors are notified more frequently (35 per cent and 31 per cent) than any other individual or group (other than the CIO/IT department). When it comes to any level of formal involvement in cyber security, more than half of respondents see high or very high involvement from non-IT departments including operations and client services.

Cyber Defence Operations Today

Whether under the daily management of the IT department or a dedicated security team, cyber and electronic security operations rely on an extensive arsenal of technologies and services. Firewalls, anti-virus and other content and network security solutions are pervasive in the enterprise across all sectors. This survey focuses on enterprise deployments and plans for emerging security technologies and approaches.

Artificial intelligence (AI) is globally one of the frequently discussed emerging technologies organisations. Although machine learning (ML) has been in use in security intelligence solutions for years, only 50 per cent of European organisations surveyed have implemented or plan to implement AI-assisted platforms. Nineteen per cent of European respondents reported they are currently not considering AI assisted platforms. More European organisations, are rolling out or have implemented other forms of security automation including automated control system testing (60 per cent) and autonomous deception/honeypot technologies (62 per cent). Next-generation data leakage prevention (DLP) incorporating ML and user analytics has been deployed or is being trialled by 56 per cent of European respondents.

Q: Which of the following emerging technologies or capabilities is your organisation considering/has your organisation implemented?

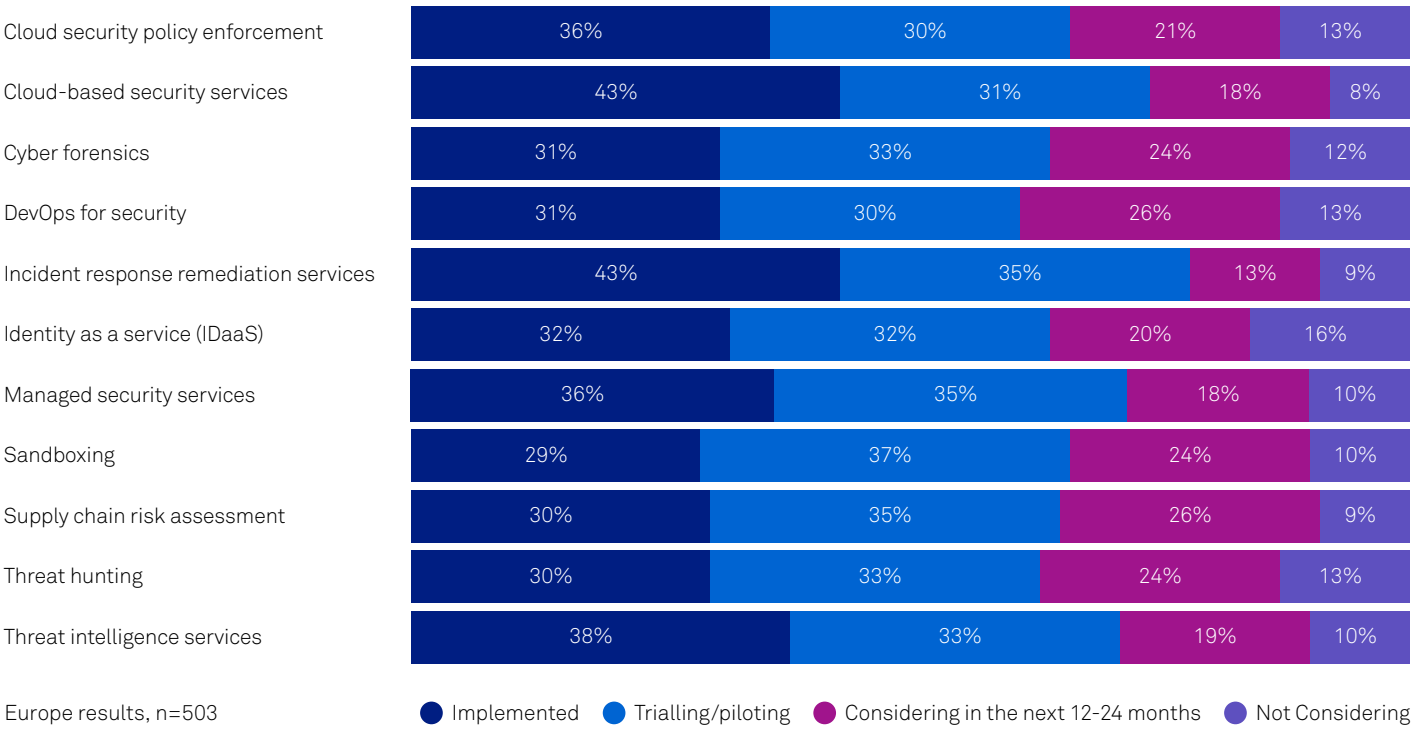


As noted previously, cloud services were frequently cited by European respondents when asked about their primary sources of concern regarding security attacks. In the above table, this is reflected in cloud access security broker (CASB) technology having been implemented already by 39 per cent of organisations. Respondents also identified security for cloud native environments as one of the top five technologies already implemented in the previous table (page 18).

The cloud is also seen as a security enabler and platform for the delivery of third-party security services. Rather than building cyber security infrastructure on premise and managing it in-house or with the help of a managed security service provider, leveraging cloud-based services frees up capex and personnel. Organisations can shift investments to specific professional skills needed in-house, while benefiting from the XaaS cloud model for key security intelligence and analytics solutions in particular.

Among European respondents, 43 per cent identified both cloud-based security services and incident response remediation as initiatives that have already been implemented, with over 30 per cent trialling or rolling out both of these capabilities (31 per cent and 35 per cent respectively). Other established capabilities include threat intelligence, and cloud-based security policy enforcement, which considers areas such as access control. Thirty six per cent of European respondents reported also adopting security as a managed security service. Adoption is most likely to address some of the pain points experienced by the European respondents, such as training of staff and keeping up to date with the latest technologies.

Q: What stage of implementation are you at with the following security service initiatives?



In Summary

Despite the increasingly focussed state of alert among European organisations, the threat of security breaches from internal and external threats continues to challenge even the best prepared security teams. With nearly a third of European respondents estimating that up to 60 per cent of security breaches still go undetected, those tasked with protecting their organisations have acknowledged the need for even more executive engagement, investment, and stronger security policies and solutions.

Our European respondents reported that 78 per cent have a plan in place for incident response, with 88 per cent reporting that testing and review of the plan is performed monthly or quarterly. Constant review is necessary, as the threat landscape, and security capabilities and strategies that aid in response, both continuously evolve.

Investment in a number of emerging tools and approaches is being planned and implemented by most enterprises surveyed, as they consider how best to improve their level of preparedness for security incident response. These include:

- DevOps for Security. The rapid pace of change makes security a natural place to implement DevOps practices. SecOps can deliver benefits beyond software development but also in security operations. Vulnerabilities can be identified earlier by having all CISO security reviews and assessments on the agenda for both development and IT operations.
- Security as a Service. The constantly changing and growing threat landscape is also a factor in the global security skills shortage. Skilled and certified professionals are highly sought after, while new security specialists are recruited directly into security technology or service provider organisations. This makes the use of third-party managed services more attractive, as skills are increasingly concentrated and even more difficult to recruit for the typical enterprise or public sector organisation. Everything from threat intelligence, to identity as a service, incident remediation, and overall managed security services are among the most heavily planned for or already implemented strategies for improving incident response.
- Supply Chain Risk Assessment. With an increasing number of attacks originating from the supply chain, such as affiliates and partners, businesses are looking at ways to manage the security risks at all points across the supply chain. Attacks launched on a third-party with weaker defences as a backdoor to a primary target with stronger defences, often carried out through hacking of credentials with greater system privileges, are on the rise. In Europe, 91 per cent of organisations have implemented or are considering implementing supply chain risk assessments to better protect against attacks on the weakest link in their ecosystems.

There are also some general best practices businesses should consider:

Multi-layered Defences

With the number of threats that can penetrate IT systems, this approach, also known as defence in depth, relies on multiple layers of security controls throughout ICT and physical security environments. Its intent is to provide redundancy in the event that one security control fails or is exploited. Layered security examples include: combining the use of web security gateways to block malicious code from being downloaded, whitelisting to prevent unknown executable files from running, and advanced endpoint protection on laptops, mobiles, and servers. In addition, continue to run and update anti-malware, managed firewalls, and VPNs to improve security across corporate networks. Passwords should also be alphanumeric, entirely unique and memorable. Password managers or passphrases should also be considered – with the purpose of enabling employees to select long, complex and unique passwords whilst also allowing them to be memorable.

Architecture Reviews

Architectural reviews should be a constant for planning for a system refresh, considering ways to interconnect physical with electronic or needing a third-party validation. This should also include system and vulnerability scans, penetration testing, and other tests to understand environments, discover vulnerabilities and prioritise fixes. Over the next 24 months, 80 per cent or more of an organisation's employees will be performing the core tasks required for their job from a mobile device. Up to 20 per cent of organisations may have moved their entire IT infrastructure to the cloud, with many employees working from home and other remote locations.[17] Considering the demands placed on IT, architectural reviews conducted regularly can help a business with an improved security posture.

Employee Awareness

Considering security adversaries will often choose the path of least resistance before launching an attack, employees can be the focus of attacks. This can be the benign employee who accidently clicked a malicious link or a person who has been targeted through social media. Organisations that have formal training programs will likely minimise security gaps, incidents and overtime contribute to improved security resiliency. A strong security capability rests on a well-trained and vigilant workforce, and having strong processes and technology capabilities. The weakest link can often be around individual employees.

The Five Knows of Cyber Security

The five things businesses should know to effectively manage risk include: know the value of their data; know who has access to their data; know where their data is; know who is protecting their data; and know how well their data is protected.[18] With these basic practices in place, known as Telstra's Five Knows of Cyber Security, additional measures may also be needed. For example, data classification can help businesses know what they own, identity and access management can ensure the right employees have the right level of access.

[17] GlobalData market estimates
[18] Telstra Five Knows of Cyber Security. Retrieved from *https://www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf*

Acknowledgements

Telstra Contributions

- Corporate Affairs
- Enterprise Marketing and pricing
- Product and Technology
- Telstra Cyber Security
- Telstra Legal Services

About Telstra Security Services

Telstra's Managed Security Services can help you navigate the security landscape and manage risk across your cyber, electronic & IoT ecosystems. Underpinned by our powerful open source Managed Security Service platform, our solutions leverage our purpose built Security Operations Centres (SOCs) in Sydney and Melbourne. These SOCs provide the visibility, expertise, intelligence and tools our customers need to help secure their business in an evolving threat environment.

Cyber Security Services

Our cyber security services are highly flexible and new services are regularly added. Our current capability includes:

Security Monitoring

Our Security Monitoring service feeds event data from a variety of sources across your on-premises, IoT and cloud infrastructure. With 24/7 visibility and actionable reports, you can gain deeper understanding of your risk status and clearer resolution paths for mitigation.

Incident Response

Receive priority access to Telstra's highly-skilled Computer Emergency Response Team (CERT) who respond quickly to any suspected incident, such as unauthorised access to your systems, electronic data loss or theft, viruses, suspicious network activity and ransomware attacks.

Electronic Security

Organisations in every sector have security and monitoring challenges, but we understand that your business has unique needs. We have always provided network services to the electronic security industry, and now we've partnered with leading security companies to combine their expertise with our high performance network. Together, we provide a suite of electronic security solutions that go beyond safety and loss prevention, offering reliable, convenient and effective ways to help protect your business and enhance business outcomes – now and into the future.

Consulting Services

Our team of security consultants can help you align your security and risk environment with your business drivers, innovate with industry leading protection, navigate complex security challenges, or take a holistic approach to cyber security risk management. Our capabilities include security consulting, security compliance, incident preparedness, intelligence and analytics, network and cloud security, end-point, mobile and application protection, as well as managed security services.

For More Information

We can assist your organisation to manage risk and meet your security requirements. For more information about our services, contact your Telstra Account Executive or visit telstra.com/enterprisesecurity

Thank you to our Partners for their contributions to this report

Carbon Black. · Cisco · Cofense · CrowdStrike · Cylance · F5 · FireEye · FirstWave Cloud Security Technology

Fortinet · McAfee Together is power. · Microsoft · paloalto Networks · Qualys. · Redshield · Symantec · Zimperium Mobile Threat Defense

Telstra regional office headquarters

Asia

Level 19, Telecom House
3 Gloucester Road
Wan Chai, Hong Kong
T +852 2983 3388

EMEA

2nd Floor, Blue Fin Bldg,
110 Southwark Street
London, SE1 OTA
T +44 207 965 0000

Americas

44th Floor
40 Wall Street
New York, NY 10005
T +1 877 835 7872

Australia

363 Oxford Street
Paddington, NSW
Sydney 2021
T +61 2 8202 5134

Visit telstraglobal.com