Redefining the security culture – a better way to protect your business

pwc

Contents

Redefining the security culture – a better way to protect your business
Information Security Breaches Survey 2017 – Key takeaways

Survey carried out by:

infosecurity BELGIUM

Spam, phishing, hackers and more and more advanced types of cybercrime continue to form a realistic threat to businesses. Infosecurity.be tackles current IT security issues and is a must for every IT professional. Over the past few years, Infosecurity.be has proved to be the online meeting place and exhibition for IT managers and IT professionals in the field of IT security. Alongside its exhibitions, Storage Expo and The Tooling Event, Infosecurity.be offers market leaders, associations, speakers and other IT professionals a platform to share ideas, techniques, services and visions on current IT topics with a focus on the central theme 'Data Centric World'.

More information on www.infosecurity.be.

pwc

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services.

Our security practice, spanning across our global network, has more than 30 years of experience, with over 90 information security professionals in Belgium and 3,500 globally. Our integrated approach recognises the multifaceted nature of information security and draws on specialists in process improvement, value management, change management, human resources, forensics and risk. PwC has gained an international reputation for our technical expertise and strong security skills in strategy, design, implementation and assessment services.

Find out more and tell us what matters to you by visiting us at www.pwc.be.

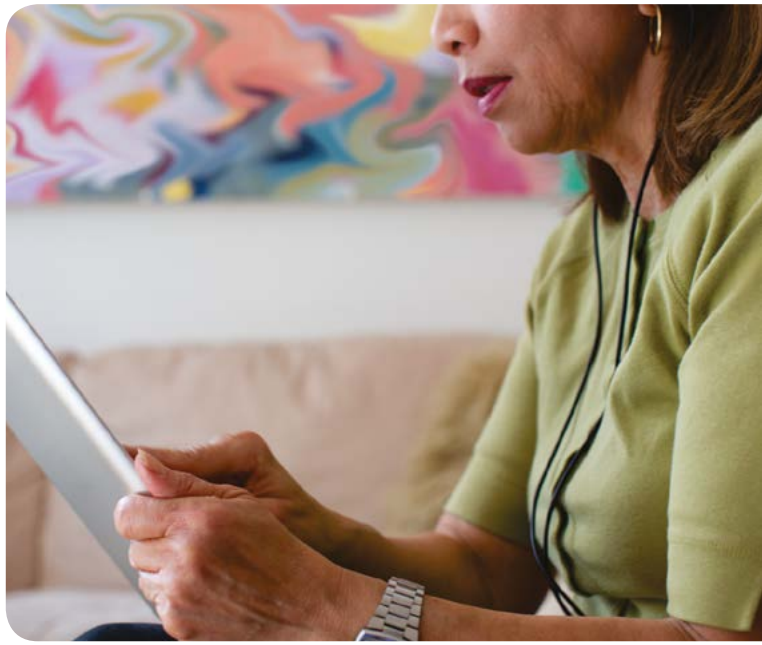
Introduction

Phishing attacks and their targeted variant, spear phishing, have increased in both frequency and complexity. Gone are the days of poorly worded and punctuated emails from banks gauchely requesting your password in a form for "security reasons". As phishers continue to hone their craft, the content of modern phishing mails is often indistinguishable from that of the legitimate messages they impersonate. The recent trend of leveraging various forms of malware, including more recently, ransomware, has made them potentially far more lethal.

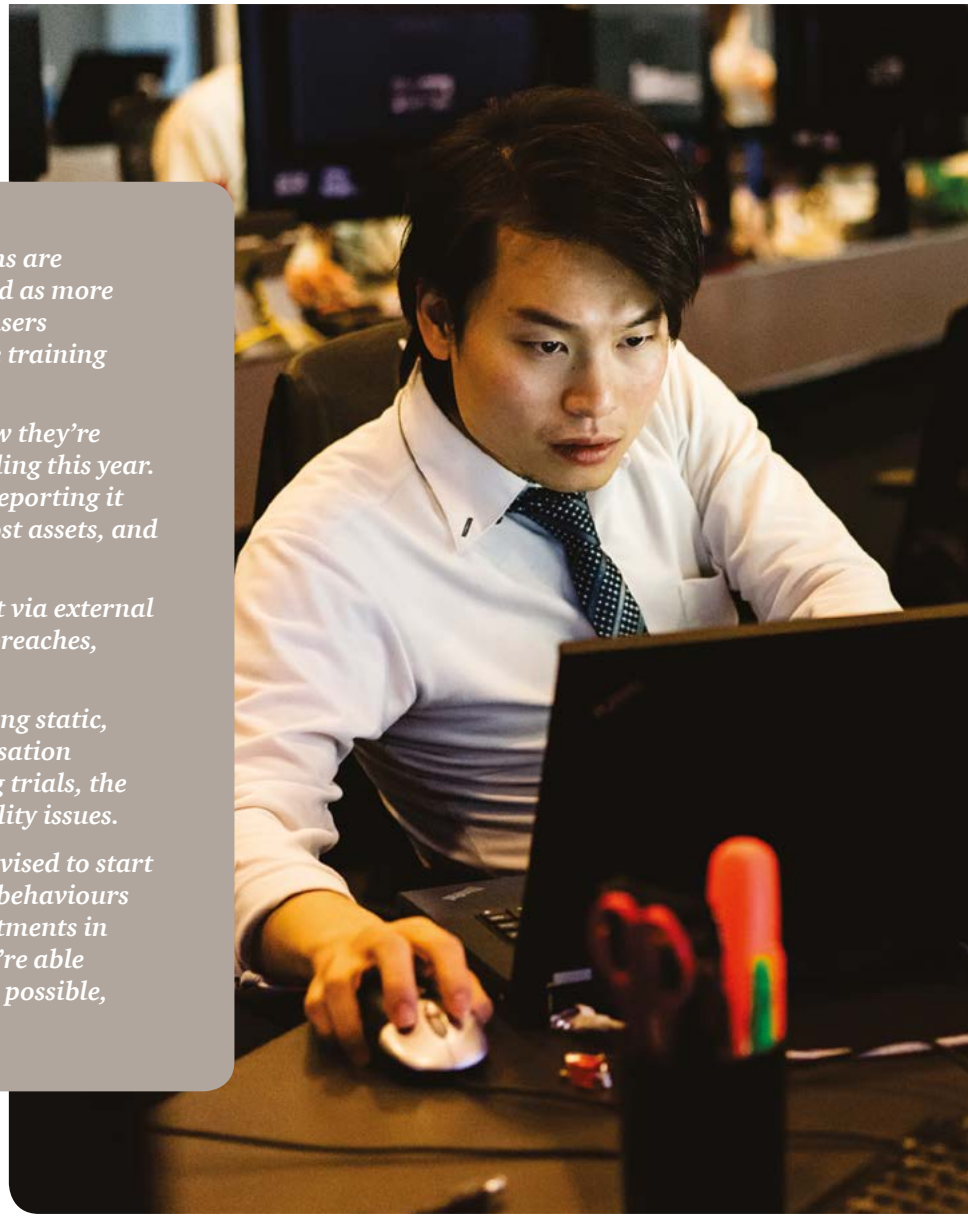
Imagine that somewhere in an organisation an employee receives an email and opens its attachment. Or they click on a link to a legitimate website which, unbeknownst to its users, was recently hijacked via a vulnerability in its popular content management system (CMS) software to serve malware to unsuspecting visitors. Half a second later, their hard drive hums or heats up for a short while before a picture of a shield or padlock fills the screen with a message informing them that their personal files are now encrypted and held ransom.

Think this sounds farfetched? According to the 2016 Verizon Data Breach Investigation Report, malware-induced breaches have increased exponentially since 2009 and they're becoming more successful: last year, 30% of sanctioned phishing emails were opened and in 12% of cases attachments or links clicked. That a quarter of computers in Belgium are infected by some form of malware - according to the Anti-Phishing Working Group (APWG) — is therefore not surprising. Sophos reports that 82% of malicious sites are hacked legitimate sites. In January 2017, a severe vulnerability was announced in the popular WordPress CMS. There's no reason why vulnerable sites couldn't be hijacked en masse to serve malware.

Users are increasingly targeted and continue to be an organisation's weakest link. Increased security awareness training, as currently practiced, doesn't appear to be having much effect on the rate of breaches. Neither is continued, purblind information security spending. It's time to do things differently.



Executive Summary



As results of our Information Security Breaches Survey (ISBS) 2017 survey highlight, organisations are struggling to deal with more targeted phishing and malware attacks, both in traditional forms and as more nefarious ransomware. Despite continued increases in ongoing security awareness programmes, users remain the chink in the organisational armour and will likely remain so until sufficiently effective training programmes are devised.

Information security budgets continue to grow, with little in the way of objective assessment of how they're spent. Protection of customer information became the biggest driver of information security spending this year. When organisations are breached however, the instinct to handle the incident internally without reporting it remains high. The cost to fix breaches remains disproportionately high compared to the value of lost assets, and the number of organisations unable to quantify the latter significant.

Most organisations prefer having internal incident response teams, whose skillset they supplement via external forensics firms when breaches occur. Threat intelligence is increasingly used to proactively detect breaches, although there is currently no evidence of reduction in the number of incidents.

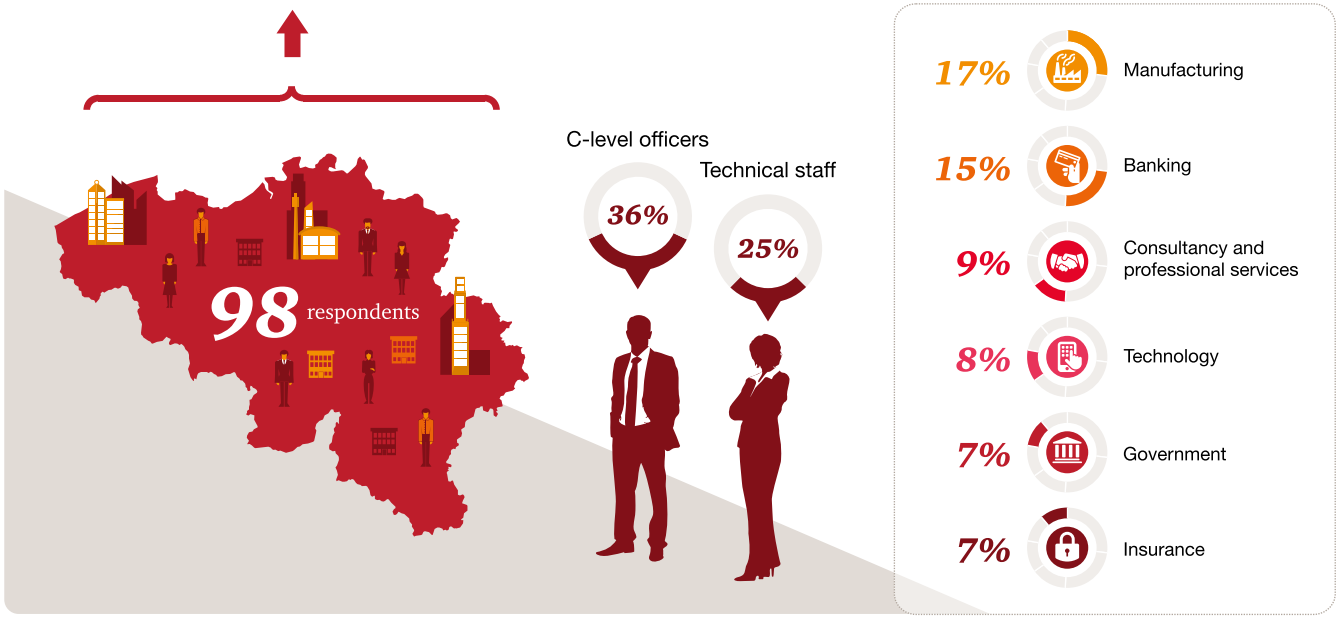
On the biometrics front, organisations have little appetite for behavioural biometrics, still favouring static, mostly fingerprint- and palm-based technologies. These are rarely deployed throughout an organisation though. While few respondents who plan to deploy biometrics reported encountering issues during trials, the reaction was not fully shared by those with production deployments who cited accuracy and usability issues.

Rather than reacting to breaches by continuing to do more of the same, organisations would be advised to start defining their security culture as a more effective means of shaping the judgements, decisions and behaviours of staff at key moments. They should first maximise the use and effectiveness of their current investments in tools, people and processes, and put in place a means of quantifying their effectiveness. When they're able to objectively show that investment in new technology is required, they should do so, giving, where possible, priority to technologies which empower end users to naturally make the right security decisions.

Methodology

The 2017 Information Security Breaches Survey was carried out by PwC Belgium and Infosecurity.be. It was conducted online from December 2016 to February 2017 with respondents representing organisations based in Belgium. It aims to provide a more focused view of the state of information security in Belgium than the global overview given by PwC's annual, far-reaching Global State of Information Security Survey (GSISS).

In what sector is your main business activity?



C-level officers are defined as respondents who describe their role as Chief Executive Officer, Chief Technology Officer, Chief Information Officer, Chief Information Security Officer or Chief Financial Officer. Technical staff were defined as respondents who describe their role Security Administrator, Security Engineer, Security Manager or IT Manager.

There were 98 respondents to the survey, from both large companies and SMEs, the majority of whom are active in their organisation's IT and information security domains. Thirty-six percent of survey respondents were C-level officers and 25% IT or security managers. Seventeen percent of the organisations surveyed were manufacturing companies and 15% were from the banking sector. Consultancy and professional services accounted for 9% of participants, and Technology companies for 8%. Government and Insurance organisations represented 7% each of the total.

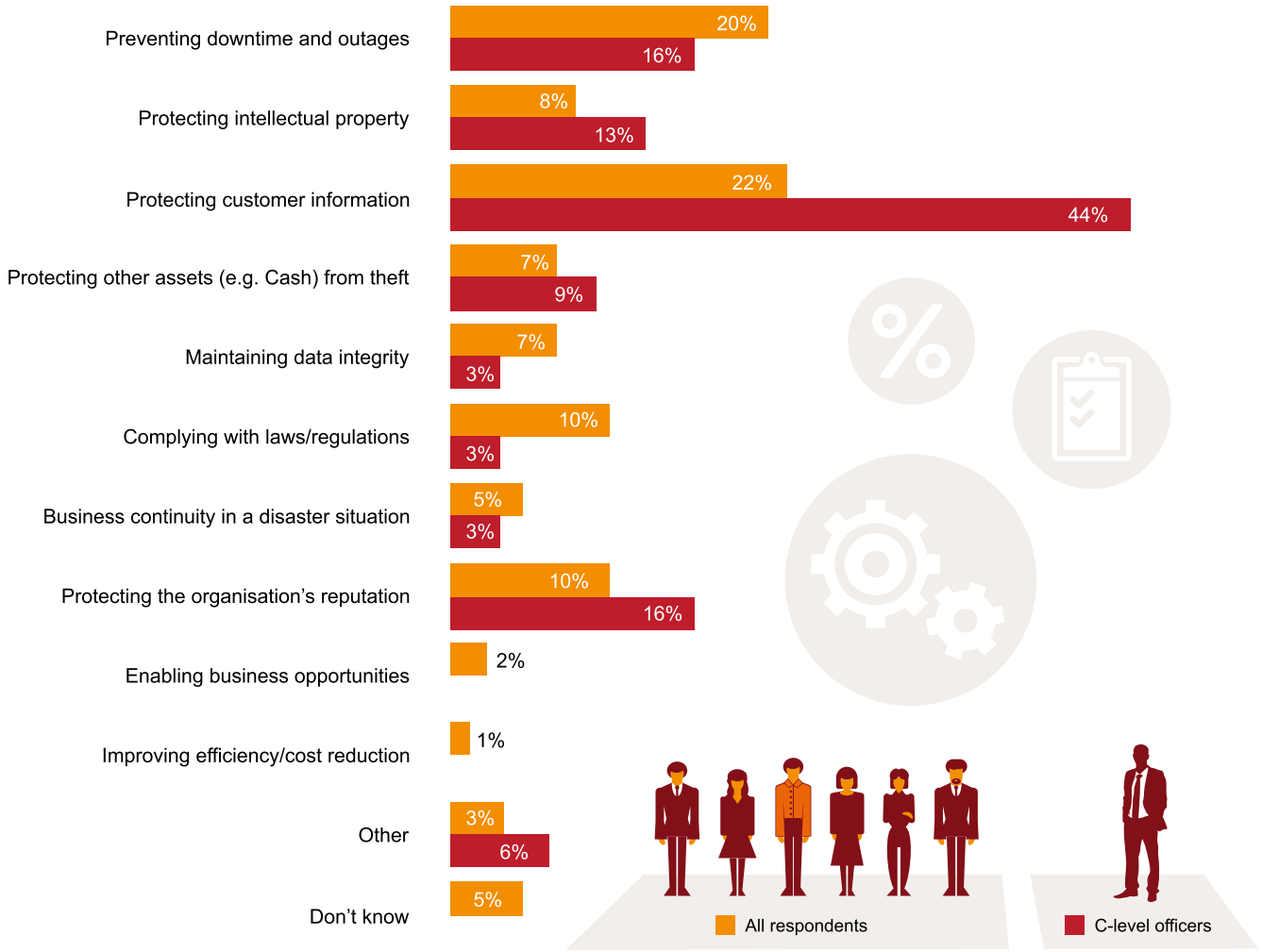
We changed the format this year for a number of reasons. Results of previous surveys indicate that while a number of interesting changes emerge each year, overall, the state of information security in Belgium evolves slowly. While annual tracking of certain trends in information security spending and breaches is useful and enlightening, for others, a timespan of two or three years is sufficient and more appropriate. By trimming core questions, we're better able to explore other interesting topics and allow participants to choose among them, yielding higher-quality answers. The new format also means respondents are able to complete the survey more quickly.

To enable meaningful year-on-year comparisons to be made, this year's survey kept the same questions at is core as in 2015, with only minor changes, to allow further insights to be gathered. We were careful to keep enough questions to allow for continued meaningful year-on-year comparisons initiated in previous versions. Respondents were also asked to complete questions from at least one of two topics, biometrics and incident response.

Six percent of survey respondents completed only the biometrics topic, 81% only the incident response and 13% completed both. In all cases, survey participants were required to also complete the core section of the survey pertaining more generally to breaches and security spending.

Information security spending

Which is the most important driver for your information security expenditure?



Our prediction in last year's survey that more organisations will prioritise the protection of customer information as the threat of sanctions under the General Data Protection Regulation (GDPR) looms closer is confirmed by this year's results; protection of customer information slid into first place with 22% of respondents indicating it's the most important driver for their information security spending, slightly ahead of the usual leading cause, preventing downtime and outages, which garnered 20% of responses compared to last year's 25%. Protecting the organisation's reputation and complying with laws and regulations were the next most popular, each at 10%.

However, the picture changes when considering respondent profiles. At C-level, protection of customer data is the most important driver of spending (44%) followed by protecting the organisation's reputation (16%). Complying with laws and regulations is prioritised more by technical profiles than C-levels.

While the heightened prioritisation of customer data is a promising sign of GDPR readiness, a number of other indicators still point in the wrong direction. The percentage of incidents only known about internally hasn't declined (74%). Almost half (43%) of respondents reported lacking a documented policy for communicating incidents, calling into question their readiness to comply with GDPR communication requirements.

The trend of increasing information security spending continues, with 46% of respondents reporting higher budgets this year than last and 37% reporting no change. With no sign of reduction in the number of reported breaches or their severity, the effectiveness of information security spending can be called into question. One third of survey participants report not formally evaluating the effectiveness of their spending on information security (the highest single category). Among those that do, a quarter of respondents say they monitor improvements in regulatory compliance, followed by measuring trends in the costs of security incidents (23%), measuring staff awareness (21%) and benchmarking security expenditure against other organisations (also 21%).

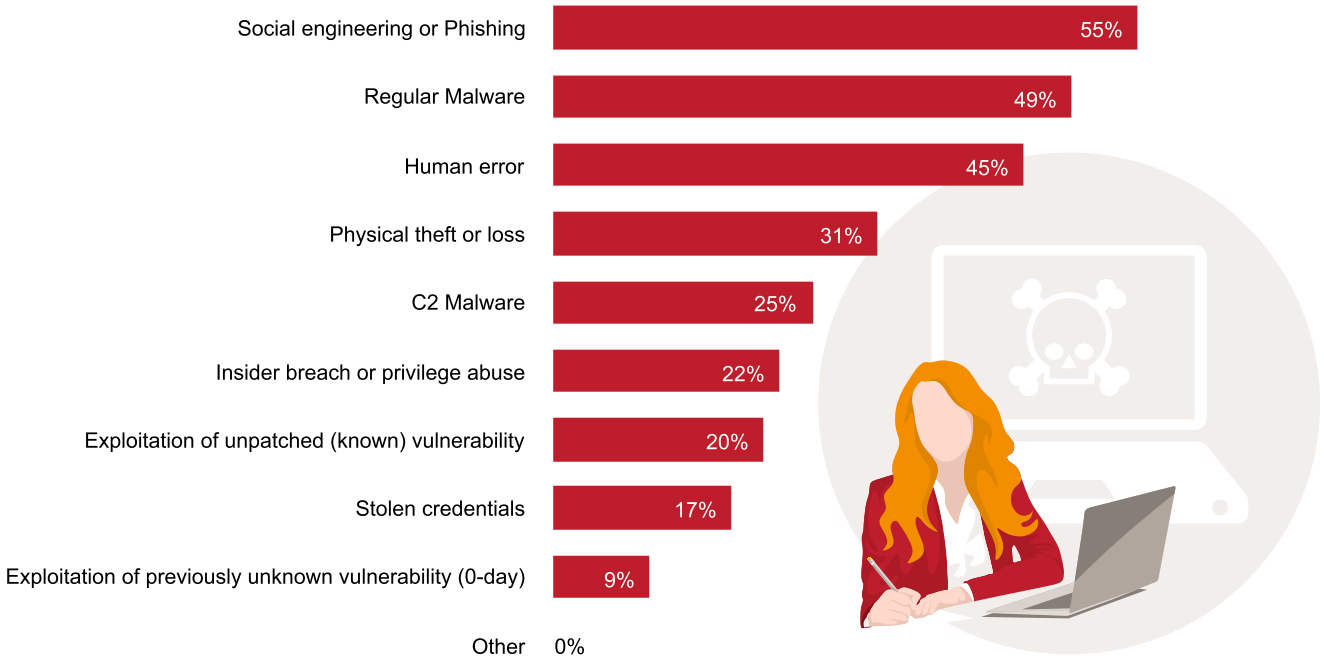
A number of observations can be offered here. While regulatory compliance is important, both in its own right, and as a stepping stone on the path to more mature organisational security and culture, it doesn't necessarily equate to higher security when practiced for compliance's sake alone. As a general rule, an organisation's security expenditure figures are not frequently shared publicly, which makes the fact that one in five respondents (with an even mix of C-level to technical profiles) use them to benchmark their spending a little puzzling.

Until organisations actively track their information security spending and objectively evaluate its effectiveness, we'll likely continue to see budgets growing without any commensurate observable improvements in security, as has been the case for the past few years.

Breaches

The percentage of people reporting a serious breach is largely unchanged from last year (15%), though we see a slight rise in respondents who don't know whether they were breached (12% vs 8% in 2016). Of those reporting a breach, almost one in three (29%) didn't know how long they had been breached for. This garnered a higher percentage of responses than any other answer with 24% citing the breach lasted a day, the next most popular answer. Given the statistics which indicate that data is successfully exfiltrated within minutes of a breach (source: Verizon 2016 Data Breach Investigations Report), the relatively short lifespan of breaches reported is isn't really comforting.

What underlying breach vectors led to the assets being compromised?



Causes

The top causes of breaches reported this year were inadvertent human error, lack of staff awareness of security risks, failure to follow a defined process and external attacks specifically targeting an organisation. The implication that human psychology, poor judgement and propensity to mistakes are key to appreciating the current breach landscape are confirmed by the incident response answers; the most frequent breach vector was social engineering or phishing (55%), followed by malware (49%) and human error (45%).

Overall, the direct link between human action and breaches is hard to ignore. More than half of respondents (57%) have implemented ongoing security awareness training programmes, continuing the trend of moving away from training at induction only. Unfortunately, this progressive move has yet to have any effect on the number and severity of breaches.

The causes of breaches are slightly different when grouped by respondent profile. Half of C-level respondents blame inadvertent human error, a quarter blame weakness in someone else's security (14% of respondents overall) and, interestingly, a further quarter blame insufficient priority placed on security by senior management (compared to 10% of respondents overall).

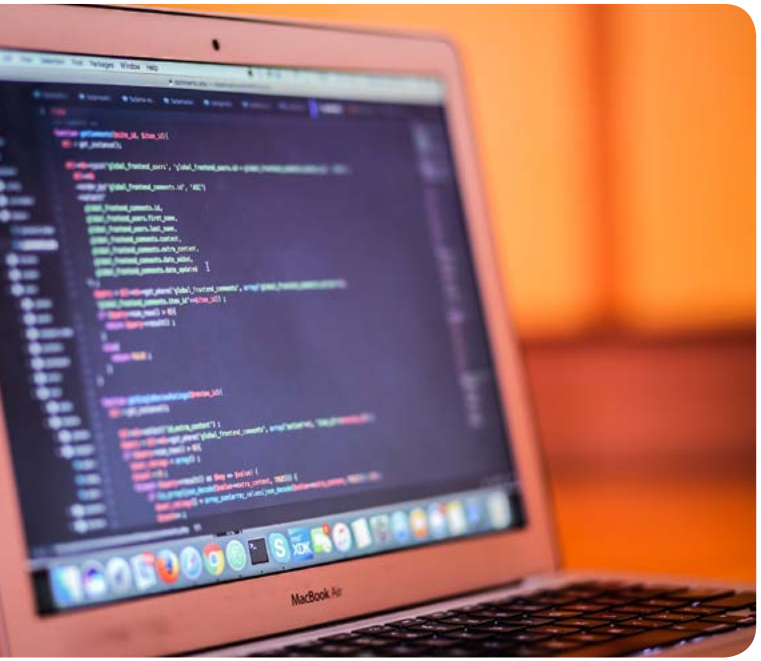
The move away from blaming management for insufficiently prioritising security continues; a three-year low was recorded with only 9% of respondents claiming it. This suggests that senior management responsible for IT now understand the importance of security enough to begin addressing technical staff demands and face the challenge of increasing the organisation's security maturity to realise clearer ownership and responsibility for data and processes. The conjecture is supported

by almost half (45%) of C-level respondents who think there is no clear view on who owns critical data and who's responsible for its protection. Globally, the number is lower (38%) due to a lower percentage of technical profiles sharing the view (34%). This suggests that responsibility for more tangible, technical assets (such as production servers, build environments, etc.) is better defined than that of higher-level ones like the systems development life cycle (SDLC) process or an organisation's operational risk framework. That a sizeable proportion of C-level respondents still blame management for insufficiently prioritising security concerns suggests that, in the eyes of their peers, not all C-level respondents are equally enlightened.

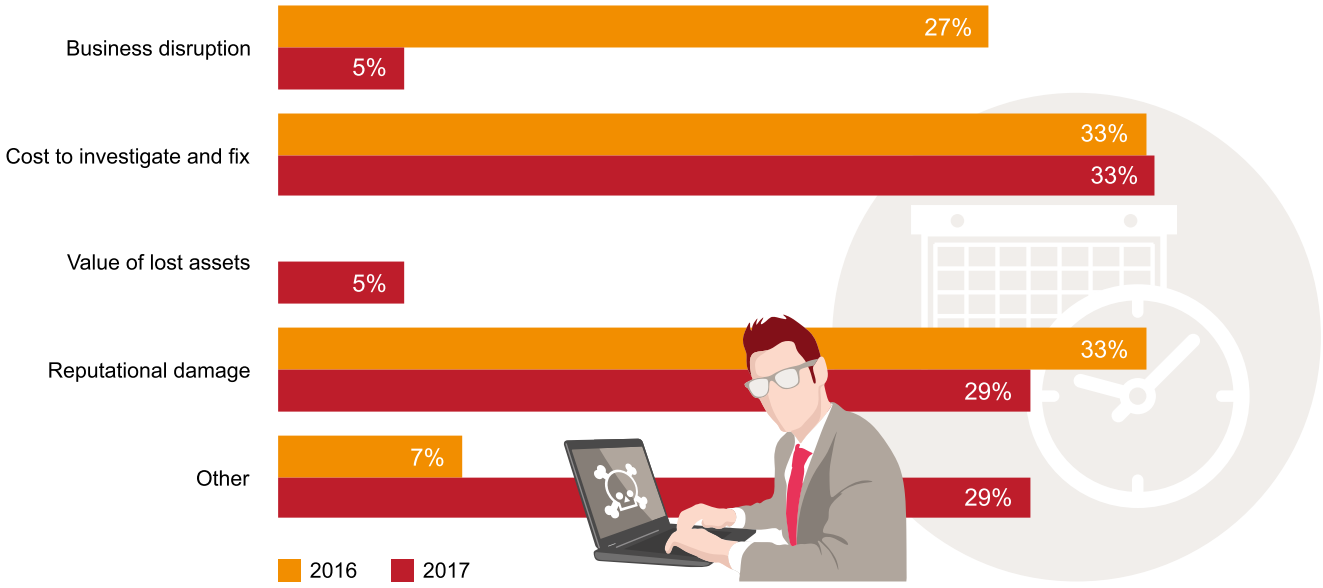
Impact

Breaches appear to have had more of a financial impact this year than last with only 21% of survey participants reporting no direct financial losses as a result of a breach. Last year this figure was three times higher (60%). When financial losses did occur, they were under 1,000 euros for 11% of respondents, more than 1,000,000 euros for 16% and rather evenly distributed between 1,000 and 250,000 euros for a further 20%. The highest percentage of respondents however (32%) didn't know the value of lost assets. This includes 25% of C-level respondents, people one would expect to have such information, if available. Globally, this represents a slight increase on last year's figure of 27%.

Despite the increase in direct financial losses caused by breaches, respondents still confirm that what makes breaches the worst is the cost to investigate (favoured by more technical profiles) and fix, followed by reputational damage (favoured by C-level profiles) with 33% and 29% of responses respectively. These numbers are remarkably similar to last year's. What does change however is the level of business disruption reported, which plummeted this year from 27% to 5%. This notable drop may be the result of the previously reported trend of moving critical business functionality to the cloud where it's more sheltered.



What made this incident the worst of the year?

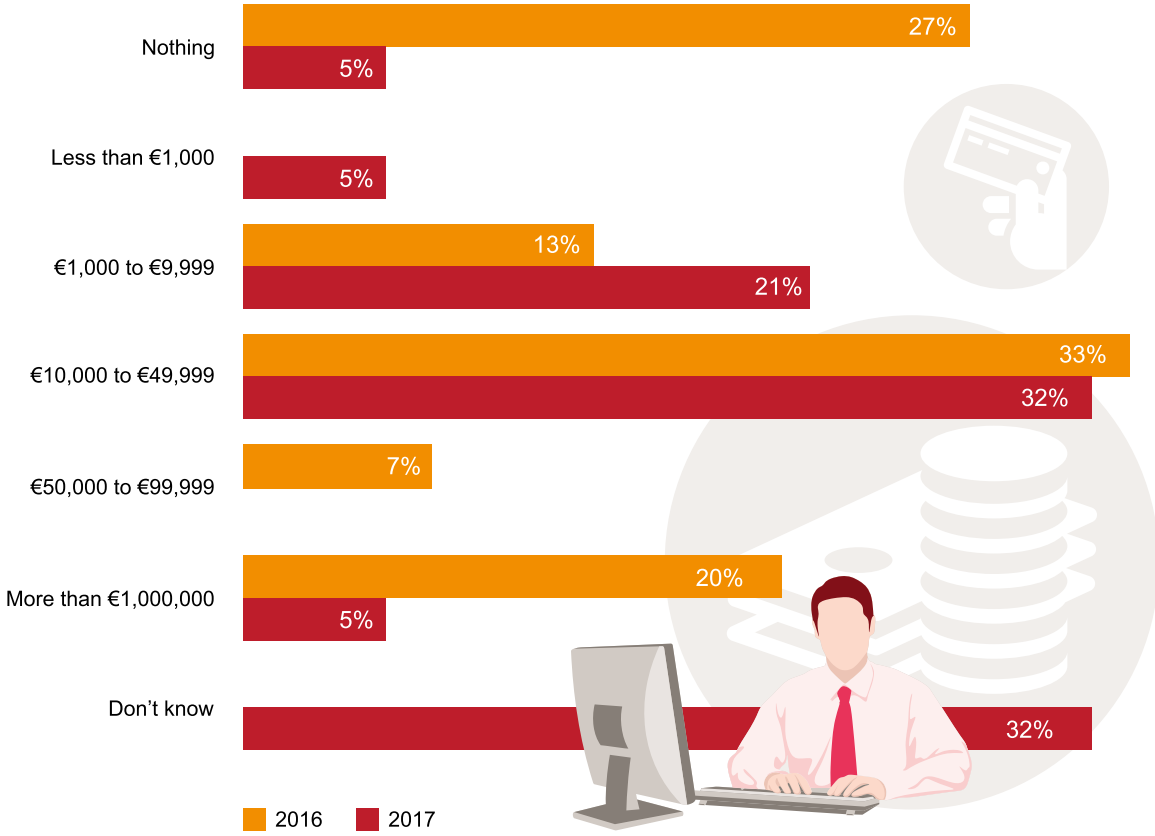


The cost of responding to breaches appears to be increasing.

Whereas last year fully half the organisations indicated having spent nothing in response to a breach, this year that figure dropped to 5%. Almost a third of organisations (32%) reported spending between 10,000 and 50,000 euros with 26% spending less than that and 5% more than 1,000,000 euros. Worryingly, almost one in three respondents could not quantify the amount spent responding to an incident. This implies that our observation last year remains relevant, the true cost of breaches is under-reported.

The emergent picture is one of a similar number of breaches this year to last, resulting in less business disruption to organisations, yet costing more to fix. This supports the informal observation that as business maturity increases, fixes reach increasingly deeper into an organisation's fabric, that of its partners and the interfaces that bind the two in business. The concern with both verifying and improving the security of supply chains and other strategic partnerships was explicitly highlighted in last year's Information Security Breaches Survey report.

How much money did you have to spend responding to the incident?



Handling

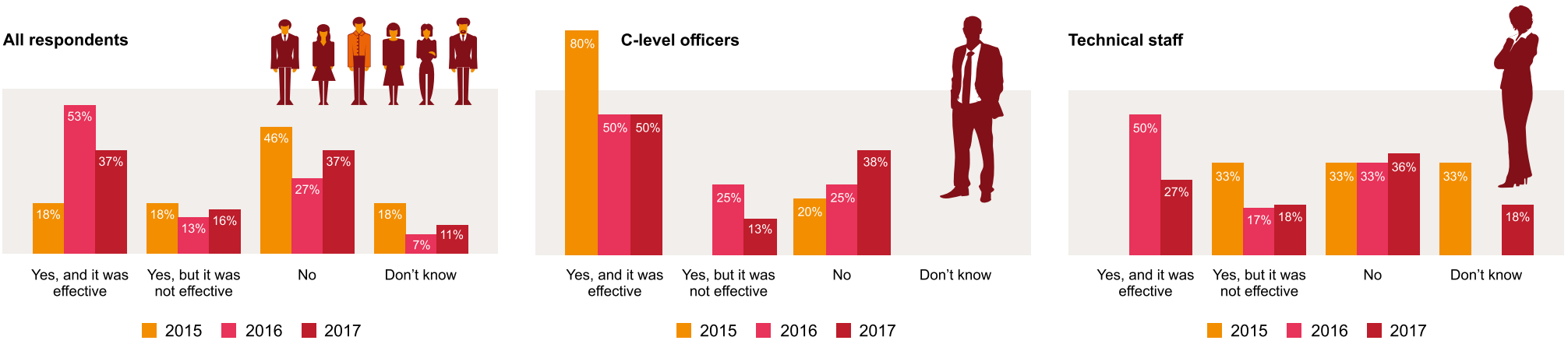
To effectively handle breaches, organisations must be prepared to enact their incident response plan. Almost a quarter (22%) of respondents report not having a formal incident response process, the same figure as last year. Of the remainder, more define their incident response team after the incident (38%) than do before it (30%), broadly similar trends to last year (then, 33% each) suggesting little evolution in incident handling. This stagnation may be related to the lack of formal evaluation of information security spending effectiveness.

Last year, we were pleased to note that the percentage of contingency plans deemed effective had risen sharply to 53% (from 18% in 2015). Unfortunately, that trend appears to have been short lived. This year, only 37% considered their contingency plan to be effective, though more C-level respondents thought so (half) than technical respondents (less than one third). Roughly one third (37%) of both C-level and technical respondents said that no contingency plan existed for the type of breach experienced. This suggests that organisations are not evaluating and updating their contingency plans quickly enough to keep pace with the rapid evolution in types of attack (ransomware) and may help explain the higher cost of breaches compared to last year.

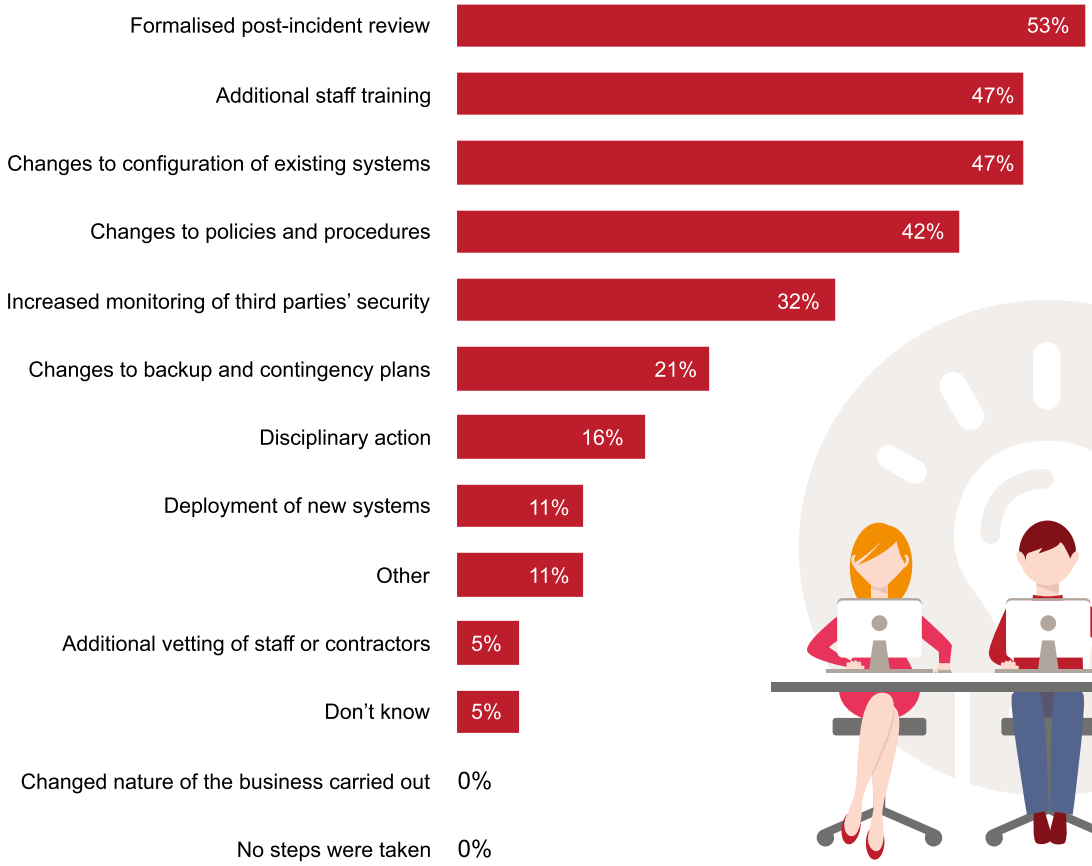
Like previous years, the vast majority of breaches (73%, the same as last year) were handled internally and not reported outside the organisation.

When asked hypothetically to whom breaches should be reported, C-level respondents tended to favour local police (66%) whereas more technical profiles opted for the Federal Computer Crime Unit (FCCU) (60%). Seventeen percent of respondents didn't know.

Was there a contingency plan in place to deal with this type of security incident?



Which of the following steps did you take to improve security following the incident?



Breach prevention

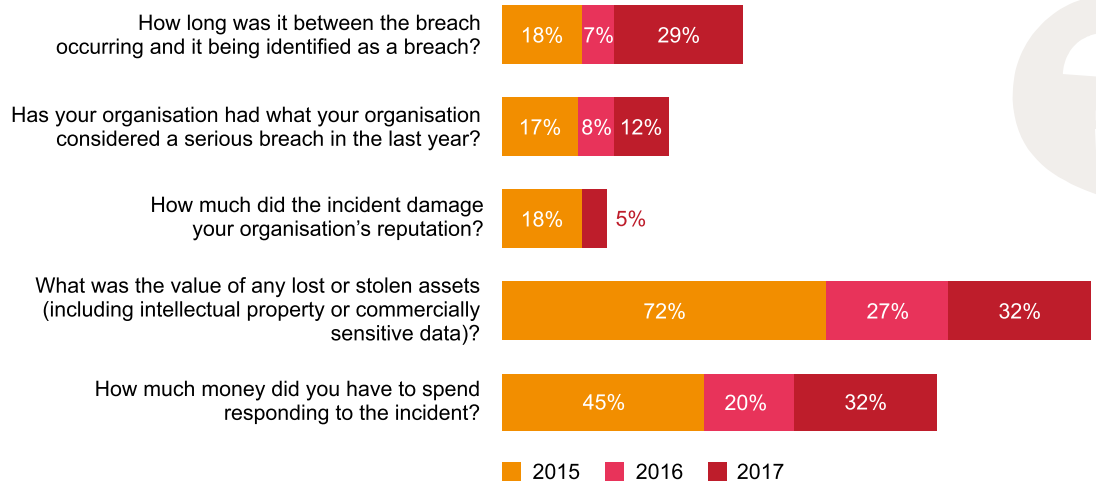
After a breach has been handled, most organisations turn their attention (for a period at least) to how best to mitigate future breaches with lessons learned from the current incident still fresh in the collective memory. With the exception of a large increase in formalised post-incident reviews this year (53%, doubling last year's 27%) and a large drop in additional vetting of staff or contractors (5% compared to 27% last year), preventative measures taken this year are largely similar to last year's. Configuration changes of existing systems were considered by 47% of respondents, changes to existing policies and procedures by 42% and, the perennial favourite, additional staff training by 47%.

The adoption of threat intelligence continues to grow by 10% annually, taking it to a total of 50% this year (it was 29% in 2015). While a few (10%) adoptions were the direct result of a breach, the majority were proactive measures. Seventy three percent of the population not currently investing in threat intelligence have plans for doing so, but interestingly, very few (8%) in the coming year. This is perhaps an acknowledgement of the security maturity baseline required to usefully leverage threat intelligence.

Not a single C-level reported being extremely confident that their organisation would be able to detect a sophisticated attack. Forty percent were somewhat confident. Globally, roughly 50% of survey participants were extremely or somewhat confident, while the other 50% were either ambivalent, not confident or not at all confident. While not particularly comforting, the numbers suggest that more organisations are opening their eyes to the reality and potential complexity of modern day attacks.

Trends

Collection of data: respondents answering "I don't know"



Biometrics

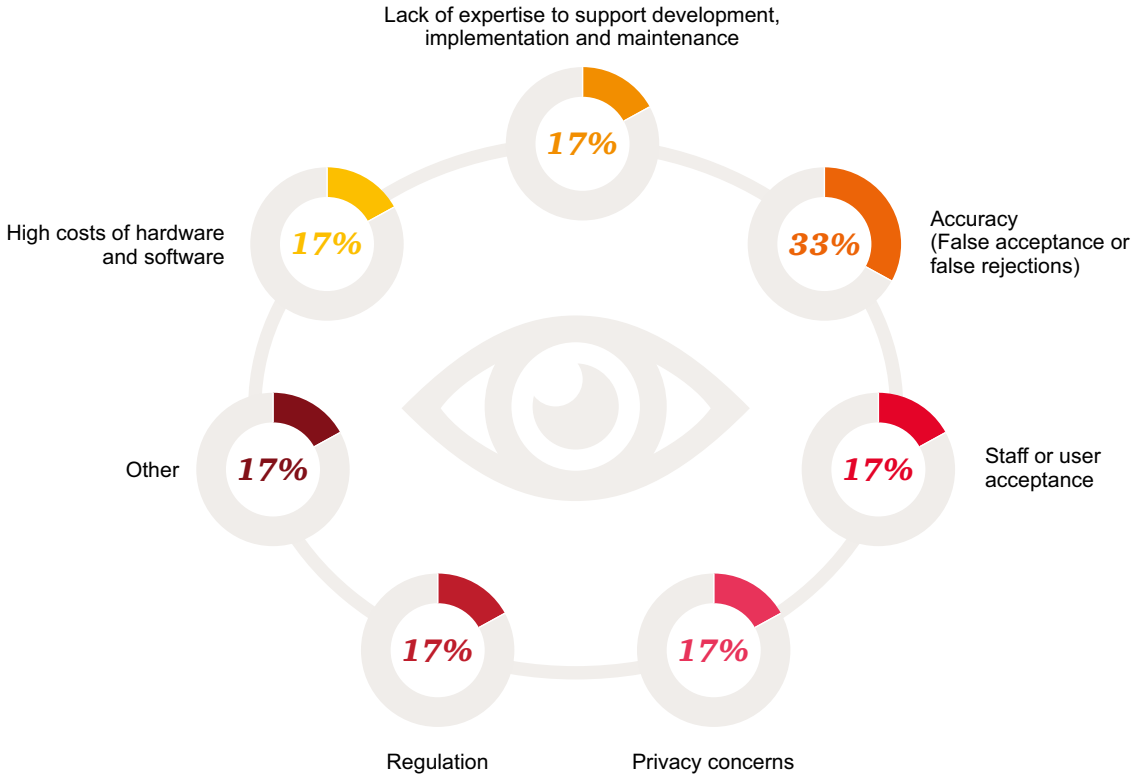
The biometrics portion of the survey was completed by just under 20% of participants. A third (36%) of which have already implemented a biometrics solution for authentication with the remainder planning on doing so. Interestingly, none of the respondents who indicated deploying biometrics reported using it throughout the organisation or even to protect all important assets. Rather, its single biggest use among almost a third of respondents (29%) is to guard access to critical assets. Other uses include access to buildings and infrastructure, or as a user-selected preferred authentication mechanism.

Users of biometrics systems are overwhelmingly employees (71% of cases), with users or customers representing 29% of the population. In all cases, traditional authentication mechanisms (something you know, something you have) remain the norm among 90% of surveyed organisations. There is currently little desire to use biometrics for other purposes besides authentication.

Results show a clear preference for fingerprint- or palm-based biometric solutions among participants currently planning on deploying biometrics (60%). Voice-based solutions are the least popular, garnering just 10% of responses. While we did not ask participants to justify their preference, it may be explained by balanced false acceptance to false rejection rate of fingerprints and palms, general availability of the technology and its relative acceptance among users. The more accurate, but perhaps less culturally accepted iris-based technology was investigated by 20% of respondents. The same number investigated behaviour-based solutions (typing pattern, gate, habitual locations, etc.) but 60% of respondents anticipated users would have some concern accepting it.

What motivated your organisation's interest in biometrics?

What have been the downsides to your organisation's adoption of a biometric solution?

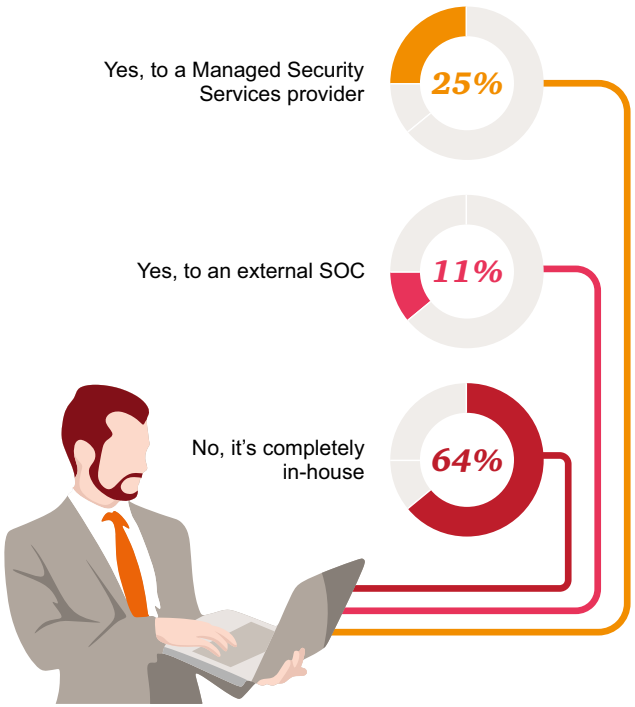


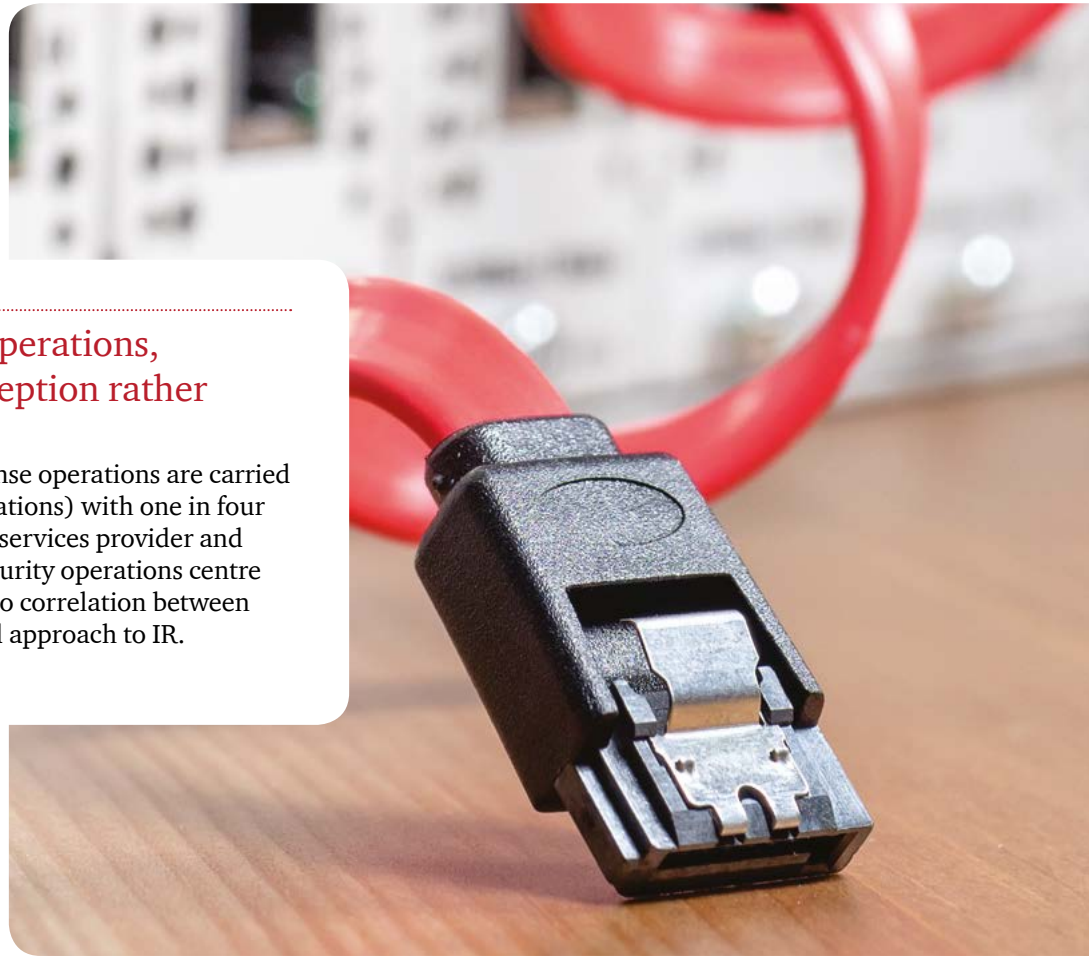
The most interesting observations we see involve issues perceived versus those experienced. There's a tendency to overestimate user acceptance of technologies and underestimate potential problems. When asked about their reasons for planning to adopt biometric solutions, ease of use was cited by most (70%), followed by efficiency (50%) and increased security (50%). Security and ease of use are generally considered to be opposing forces so it should come as no surprise that attempting to marry the two may be problematic.

Whereas no participants who trialled biometrics systems reported unfavourable results, this experience was not fully validated by current adopters. When asked about the downsides of biometric adoption, one third cited the accuracy of the systems (false acceptance or false rejection of users). The remainder of the responses were fairly evenly distributed among high hardware and software costs, user acceptance, lack of expertise to support the deployment and use, and regulation. No one complained about known security flaws in the systems. When asked what still hindered their adoption, half of those planning to adopt biometrics pointed to lack of expertise to support development, implementation and maintenance. This was followed by high costs and privacy concerns (40% each). The differences between the two groups highlight emergent issues when deploying biometrics at scale which limited trials may not uncover.

Incident Response (IR)

Does your organisation outsource any part of its IR operations?





When it comes to IR operations, outsourcing is the exception rather than the norm.

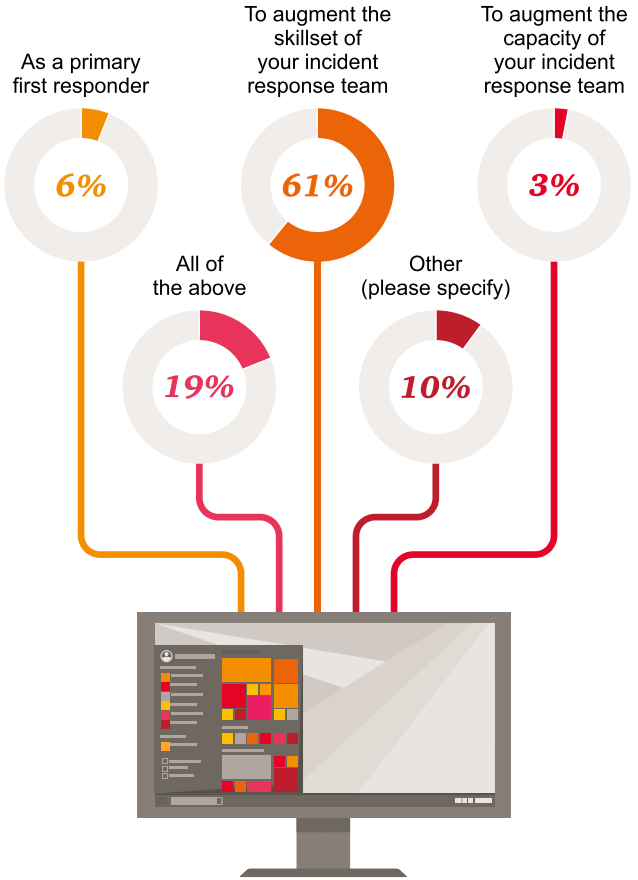
The majority of incident response operations are carried out internally (64% of organisations) with one in four relying on a managed security services provider and one in 10 using an external security operations centre (SOC). There appeared to be no correlation between size of organisation, sector and approach to IR.

When incidents do occur, just under half (48%) of respondents make use of third-party firms.

Most do so to temporarily augment the internal staff's skillset (61%), very few to increase the team's capacity (3%) or as primary first responders (6%). This suggests that internal security teams frequently operate without more advanced skills. Forensics and investigative firms are preferred by almost half of survey participants (45%) over audit, consulting or legal firms.

The vast majority (80%) of respondents make use of threat intelligence. Technical intelligence (such as indicators of specific malware) is most popular (75%), followed by operational intelligence detailing specific incoming attacks, used by just over half (53%). Responses suggest there's less of an appetite for tactical intelligence such as attacker methodologies, tools and tactics (29%) and higher level information on strategic shifts in risk (14%).

What best describes how this third-party service provider is utilised by your organisation?



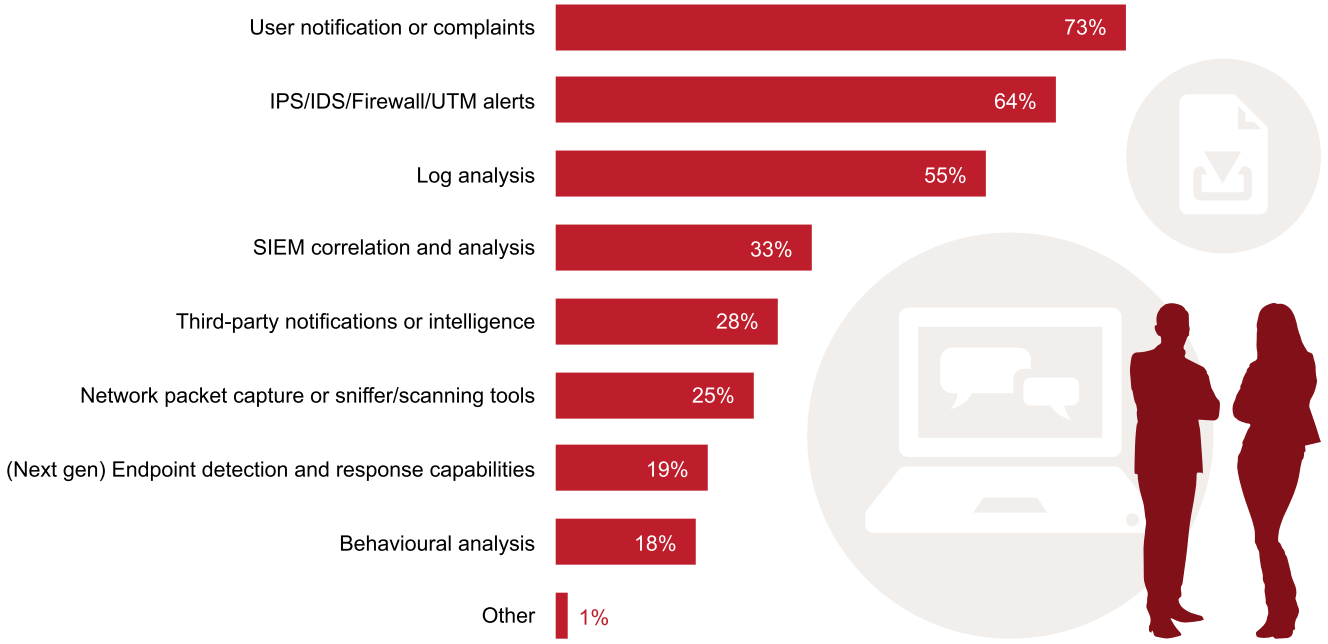
Despite the prevalence of threat intelligence and the increased spending on security tooling, when it comes to identifying compromised devices, user notifications or complaints are the most relied upon methods used by 73% of respondents. This human intrusion detection system is followed by more traditional alerts from firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), unified threat management (UTM) devices (64%) and log analysis (55%). Newer, more dynamic technologies have relatively low adoption rates, with less than one in five participants relying on endpoint detection capabilities or behavioural analysis.

The types of compromised devices analysed during breaches show that corporate-owned laptops and mobile devices, and internal network devices and systems are far more targeted (around 86% each) than employee-owned laptops and mobile devices (BYOD). The latter account for around 27% of assets investigated, a non-negligible number nevertheless, suggesting that BYOD adoption and abuse are both alive and well.

Three quarters of investigated breaches were financially motivated. Most were caused by social engineering or phishing (55%) regular malware (49%) and human error (45%).

Physical theft or loss represent a healthy 30% of breaches highlighting the importance of physical security and basic data protection technologies such as drive encryption.

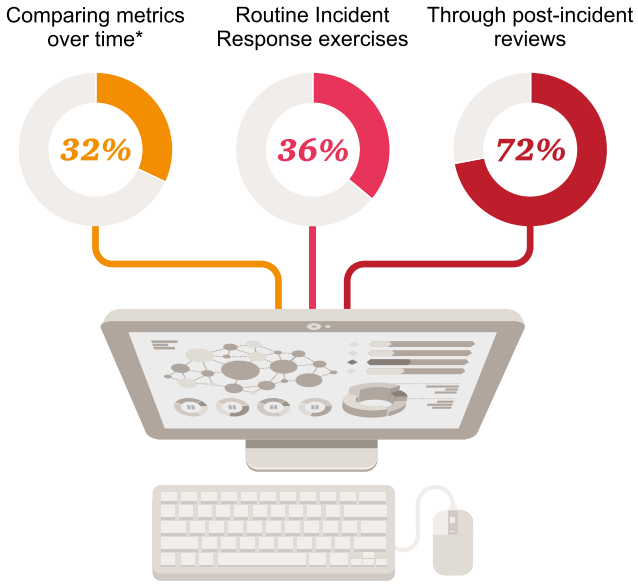
Which of the following do you use to identify compromised devices?



In general, organisations are not proactively evaluating and improving their IR procedures.

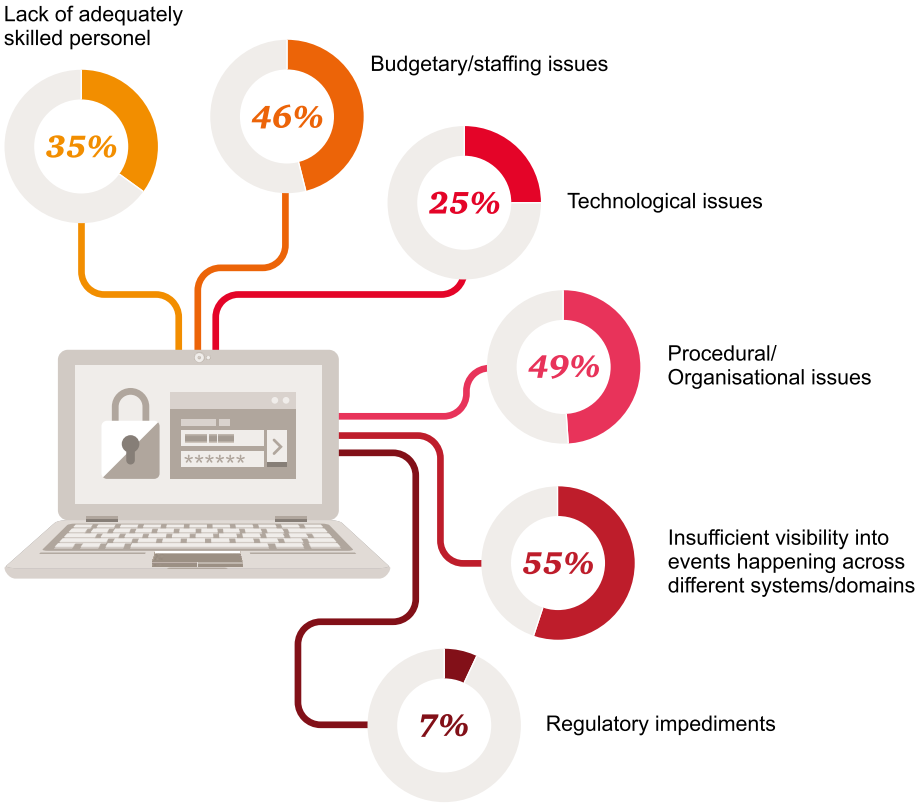
Only half the organisations surveyed carry out any form of evaluation, and the majority of those (72%) only in the wake of a breach. Those proactively evaluating their procedures do so roughly equally by gathering and comparing metrics over time (such as the speed of detecting breaches, of remediating them, root cause analysis, etc.) and through routine incident response exercises (roughly a third of proactive respondents each).

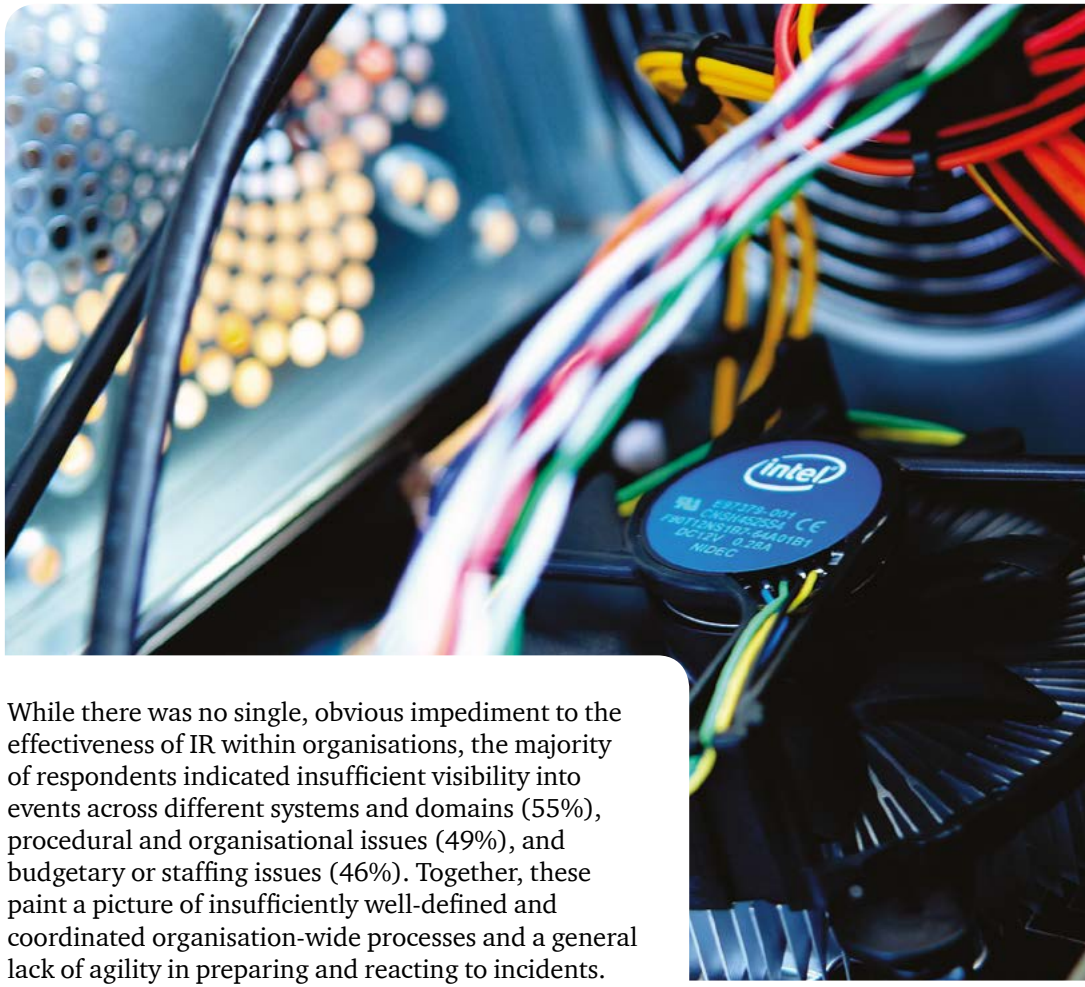
How do you assess the effectiveness and maturity of your IR processes?



** speed of breach detection, remediation, root cause analysis, etc.*

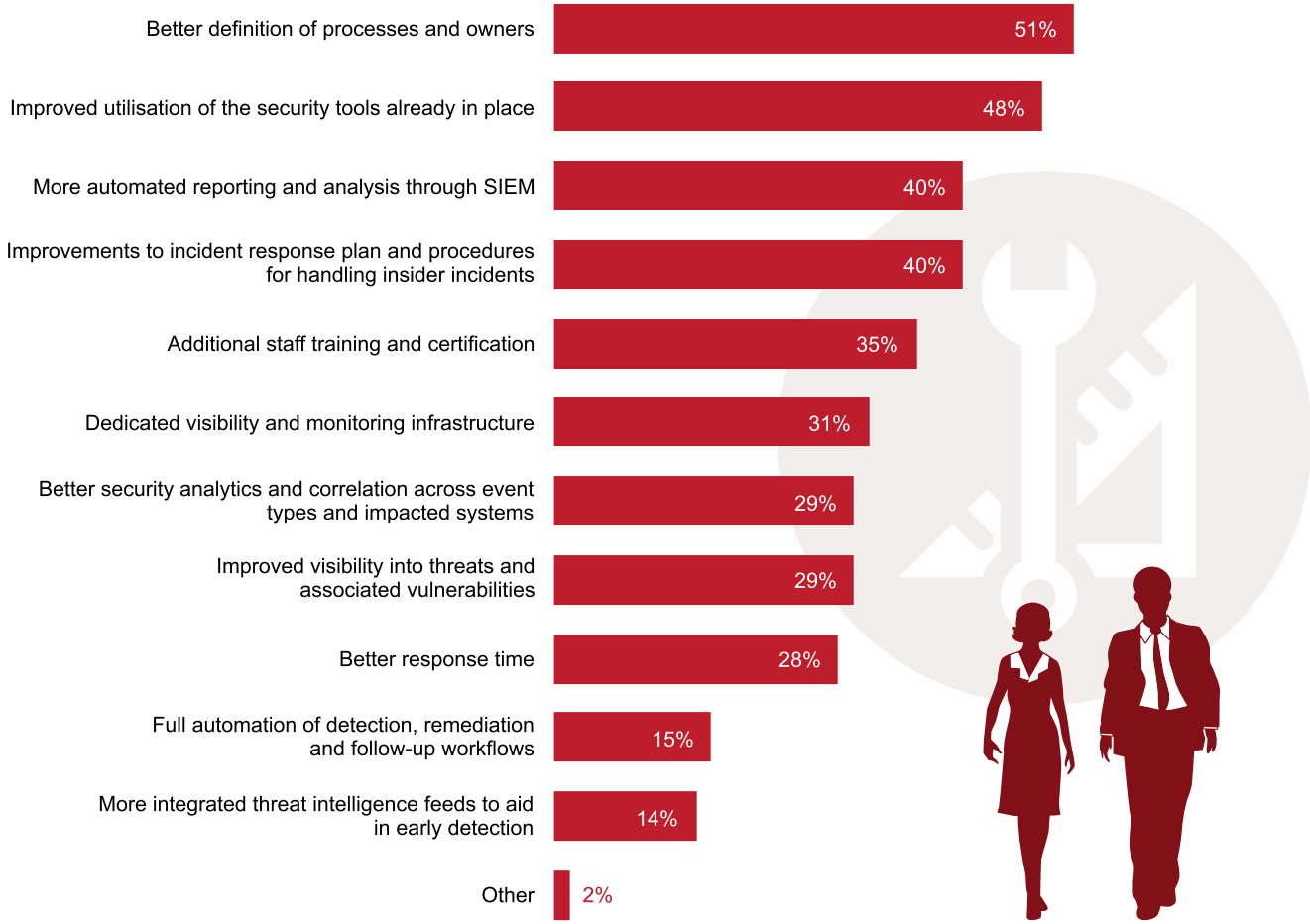
Which issues do you think impede the effectiveness of IR within your organisation?





While there was no single, obvious impediment to the effectiveness of IR within organisations, the majority of respondents indicated insufficient visibility into events across different systems and domains (55%), procedural and organisational issues (49%), and budgetary or staffing issues (46%). Together, these paint a picture of insufficiently well-defined and coordinated organisation-wide processes and a general lack of agility in preparing and reacting to incidents.

Which improvements to your IR capability are you planning on making in the near future?



Unsurprisingly, the near-future IR capability improvement plans are equally diverse, suggesting the process of streamlining organisations' IR will likely be incremental over a period of time.

The largest number of respondents indicated plans to better define processes and owners (51%), followed by improved utilisation of security tools already in place (48%). The least popular planned improvement was more integration of threat intelligence feeds to aid early detection (14%). Combined with the fact that only 24% of respondents use knowledge gained from incidents to feed their security information and event management (SIEM) system with fresh indicators of compromise, this suggests that organisations tend to use feed services as-provided rather than customise them or create their own.

Conclusions

Survey results over the past few years suggest that senior management understand the importance of security and are no longer blamed for not prioritising it. Despite this positive evolution, both the number and severity of reported breaches remain stubbornly constant with little to suggest a turning tide.

Security consulting firms (including PwC) know from their experience in carrying out phishing and social engineering campaigns at customers how successful they are. It only takes one naïve user for an attacker to gain an initial foothold into the corporate network. In the majority of cases, lack of adequate network segmentation, poor visibility and correlation across domains, compounded by weak endpoint and network security and monitoring allow attackers to cause untold harm.

The average user is crucial to the success of these attacks. Organisations must find innovative and effective ways to go beyond security awareness, training and education. They must seek to better understand human motivation and cognitive bias, and situate them within their current culture to adequately address the important, hidden aspects of culture. Assumptions, norms, values and beliefs are all key components of a solid organisational security culture, which shapes how employees behave instinctively, even when no one is looking.

The ability to more predictably shape shared employee judgements, decisions and behaviours at key security moments will greatly strengthen an organisation's human firewall. By itself however, it's still unlikely to fully stem the tide of damaging phishing and social engineering attacks, which are becoming ever harder to detect as they grow in sophistication.

The dual approach of complementing a sound security culture with good visibility into events across systems and domains, and the ability to correlate these across an organisation is key. In a first step, honest, regular evaluations of current processes, methodologies and skillsets will reveal gaps which organisations can meaningfully address. For these, finely-tuned tools, strategically deployed and operated by skilled users who are supported by well-defined and rehearsed procedures will yield a higher return on their investment than blindly stockpiling the latest shiny toys in the misguided hope that one will reveal itself to be the proverbial silver bullet.

However, as breaches become stealthier and the volumes of data in which they can hide multiply, the difficulty of correctly determining whether a particular event or artefact across an organisation is indicative of an attempted or successful security breach can be expected to increase. The sensitivity and reaction times of security teams, continuously faced with a deluge of data supporting events may simply prove inadequate, no matter how well-tuned current tools and procedures are. There is hope that technologies underpinning such trail-blazing tools as Siri, Cortana and Alexa will evolve towards real-time security assistance for end users, based on run-time observations and analysis of their environment, and, crucially, delivered in a form understandable to them.

How we can help

PwC can help you understand the implications of today's security landscape and guide you in adopting a forward-thinking approach by applying new concepts to the unique needs of your business, your industry and your threat environment. Let us show you how to effectively combat the security threats of today and plan for those of tomorrow.

Contacts

Ivo Meertens
Infosecurity Belgium
ivo.meertens@jaarbeurs.nl

Filip De Wolf
PwC Belgium
filip.de.wolf@be.pwc.com

Floris Ampe
PwC Belgium
floris.ampe@be.pwc.com

Marc Sel
PwC Belgium
marc.sel@be.pwc.com

Peter Versmissen
PwC Belgium
peter.versmissen@be.pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.