The state of enterprise security: Safeguarding your organisation

Concerns about the cloud are driving security investment, while GDPR is spurring businesses to adopt better practices.

Cybersecurity is now one of the biggest existential issues facing organisations of all sizes the world over. Threat actors are becoming increasingly numerous and sophisticated, breaches are now daily headlines and new data protection regulations such as GDPR have pushed the cost of failure ever upwards.

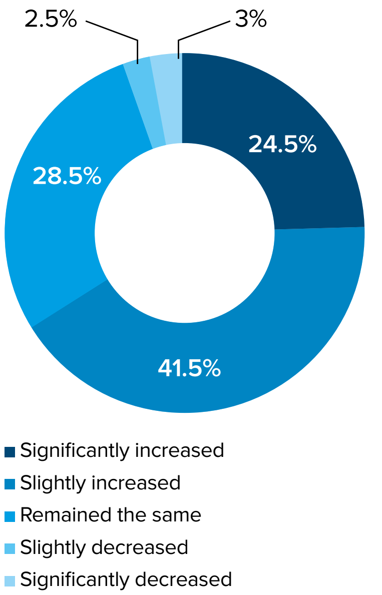
Digital transformation has changed the way businesses operate and security teams are now being tasked with protecting information that sprawls numerous clouds and devices, while new technologies present continually evolving opportunities and challenges. At the same time, security professionals are tasked with balancing the day-to-day around keeping the business secure – whether that's patching, managing incidents or educating staff around security – with trying to aid the goals of the business and promote the role of the Chief Security Officer or Chief Information Security Officer.

While this might be daunting, never before has cybersecurity been so prominent a topic within the business landscape. Good security can be a competitive advantage, a business enabler and a cost-saver if done correctly, presenting opportunities for companies who are willing to seize it.

IDG UK's state of enterprise security survey, fielded between April and June 2019, gathers the responses of some 200 IT leaders from major UK enterprises and analyses how senior IT professionals are safeguarding their organisations; from preventing cyberattacks to creating a cybersecurity culture.

66% of organisations in the study said their cybersecurity budgets have increased compared to the year before

Has your cybersecurity budget increased, decreased or stayed the same this fiscal year?



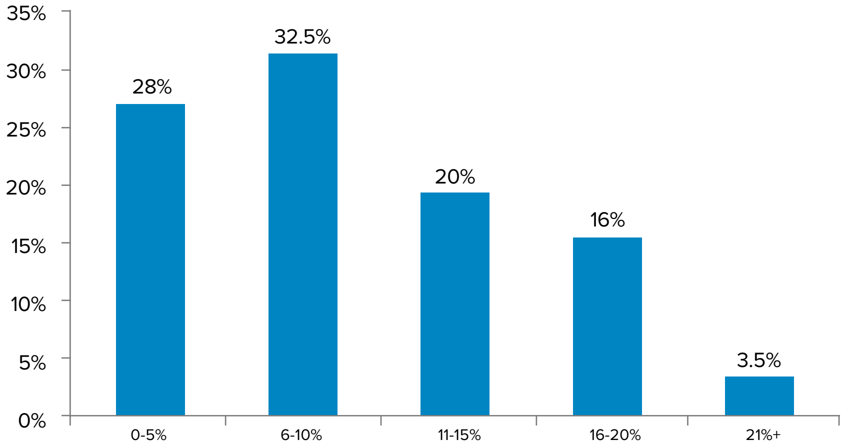
Security budgets increase in the face of ever-more threats

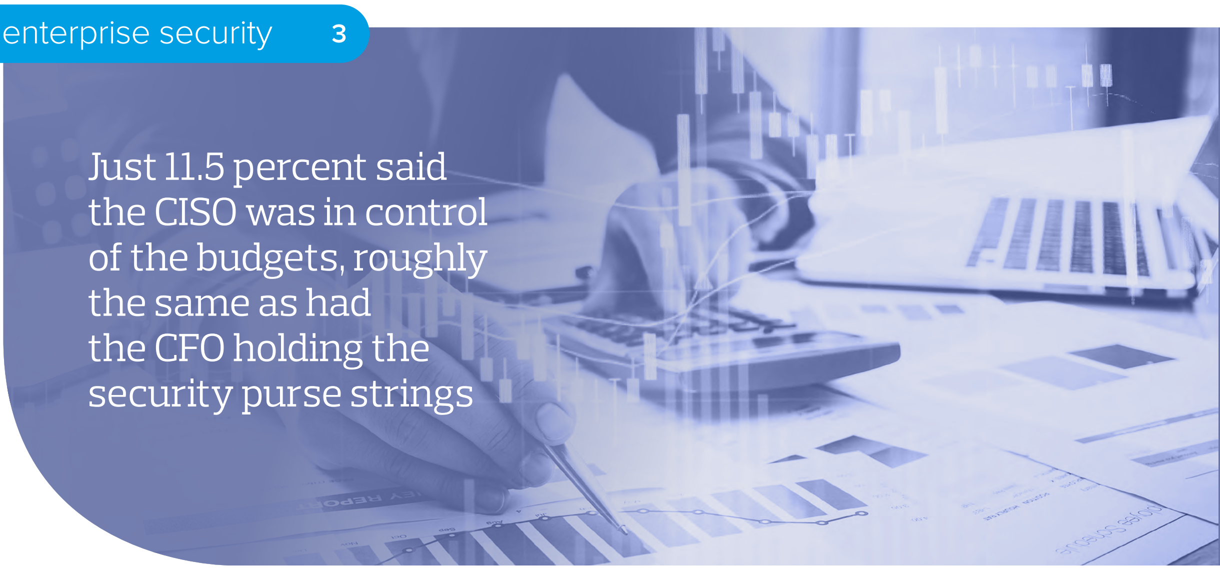
Given the regular headlines around the latest breaches and vulnerabilities, combined with the massive amount of press around GDPR, cybersecurity has never had more prominence as a topic within businesses. As a result, spending within the area is being pushed continually upwards as companies spend more money trying to defend their organisation from losing data, and eventually losing even more money through loss of business and fines.

Some 66 percent of organisations in the study said that their cybersecurity budgets have increased compared to the year before, with just under a quarter saying this increase had been 'significant'. A little under 29 percent of respondents said their budget had remained the same, while 5.5 percent of companies had seen their cybersecurity budget decrease compared to the year before.

Though security budgets are on the increase, for most companies it still makes up only a small slice of overall IT spending. Approximately 28 percent of organisations surveyed spend less than 5 percent of the IT budget on cybersecurity-related technology and activities. Just under a third of companies said they dedicated 6-10 percent of their IT budget to cybersecurity, while 36 percent revealed they designated 11-20 percent of their IT pot to security. Only 3.5 percent of companies dedicate more than a fifth of their overall IT budget towards the security function. While a higher security-to-IT ratio may indicate how seriously a company takes its cyber-related risk, budgets are relative and unique to each organisation, and do not necessarily reflect effectivity.

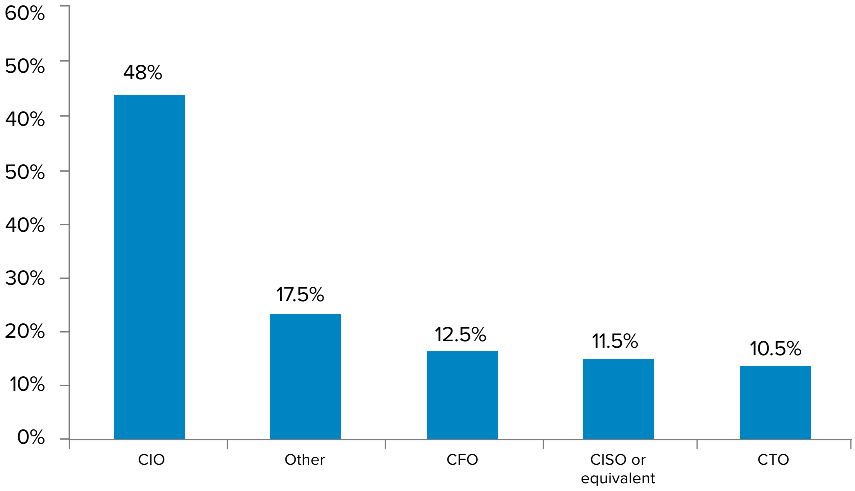
How much of the IT budget is designated to cybersecurity?





Just 11.5 percent said the CISO was in control of the budgets, roughly the same as had the CFO holding the security purse strings

Who controls the cybersecurity budget within your organisation?



CIOs still hold the power and purse strings

Despite the majority of companies now having a CISO, the role is still largely second to the CIO in the organisational chain of command.

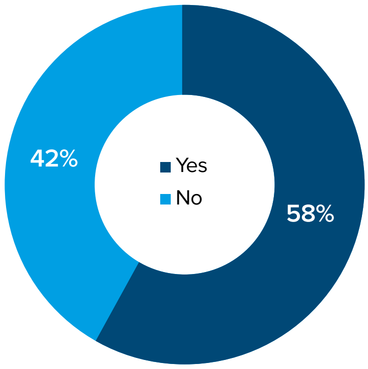
Approximately 58 percent of organisations said they have a CISO or equivalent. Yet despite this only 29 percent of companies said the CSO was primarily responsible for cybersecurity within their business. The CIO or CTO was more likely to be primarily responsible, and at the same time over half (58 percent) of companies said the CSO reported into the CIO or CTO, with around a quarter of CISOs reporting into the board.

Of companies that don't currently have a CSO or equivalent, 55 percent said they have no need to hire one, while a third were exploring the option.

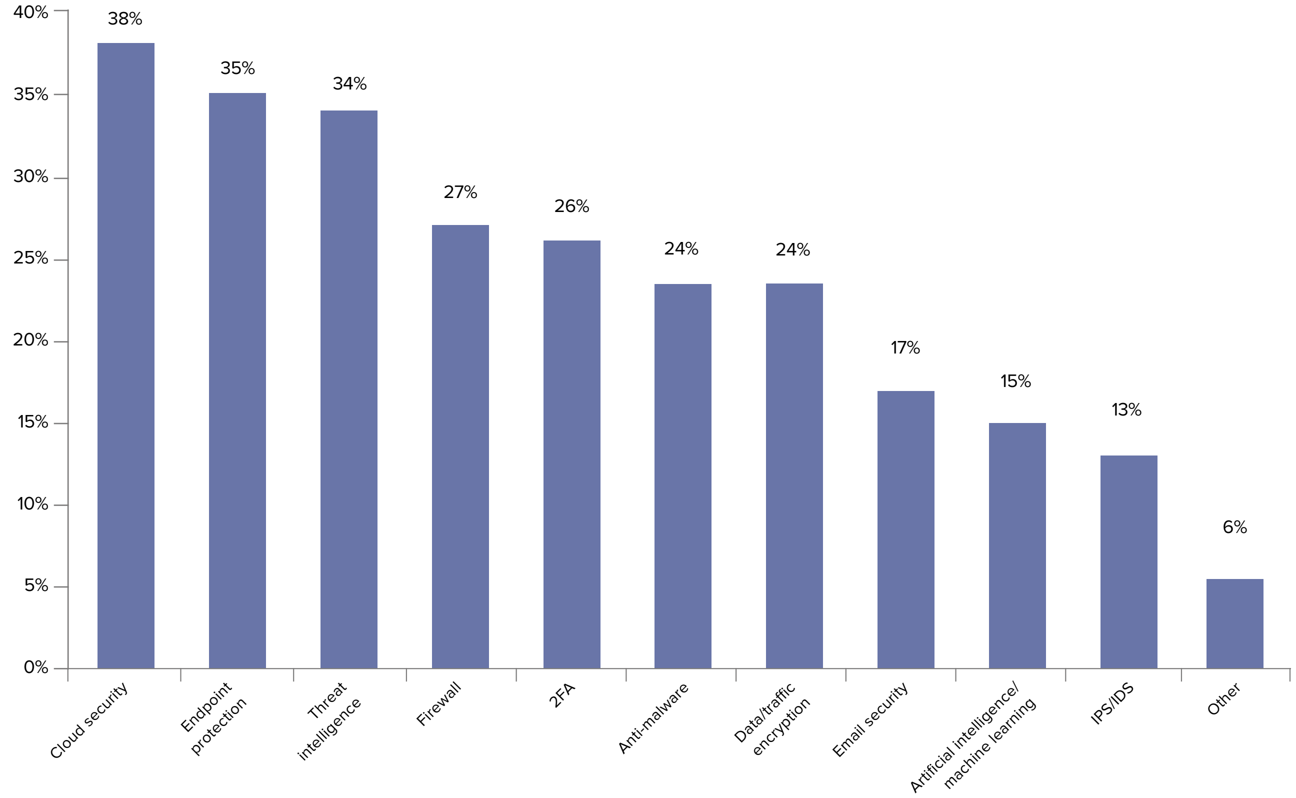
Over half (59.5 percent) of companies said the CIO or CTO controls the cybersecurity budget within the organisation. Just 11.5 percent said the CISO was in control of the budgets, roughly the same as had the CFO holding the security purse strings.

In *CIO UK*'s 2019 CIO 100, only 12 percent of CIOs said that the CISO is a peer within their organisation. However, as the role matures – and executives see more value in security, rather than merely a cost centre or compliance requirement – the prominence and standing of the CSO is likely to elevate.

Does your organisation have a CISO or equivalent?



What cybersecurity technologies are you looking to invest in?



40%

say that cybersecurity concerns have stopped their company from moving specific IT applications into the public cloud

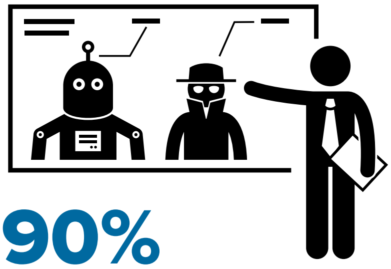
Cloud concerns driving security spending

While the value and benefits of cloud computing are well understood – being a 'cloud-first' or 'cloud-native' company is now the de facto position for many organisations – the security aspects of such technologies are often underappreciated. Major enterprises, notable start-ups and even intelligence agencies have been guilty of leaving sensitive information openly exposed on the Internet via insecure cloud instances.

Over 40 percent of companies surveyed agreed with the statement that cybersecurity concerns have blocked specific IT applications being moved into the public cloud. As such, it's little surprise that 'cloud security' was the top security technology that organisations were looking to invest in this year. And given that access to cloud environments is such an integral part of cloud security, it's also not surprising to see that two-factor authentication (2FA) was also in the top five, with just over a quarter of companies looking to invest in the technology.

Beyond cloud concerns, there are an array of day-to-day threats that organisations must deal with. Phishing emails are often the primary delivery mechanism for a number of attacks, including ransomware and a wide variety of malware variants, and act as the entry point for business email compromise (BEC) scams. It was no surprise then that phishing/social engineering was listed as the main threat that organisations were worried about. Ransomware, malware and BEC attacks were also listed as major concerns for around half of companies.

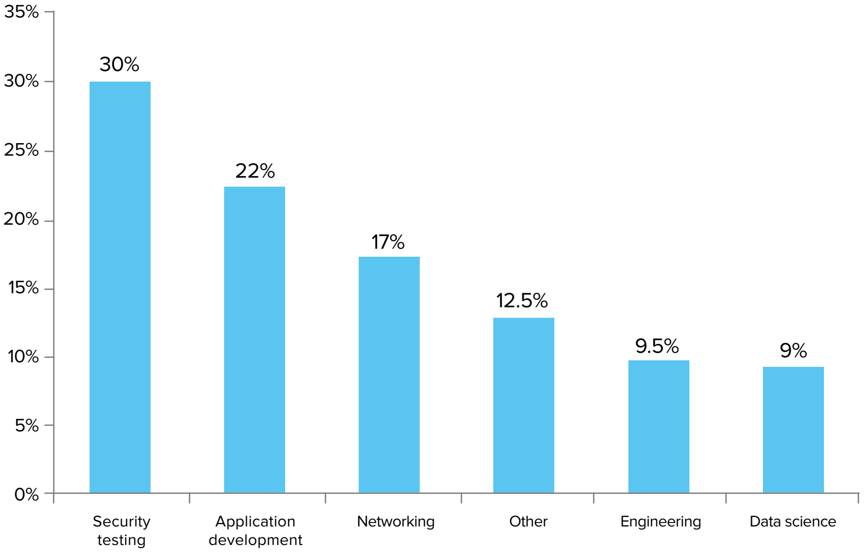
The high concern around email-based attacks, as well as ransomware and malware, tallies with endpoint protection, firewalls, anti-malware and email security technologies all being among the top 10 main security investment areas. Threat intelligence – which provides organisations with a variety of intel that can help them identify, prevent and remediate all types of attacks – was also a major source of investment.



90%

believe that artificial intelligence/ machine learning is important in the future when it comes to emerging threats and how to combat them

Where do you see the biggest cybersecurity skills gaps within your organisation?



Will automation fill the talent shortages and skills gaps?

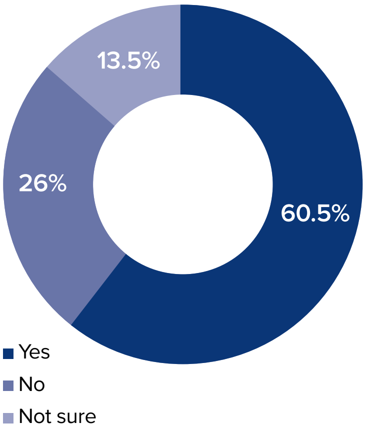
Unemployment in the cybersecurity industry is rarely above zero percent. Talent shortages in the industry are estimated to number in the millions globally and in the hundreds of thousands across EMEA. In a seller's market, in-demand cybersecurity professionals can essentially pick and choose the roles they want from the employers of their choice.

This high-demand, low-supply market means organisations are left trying to fill the void where they can. Some 60.5 percent of respondents admitted that they were suffering skills gaps within their cybersecurity functions. Just under a third said they were suffering skills gaps around security testing, 22 percent said application development was short, while 17 percent said they had skills gaps within their network security function.

Given the talent shortage and the slow pace at which new blood can enter the market, many within the cybersecurity industry are claiming automation can help fill the shortfall. Machine learning is already being applied to almost every area of the security stack in order to do more with the massive amounts of data being collected in a way that – in theory at least – reduces the workload on understaffed and overworked security teams.

And while it can often be easy to dismiss buzzwords in the security industry, organisations seem sure that automation in its various forms will be key to future operations. A massive 90 percent of respondents agreed that artificial intelligence/ machine learning will be important when combating threats in the future, with 40 percent claiming it would be 'very important'. Approximately 15 percent of companies said they were planning on investing in the technology over the coming year.

Does your organisation have a skills gap within cybersecurity functions?

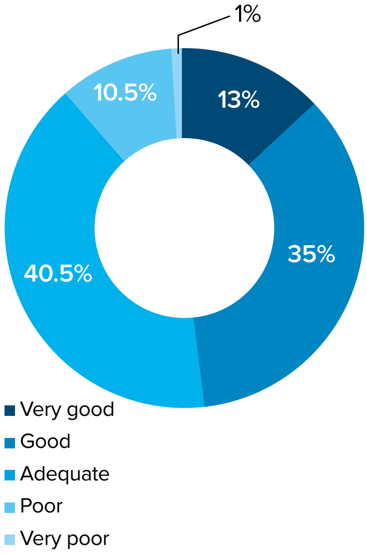


People still a security problem for CIOs and CISOs

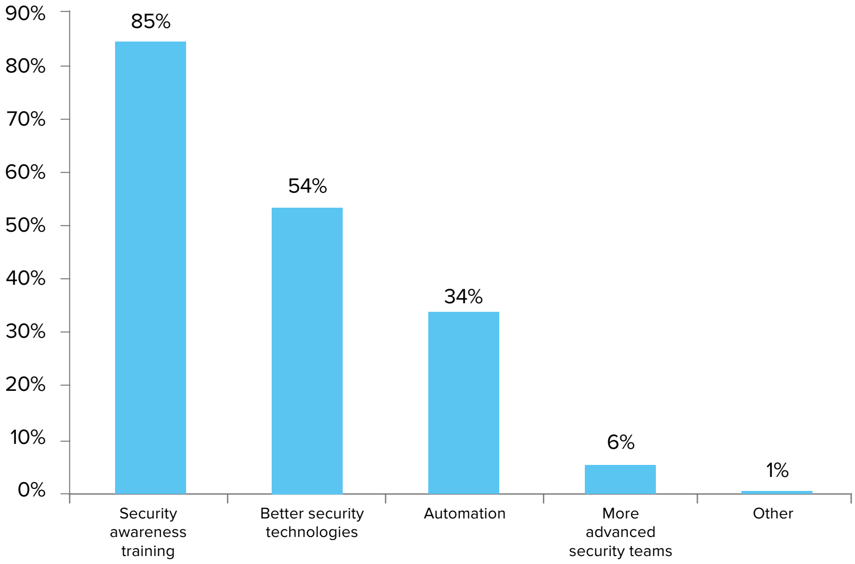
Try as they might, security controls are still often undone by the one thing companies can't control; their employees. All the monitoring and controls in the world won't be able to stop an employee determined – whether through malice, frustration with processes or ignorance – to flout proper procedure.

This is clearly well-understood by organisations; 98 percent agreed with the statement that humans are the weakest link when it comes to cybersecurity. At the same time, 30 percent cited insider threats as a security concern.

How would you rate cybersecurity awareness within your organisation?



How is your organisation looking to reduce human error?

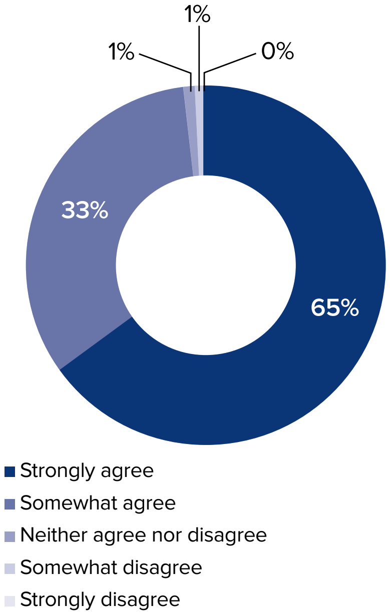


The best way to prevent human error is to educate users and instill a security-minded culture within the organisation. On this front, there is clearly still work to be done; 40.5 percent of those surveyed said cybersecurity awareness was merely 'adequate', 35 percent said awareness was 'good' and a further 13 percent claimed awareness was 'very good'. Approximately 11.5 percent said awareness was 'poor' or 'very poor'.

While around half of companies are looking to technology-based solutions in order to help reduce human error, 85 percent said they were running security awareness training, showing that organisations understand that technology alone is not the answer.

If security is going to be viewed as a business enabler, and not a bottleneck or fearmonger within the business, it needs to instill a cybersecurity-minded culture within the entire organisation. Employees not only need to be aware of potential threats in the context of their own job and the consequences to the business, but they need to feel assured that if they ever do make a mistake they will not be reprimanded for it, as fear may lead to attempts to hide issues.

To what extent do you agree with the following statement: The human employee is the weakest link when it comes to cybersecurity



Prevention is hard, value comes from reducing breach costs

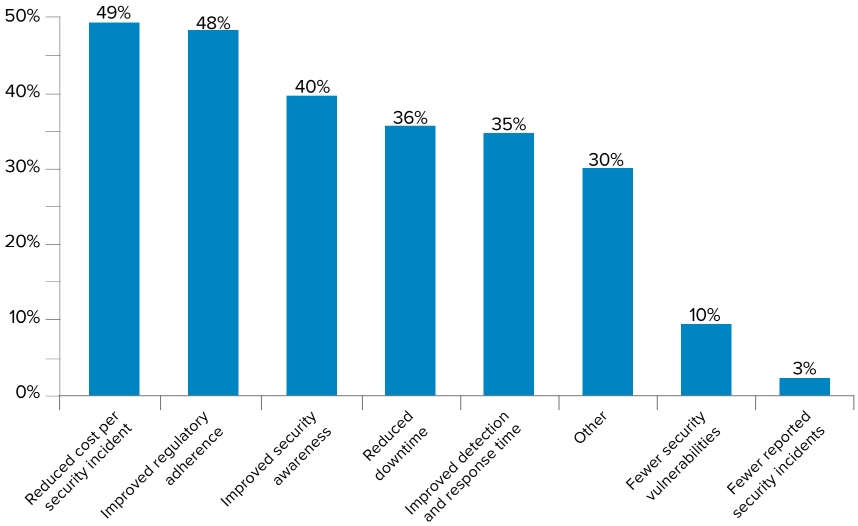
Measuring the value of security technology can be notoriously difficult and the cost of a security incident can vary wildly depending on numerous variables. It can be hard to pinpoint exactly what attacks were stopped by which technologies and whether they would have been stopped by another technology at a different point, and determine what is the best way to measure the return on investment of a product when its job is to keep business operations running normally.

According to those surveyed, it seems the response to an incident is more important than prevention when it comes to value. It has become something of a mantra within the security industry that it is a case of 'when, not if' an organisation is faced with a data breach, and over 61 percent of respondents in the survey agreed with the idea that it is inevitable. And as a result, the value of security products should be measured in terms of keeping incident costs – and subsequent punishment from regulators – to a minimum.

'Reduced cost per security incident' and 'improved regulatory adherence' were the two key metrics organisations used to measure the return on investment (ROI) and value to the business of cybersecurity products, cited by just under half of organisations.

Fewer than three quarters (67 percent) of respondents said that senior management understood the cybersecurity challenges facing their organisation

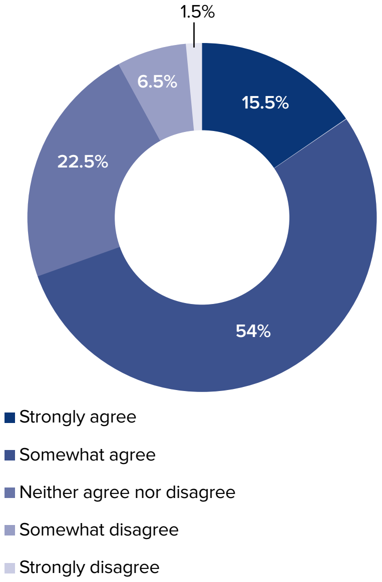
What are the key return on investment (ROI) metrics that show cybersecurity technology is delivering true value to the business?



Improved security awareness, reducing downtime, and improved incident detection and response times were the next most important metrics for organisations, all of which have measurable value to the wider business and not just to the security department.

Despite often being the overall objective of many security technologies, fewer vulnerabilities or reported incidents were only key metrics for 10 and 3 percent of companies respectively.

To what extent do you agree with the following statement: GDPR has improved my organisation's cybersecurity maturity



GDPR; failure is costly, but has wider benefits for security

While boards and management have now become attuned to the importance of digital transformation, security is still often something of a foreign language to those outside of the technology function. Executives and security professionals can often have conflicting goals – getting products to market faster and cheaper versus making sure those products are secure is a classic example – and explaining risk in business terms can often be a challenge.

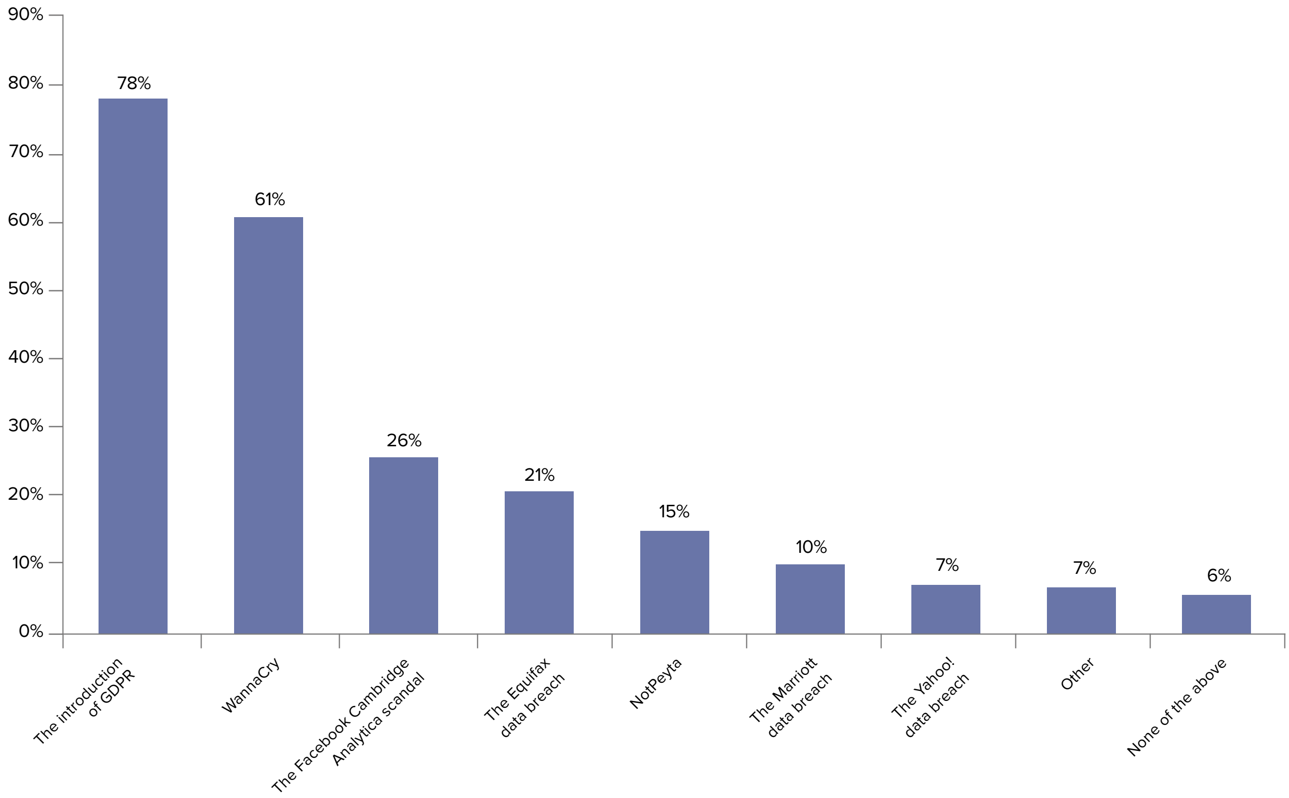
Fewer than three quarters (67 percent) of respondents said management understands the cybersecurity challenges facing the company, but only 10 percent of those said it understands them 'very well'. A third of those surveyed said management does not understand the organisation's risk very well, and another 4 percent said 'not well at all'.

However, understanding around security – and the standing of the security function as a result – has increased in recent years. GDPR – the sweeping data protection and privacy legislation coming out of the European Union – sent waves across the business world, and gave the security function a new impetus and far greater standing within organisational hierarchies than before.

Almost 80 percent of companies said the introduction of GDPR improved cybersecurity understanding at the boardroom the most over the past two years, with 69.5 percent also agreeing that the regulations had improved their organisation's cybersecurity maturity.

With the UK's Information Commissioner's Office (ICO) recently fining British Airways £183 million and the Marriott hotel chain £99 million for GDPR failures, combined with a growing number of copycat data protection laws being passed around the world, regulatory compliance and a fear of fines will likely allow CISOs and other security professionals to lead from the front and drive a security-first agenda for years to come.

Which of the following incidents have improved cybersecurity understanding at the boardroom the most over the past two years?



Old challenges remain, new ones appear, and opportunities present themselves

Despite most organisations now having a CISO or equivalent and more investment than ever, security professionals are still pessimistic and feel they are all waiting for an inevitable data breach. Talent shortages remain commonplace across a range of skills, and teams feel awareness of the importance of security still has some way to go.

The fact that social engineering, phishing, business email compromise and insider threats all top the list of threats organisations are most worried about shows there needs to be more focus on the 'human' side of security. Organisations need to double down efforts around security education and awareness in order to create security-first mindset among all staff, not just the security or IT teams.

Investment, while pivoting to new issues such as cloud security, automation and machine learning, is still largely focused on old staples such as endpoint protection, firewalls, encryption and email, highlighting the fact that cybersecurity professionals can take nothing for granted.

And yet while businesses may often lament regulations and the burden of achieving compliance, the survey suggests that not only has GDPR done more than any one single incident to raise awareness of security among company leadership, but is also a major driver for increasing cybersecurity maturity.

Among these challenges is an opportunity for CISOs and other cybersecurity professionals to step up and become business leaders. By showing that security can be a business enabler and can help be a competitive advantage rather than merely a cost centre or bottleneck, CISOs – in collaboration with CIOs – can elevate the issue of security to even more prominence within the business.