Global Advanced Threat **Landscape Survey**

2016

CYBERARK®

Table of Contents

Executive Summary

The 10th annual CyberArk Global Advanced Threat Landscape Survey 2016, themed "Cyber Security: Past, Present & Future," examines whether global enterprises are learning and applying lessons as a result of years of highly publicized cyber attacks, and how security priorities and decision making are being impacted.

The report juxtaposes rising confidence in cyber security strategies and leadership, with poor IT security habits that persist across the enterprise in critical areas such as privileged account security, third-party vendor access and cloud.

The report is the result of surveys conducted with 750 IT and IT security decision makers from around the world including C-level executives, directors and department heads among enterprise organizations. Respondents represent a range of public and private organizations across multiple vertical industries from the United States, Europe (France, Germany, United Kingdom), Israel and Asia Pacific (Australia, New Zealand, Singapore).

Following are key highlights from the report.

Let History Be Your Guide? Security Awareness on the Rise, but Bad Habits Persist

Despite increased cyber security awareness, nearly every IT security breach or cyber attack continues to be underpinned by the failure of organizations to enforce best practices or adequately protect against advanced threats.

Since the last report, cyber attacks have continued across critical industries including attacks on the global banking system that exploited known vulnerabilities in IT infrastructure, a ransomware epidemic that impacted leading healthcare organizations such as Hollywood Presbyterian Medical Center, critical infrastructure attacks that demonstrated the ability to cause a power outage (Ukraine), and data breaches of consumer and government organizations (U.S. Internal Revenue Service, U.S. Democratic National Committee and toy manufacturer VTech), as well as the Panama Papers breach.

As a result of these and other high profile attacks, many global organizations are taking positive steps toward better protecting against the damaging effects of a cyber attack, including implementing measurable security programs to benchmark progress. However, there is still a gap between "awareness" and "preparedness" in protecting against attacks. Consider these points:

- 79% of respondents say their organization has learned lessons from major publicized security breaches and taken appropriate actions to improve security.
  - Malware detection (25%), endpoint security (24%) and security analytics (16%) are ranked first among the changes implemented as a result of increased security awareness.
- 55% of respondents state they have changed or evolved processes for managing privileged accounts. However, these changes do not always equate to best practices.
  - Surprisingly, 40% still store privileged and/or admin passwords in a Word document or spreadsheet on a company PC/laptop, and 28% use a shared server or USB stick.
  - 35% are planning to implement new measures for managing privileged accounts, but have yet to take action.
- More than 70% of organizations increased their budget for perimeter defenses, despite less than one quarter of respondents citing a perimeter breach as the attack stage most difficult to mitigate, and only 12% rank a perimeter breach as the top security concern in the next 12 months.
- Nearly half of organizations (49%) allow third-party vendors (such as supply chain and IT management firms) remote access to their internal networks.
  - While the majority of respondents secure and monitor that access, the public sector has the least third-party vendor access controls in place compared to other industries, with 21% not securing and 33% not monitoring that activity.

Current State of Cyber Security Risk and Threat Response

Many organizations today have adopted a "post-breach" mindset, meaning they operate under the presumption of a breach and have developed post-breach response plans. This preparedness is leading to positive steps in post-breach planning, but concerns emerge about the risks of overconfidence – or perhaps complacency – and the ability to adequately protect valuable assets from cyber attacks.

- Three quarters (75%) of IT decision makers believe that their organization can prevent attackers from breaking into their internal network, up from 44% in 2015.
- 67% believe their organization's CEO and/or board of directors provide sound leadership for their cyber security strategy, up from 57% in 2015.
- More than one third (36%) believe a cyber attacker is currently on their network, or has breached their organization's network in the past 12 months.
- At the same time, nearly half (46%) believe their organization has been a victim of a ransomware attack in the past two years.
- 68% of respondents cite losing customer data as one of their biggest concerns following a cyber attack.
  - 60% of those who use the cloud store customer data in it. Other sensitive data stored in the cloud includes employee information (47%), corporate IP (42%), personally identifiable information (PII) (39%), network or admin passwords (29%) and personal passwords (27%).
  - 57% of those who store information in the cloud are not completely confident in their cloud provider's ability to protect their data.
  - Nearly half (46%) state they aren't completely aware of what their organization's cloud services provider is doing to protect and monitor privileged accounts.
- In response to a breach, respondents' top three priorities are most likely to include stopping the breach/removing the attackers (69%), detecting the source of the breach (53%) and updating IT security to prevent the same breach occurring again (44%).
- The vast majority (95%) of respondents report that their organization has a cyber security emergency response plan.
  - However, less than half (45%) of respondents report that it has been communicated and is regularly tested with all IT staff, while four in ten (40%) state that their organization's plan has only been communicated and regularly tested with senior IT staff.

On the Radar: Future Risks Emerge

With the threat landscape constantly shifting, respondents prioritize the types of cyber attacks or tactics that are the most concerning for their organization in the next 12 months. Those include: Distributed denial-of-service (DDoS) attacks (19%), phishing (14%), ransomware (13%), privileged account exploitation (12%) and perimeter breaches (12%).

Responses are fairly consistent, underscoring the breadth of risks that organizations consider important to mitigate, and pointing to very real challenges in determining how to prioritize related cyber security initiatives. Of note, one clear discrepancy between respondents is associated with privileged account security. While 17% of business/technical staff rank it as their top concern, only 10% of C-level executives feel the same. This indicates the need for greater C-suite education and awareness about privileged account security threats, and the potential for direct business impact.

As threats against critical infrastructure become a reality, such as the much-publicized power outage in the Ukraine and the attack on the Gundremmingen nuclear power plant in Germany, respondents share their opinion on what scenarios present the most immediate and potentially catastrophic cyber security threat in general. The majority (58%) feel an attack on financial systems, including disruption of global stock markets, is the most threatening.

Respondents' views of the security industry's ability to cope with cyber attacks is decidedly mixed. While 82% believe that the security industry is making progress against cyber attacks, nearly one fifth (17%) think that the security industry is falling further behind in this area.

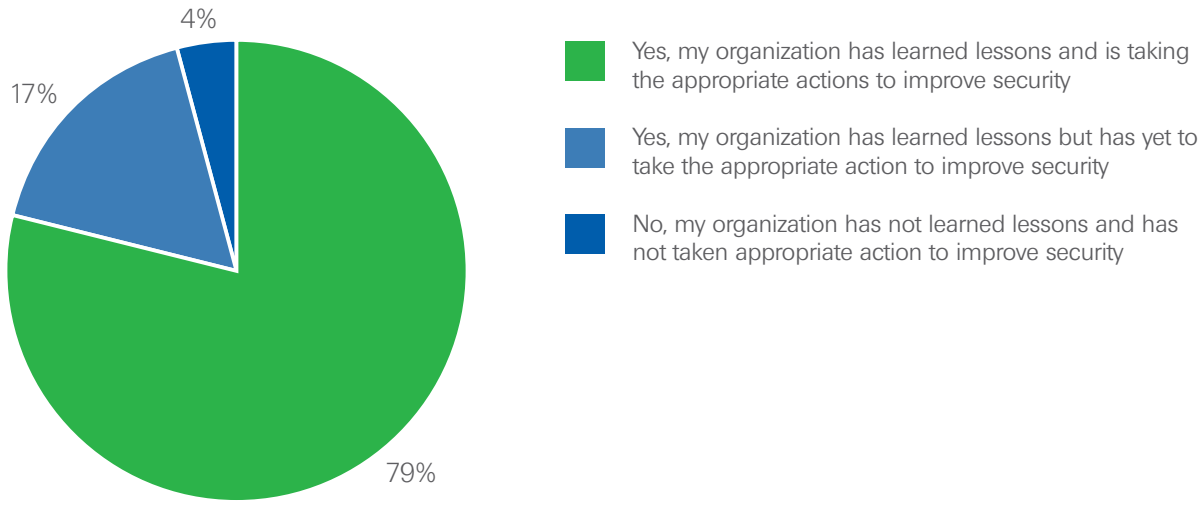
Looking at the reality or imminent prospect of heightened regulatory environments and the impact on cyber security programs and accountability, while 70% of global respondents agree that the threat of legal action and fines impacts the level of executive/board involvement in security-related decisions, 22% of the respondents do not incorporate compliance fines or legal fees (19%) into the cost of a breach. This is surprising given that certain legislation, like the European Union General Data Protection Regulation (EU GDPR), will levy hefty administrative fines for data security breaches. The survey finds a varied global picture in terms of preparedness for increased regulatory oversight.

Key Report Findings

Lessons Learned and the Impact on Prioritizing IT Security

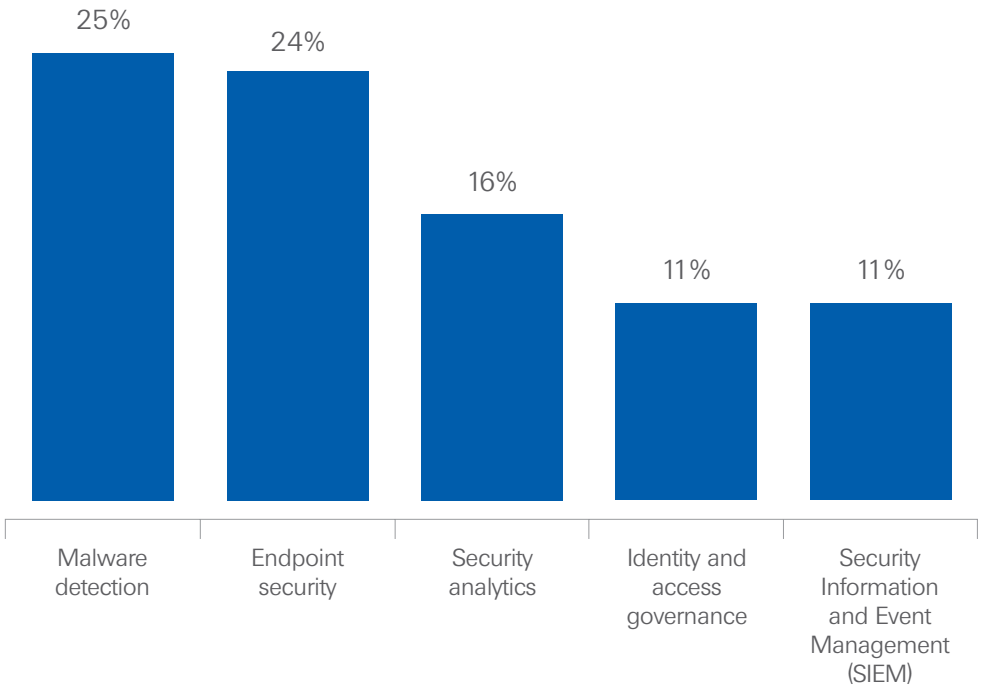
The majority (79%) of respondents say their organization has learned lessons from major publicized security breaches and is taking appropriate actions to improve security. (figure 1) While many organizations are indeed doing the right things, like nearly 80% measuring how they manage or reduce the risk of a cyber attack, the prevalence of poor IT security habits threatens to undermine this progress.

Fig. 1: **Over the past two years, do you think your organization has learned lessons from major publicized cyber attacks and changed or updated its security strategies as a result?**



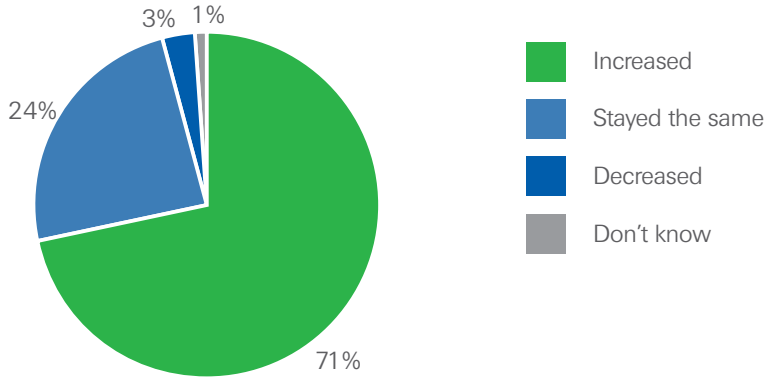
Those respondents whose organization learned lessons and took actions to improve security say the following areas ranked first among the changes they implemented: malware detection (25%), endpoint security (24%) and security analytics (16%). (figure 2)

Fig. 2: **In response to cyber attacks that have been widely publicized in the news or by other means over the past two years, what has been the top change implemented by your organization to better protect itself?**



Indicating a gap between perceived risk and spending levels, more than 70% increased their budget for perimeter defenses. (figure 3) This increase is despite the fact that less than one quarter of respondents cite a perimeter breach as the attack stage most difficult to mitigate, and only 12% rank a perimeter breach as a top security concern in the next 12 months.

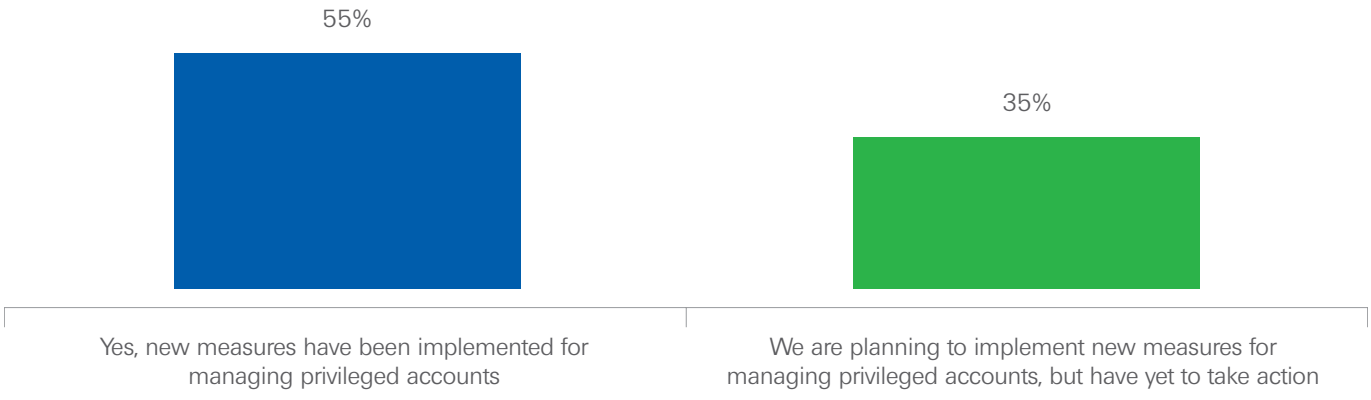
Fig. 3: **How has your organization's perimeter security budget (e.g. for firewalls, intrusion detection, antivirus/ malware detection, DLP, etc.) changed in the past two years?**



Lax Privileged Account Security Best Practices Put Enterprises at Risk

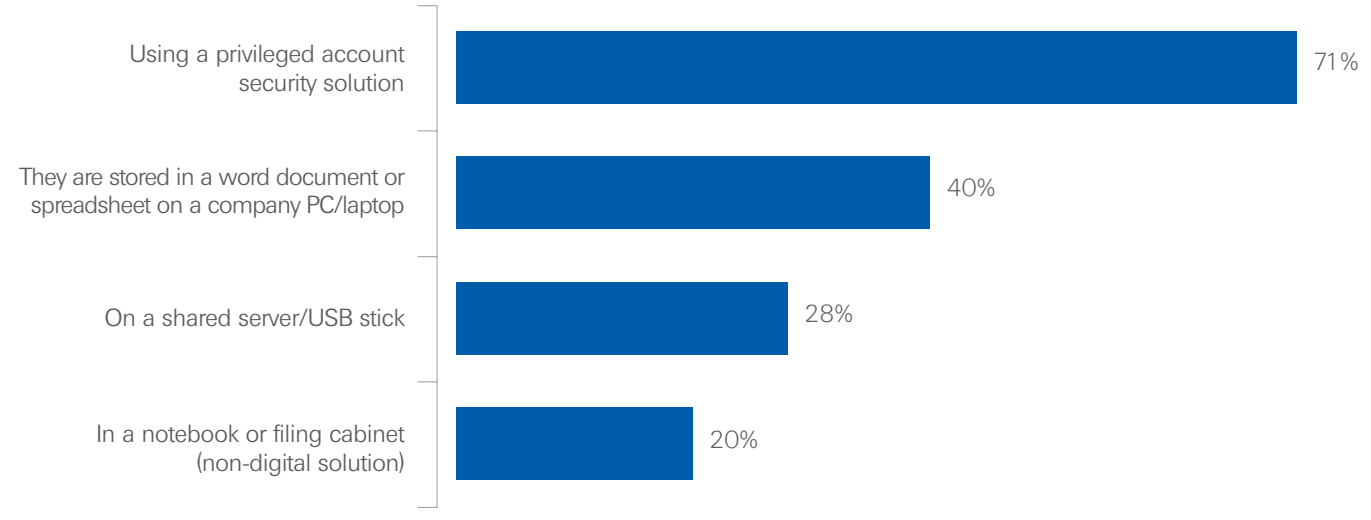
Privileged accounts and credentials provide a pathway to an organization's high-value digital assets and are consistently exploited in nearly all advanced cyber attacks. The fact that more than half (55%) of respondents say that their organization has changed or evolved processes for managing privileged accounts (figure 4) points to greater awareness about the power of privileged credentials, and why attackers specifically seek them out in order to accomplish their goals. Those goals can include financial gain, espionage, sending a message or impacting an organization's ability to operate. Indicating there is still progress to be made, more than a third (35%) report they are planning to implement new measures but have yet to take action.

Fig. 4: **Has your organization changed or evolved the process of managing privileged accounts over the past two years?**



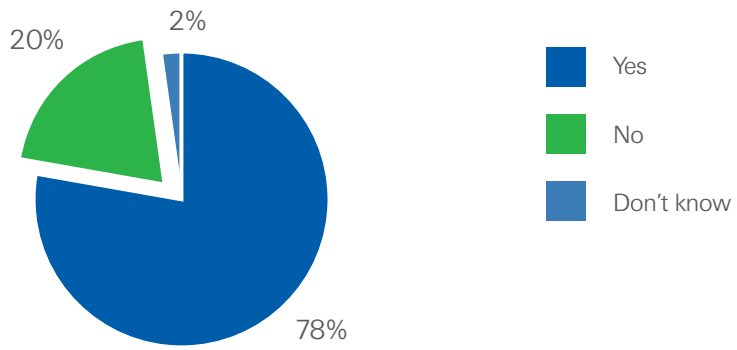
While 71% of respondents say they use a privileged account security solution, it's clear the adoption of best practices lags far behind. For example, while respondents rank privileged account takeover as the second most difficult stage of a cyber attack to mitigate, organizations aren't making it harder for attackers. Four in ten (40%) of respondents are still storing privileged and/or admin passwords in a Word document or spreadsheet on a company PC/laptop, just under three in ten (28%) use a shared server/USB stick, and two in ten (20%) use a non-digital solution. (figure 5)

Fig. 5: **How does your organization store and manage its privileged and/or administrative passwords?**



According to the survey, one-fifth aren't treating privileged account passwords for applications with the same level of security as human user accounts. (figure 6) Given this is an emerging area with nascent best practice adoption seen in the field, this response seems to indicate overconfidence about the steps being taken to protect these accounts. Not adopting best practices around protecting application credentials is troublesome given the critical functions that commercial off-the-shelf (COTS) applications control such as policy setting, provisioning an SSL certificate, asset discovery, importing and exporting data, identifying configurations and more.

Fig. 6: **Does your organization treat privileged account passwords for applications with the same rigor as human user account passwords?**

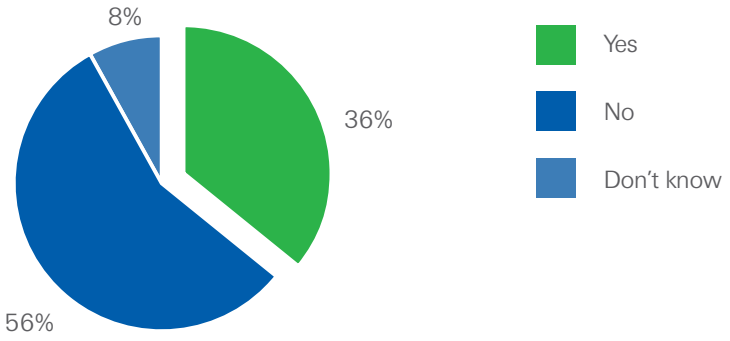


Managing the Threat of an Attack

Three quarters (75%) of surveyed IT decision makers believe their organization can prevent attackers from breaking into their internal network, up from 44% in 2015. This increase may be an indicator of a false sense of confidence – or overconfidence - given the rise of aggressive, damaging attacks, like those attributed to ransomware. In fact, 46% believe their organization has been a victim of a ransomware attack over the past two years.

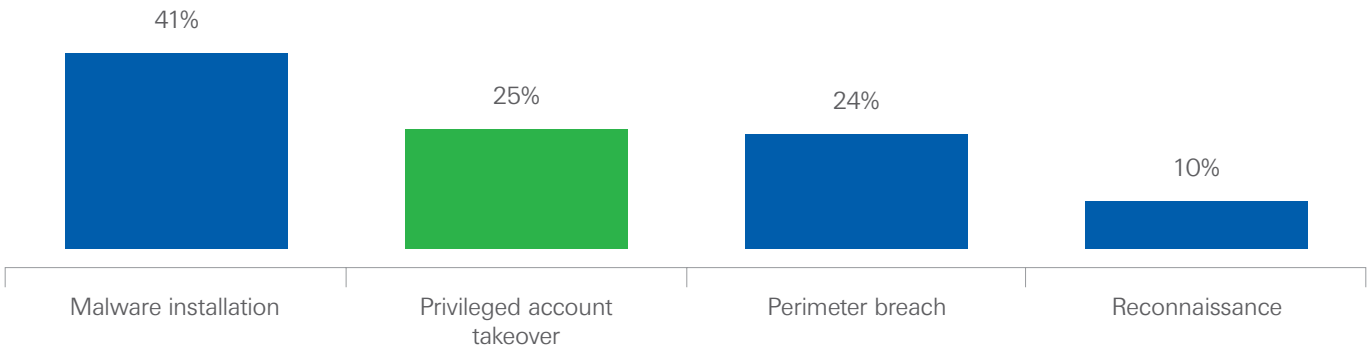
More than a third (36%) believe a cyber attacker is currently on their network, or has breached their organization's network in the past 12 months. This finding continues to reinforce the need for adopting a post-breach mind set, one that presumes motivated attackers will find their way onto the network. (figure 7)

Fig. 7: **Do you believe a cyber attacker is currently on your network, or has breached your network in the past 12 months?**



Examining perceptions of the most difficult stage of a cyber attack to mitigate, malware installation ranks number one (41%), privileged account takeover is second (25%). (figure 8)

Fig. 8: **At what stage of a cyber attack does it become the most difficult for your organization to mitigate?**

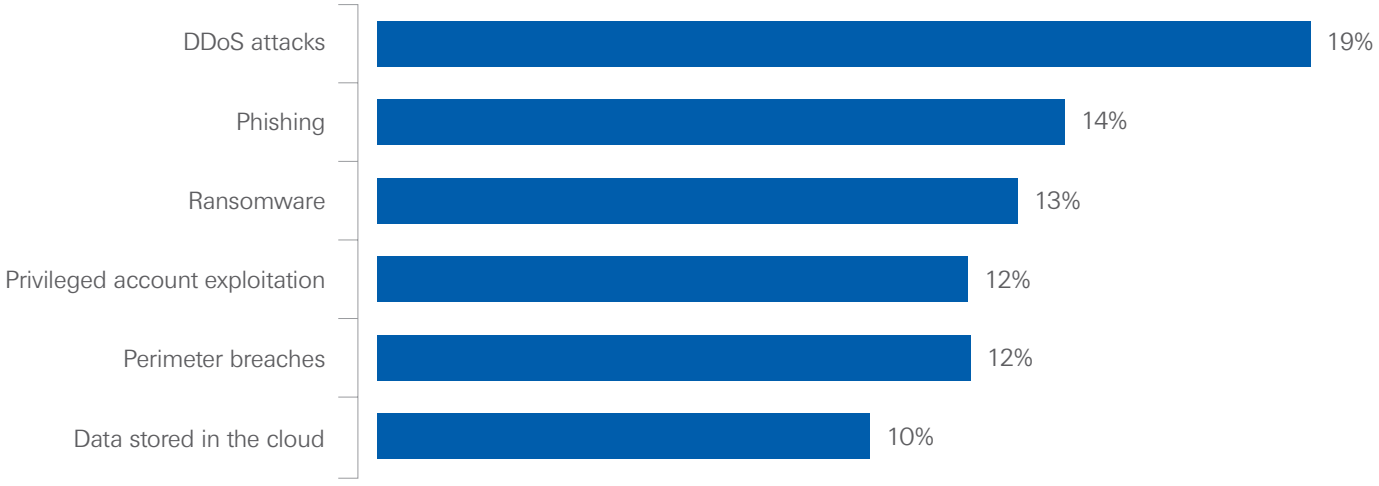


With the threat landscape constantly shifting, respondents prioritized the types of cyber attacks or tactics they think are the most concerning for their organization in the next 12 months. Those include: Distributed denial-of-service (DDoS) attacks (19%), phishing (14%), ransomware (13%), privileged account exploitation (12%) and perimeter breaches (12%). (figure 9)

Responses are fairly consistent, underscoring the breadth of risks that organizations consider important to mitigate, and pointing to very real challenges in determining how to prioritize related cyber security spend. Of note, one clear discrepancy between respondents is associated with privileged account security. While 17% of business/technical staff rank it as their top concern, only 10% of C-level executives feel the same. This indicates the need for greater C-suite education and awareness about privileged account security threats, and potential for direct business impact.

In examining regional perspectives, respondents rank DDoS attacks higher than the global average (19%) as a concern in Germany (27%), Singapore (26%), Australia and New Zealand (27%) and Israel (28%). This may be a combination of the increased visibility and prevalence of these types of attacks, which are relatively inexpensive and easy to execute today, the availability of "DDoS-as-a-Service" attacks and the ability (or inability) for organizations in these markets to effectively identify and defend against these sorts of attacks.

Fig. 9: **In the next 12 months, what types of cyber attacks or tactics do you think are the number one concern for your organization?**



As threats against critical infrastructure become a reality, such as the much-publicized power outage in the Ukraine and the attack on the Gundremmingen nuclear power plant in Germany, respondents share their opinion on what scenarios present the most immediate and potentially catastrophic cyber security threat in general. The majority (58%) feel an attack on financial systems, including disruption of global stock markets, is the most threatening. (figure 10)

Massive utilities damage caused by a cyber attack is the most likely scenario that the general public has never even considered a possibility at 31%, but in their opinion poses one of the greatest threats (55% of respondents feel this presents an immediate and potentially catastrophic effect). (figure 11)

Not surprisingly, respondents from the biotechnology/pharmaceutical (55%) and manufacturing sectors (45%) are most concerned about cyber attacks on organizations such as automobile or drug manufacturers to tamper with product quality or safety.

Fig. 10: **Based on your knowledge and understanding, when thinking about cyber attacks in general, which scenarios present the most immediate and potentially catastrophic threat?**

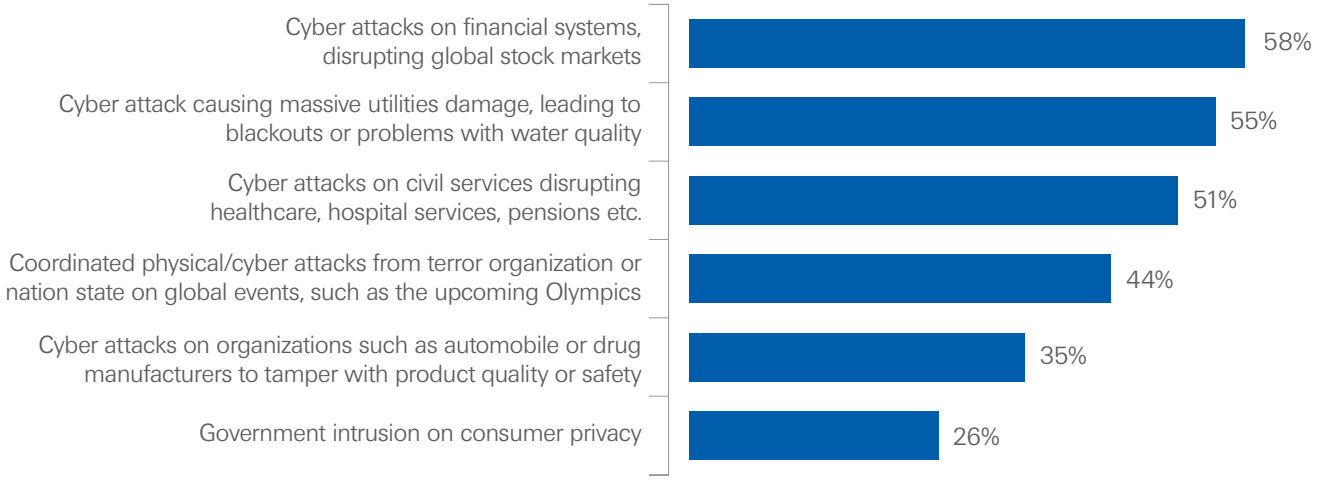
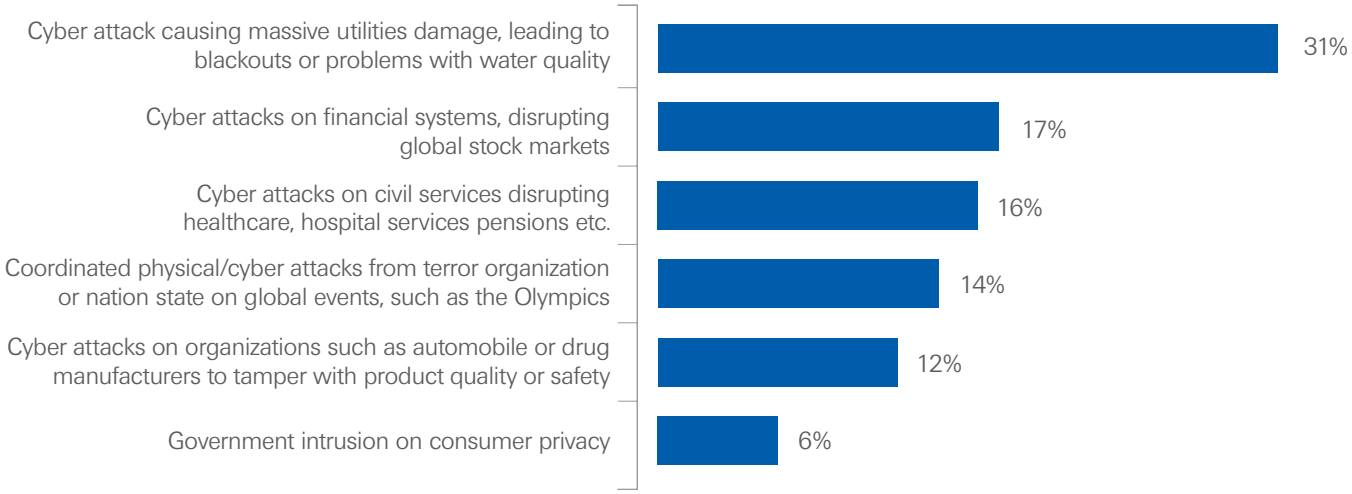


Fig. 11: **Which of the following attacks is the one that you believe the general public has never even considered a possibility?**

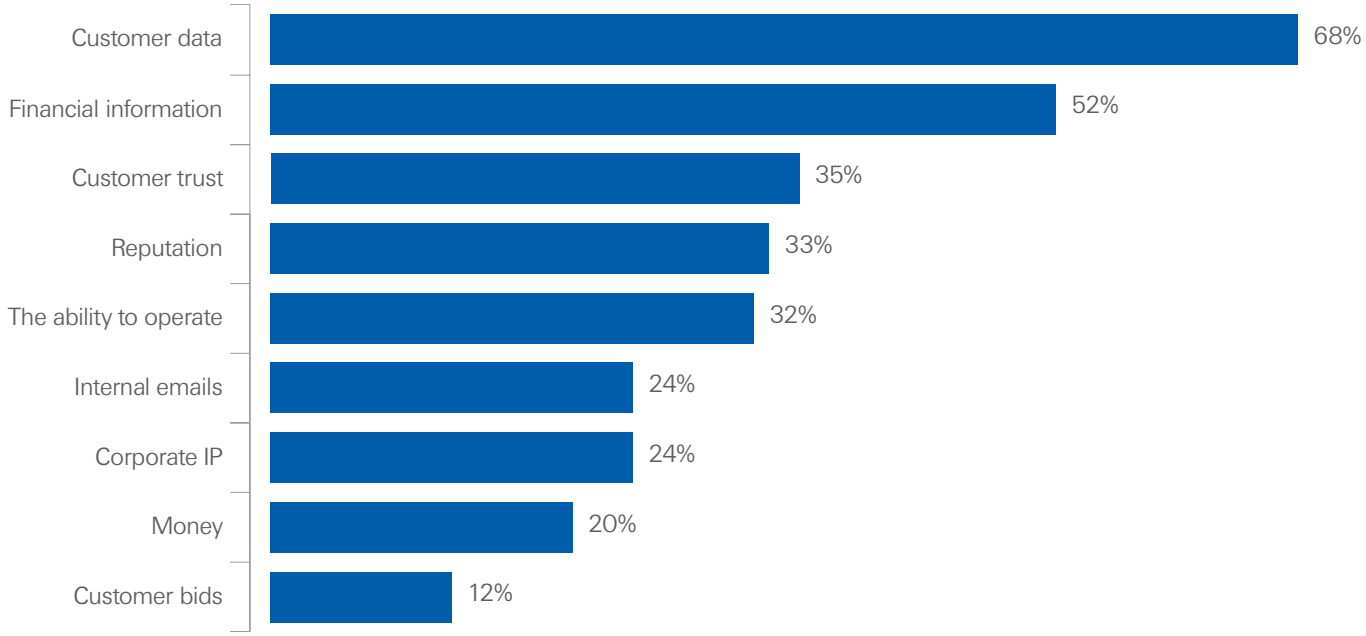


Cyber Attack Preparedness, Response & Future Outlook

Many organizations today have adopted a "post breach" mind set, meaning they operate under the presumption of a breach and have developed post-breach response plans. This preparedness is leading to positive steps in post-breach planning, but concerns emerge about the risks of overconfidence – or perhaps complacency - and the ability to adequately protect valuable assets from cyber attacks.

Global respondents are most worried about losing customer data (68%) as a result of a cyber attack, followed by financial information (52%), customer trust (35%), reputation (33%) and the ability to operate (32%). (figure 12) It's interesting to note the emphasis on trust and reputation, over the ability for the organization to conduct business.

Fig. 12: **What would your organization be most concerned about losing in a cyber attack?**

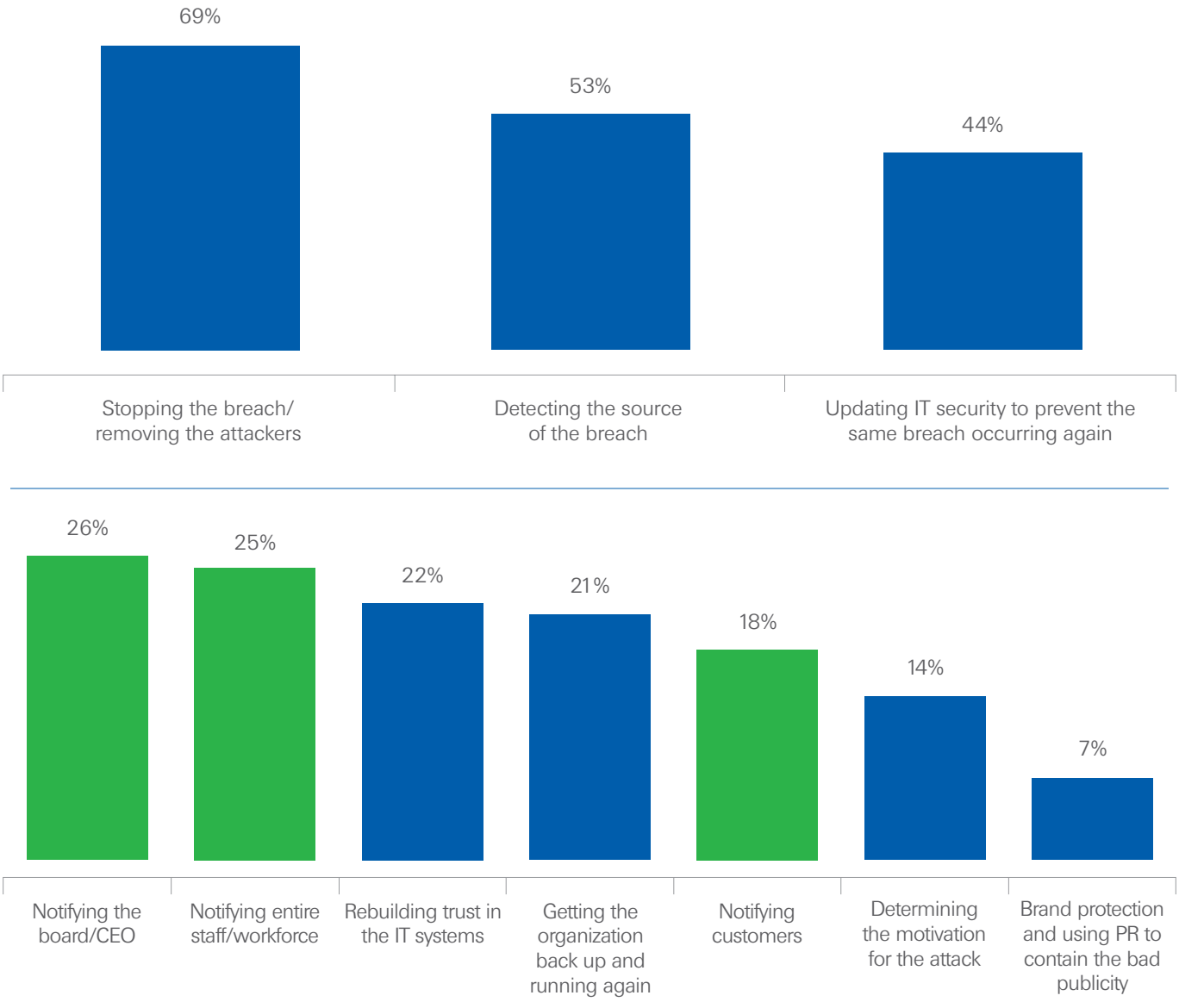


Nearly seven in ten (69%) respondents state that in response to a breach or cyber attack, stopping the breach/removing the attackers is among their top priorities. More than half (53%) also cite detecting the source of the breach as a top priority, while fewer respondents believe the same for notifying either the board/CEO (26%), entire staff/workforce (25%) or customers (18%). (figures 13 & 14)

Given evolving regulatory environments and breach notification laws, the fact that customer and board/CEO communication are so low on the list bears further examination. Consider the European Union General Data Protection Regulation (EU GDPR) that calls for a data breach to be reported within 72 hours of the organization becoming aware of the breach, or face steep fines. The LinkedIn breach is an example of a four year delay in breach notification, leaving many to think the company did not take the potential security implications seriously enough.

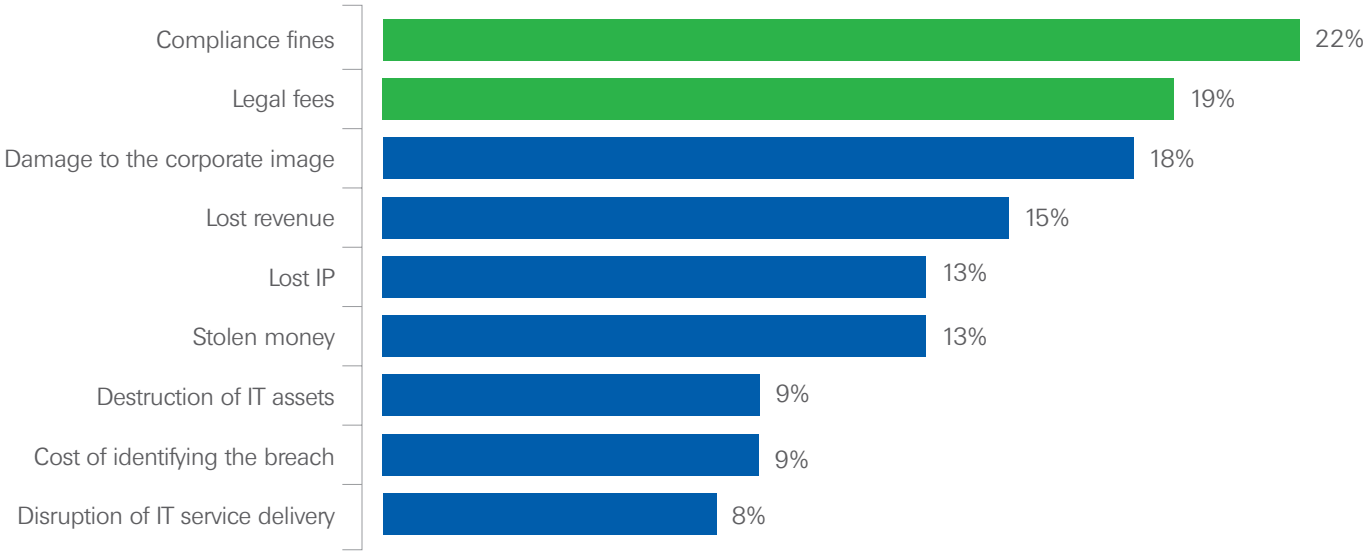
Of the vertical industries surveyed, consumer-oriented sectors like retail did not prioritize customer notification following a breach (19%), surprising given the number of point-of-sale system attacks in the news. On a positive note, IT and telecoms ranked customer notification higher (28%), perhaps indicating these organizations have learned lessons from high profile attacks hitting this sector.

Fig. 13 and 14: **In response to a breach or cyber attack, what would be your organization's top three priorities?**



A common thread of this report is understanding the impact of a breach – beyond financial – on organizations' longer term cyber security priorities and planning. When asked how their organization estimated the cost of a data breach, the items that weren't considered or weren't prioritized highlighted some worrisome issues, especially in light of tightening legislation and breach notification laws, with 22% not including compliance fines and 19% not including legal fees. (figure 15)

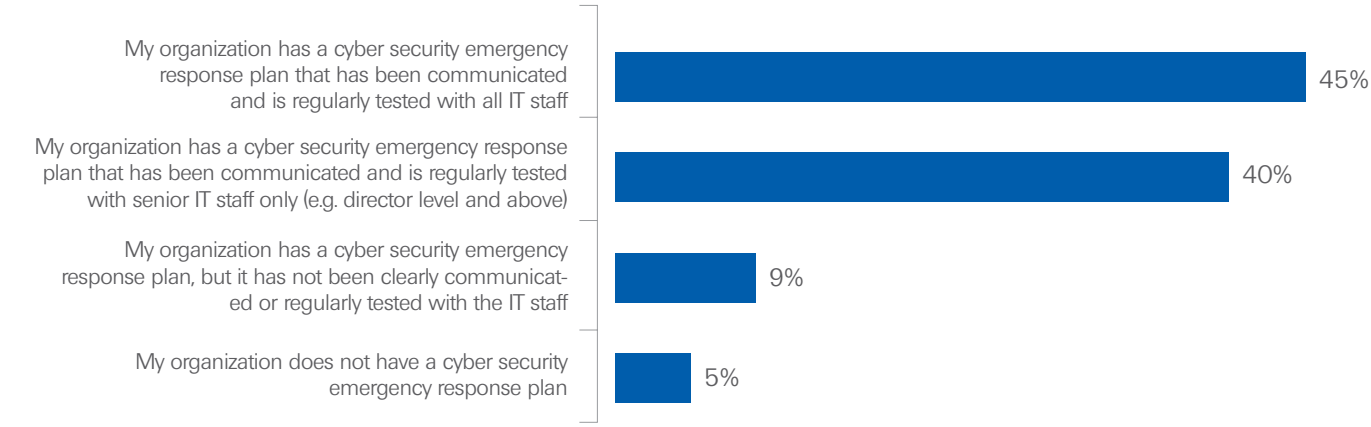
Fig. 15: **How does your organization estimate the cost of a data breach and what is not included in the cost of a breach?**



The vast majority (95%) of respondents report that their organization has a cyber security emergency response plan. However, simply having a plan should not equal confidence in an organization's leadership team.

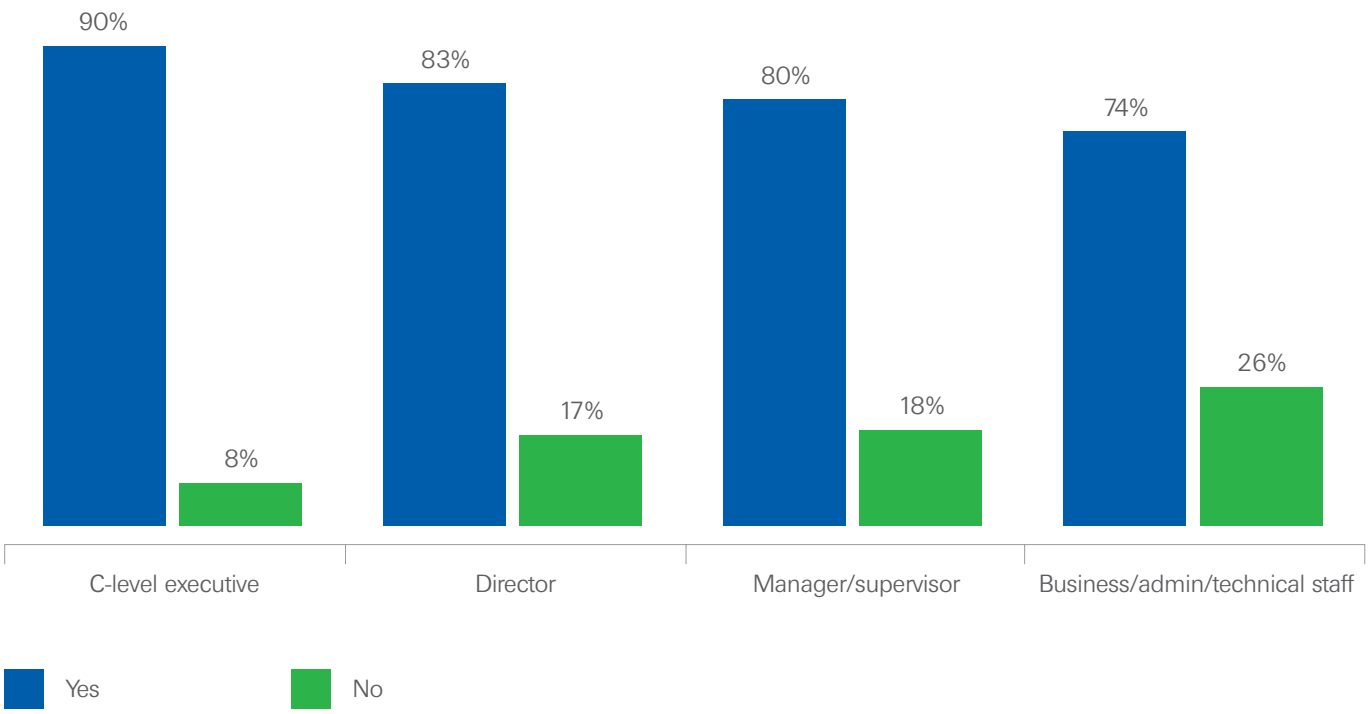
Further, 57% of respondents are not completely certain about their specific role in response to a cyber attack/cyber emergency. Drilling down into vertical markets, 14% of public sector respondents do not have a cyber security response plan, followed by transport and distribution (11%).

Fig. 16: **Which of the following statements best describes your organization's cyber security emergency response plan?**



Of the respondents, 82% feel that the security industry is making progress against cyber attacks, while 17% think it is falling further behind. (figure 17) That optimism is skewed within an organization, with more than three times more business and technical staff feeling the industry is falling behind (26%), compared with C-level executives (8%). This delta could again be attributed to an over-confident leadership team, versus the teams on the front lines of cyber security.

Fig. 17: **Will the security industry ever be able to make progress against cyber attackers?**



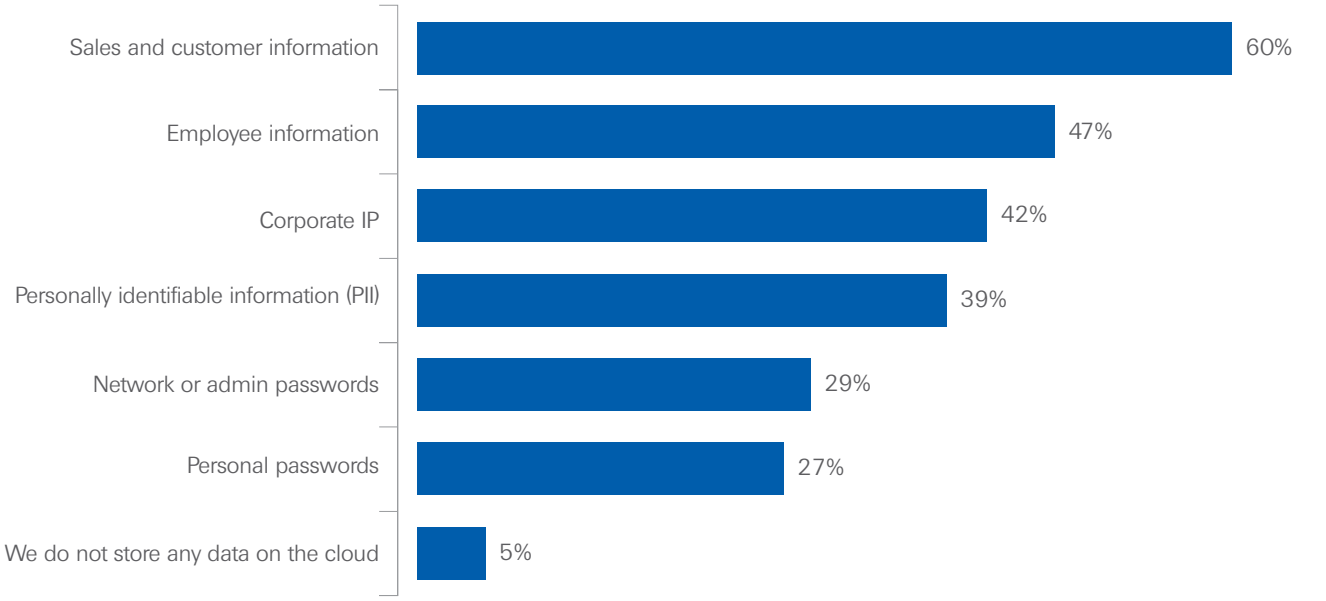
Cloud Investments and Security Confidence

The vast majority (93%) of respondents report that their organization invests in or currently uses cloud. More than half (54%) state that their organization currently invests in or uses Software-as-a-Service, while around four in ten say the same for public Platform-as-a-Service (39%) and public Infrastructure-as-a-Service (37%). Additionally almost half (45%) are investing in or using hybrid cloud.

While the business benefits of utilizing the cloud for elasticity and business agility are well documented, the survey identifies several security concerns that have a direct impact on the business. More than one third (31%) of respondents cite storing data in the cloud as a top security concern in the next 12 months. Additionally, the majority of respondents (68%) cite losing customer data as one of their biggest concerns following a cyber attack. According to the survey, 60% of respondents who use the cloud store sales and customer data in it. (figure 18) More than half (57%) who store information in the cloud are not completely confident in their cloud provider's ability to protect confidential information.

And, when it comes to storing data in the cloud, nearly half (46%) stated they aren't completely aware of what their organization's cloud services provider is doing to protect and monitor privileged accounts. An effective cloud strategy includes securing privileged accounts from the beginning – from protecting assets running in the cloud, and integrating security into DevOps processes, to facilitating secure cloud migrations and enabling organizations to get the full benefit of the cloud.

Fig. 18: **What data does your organization store in the cloud?**

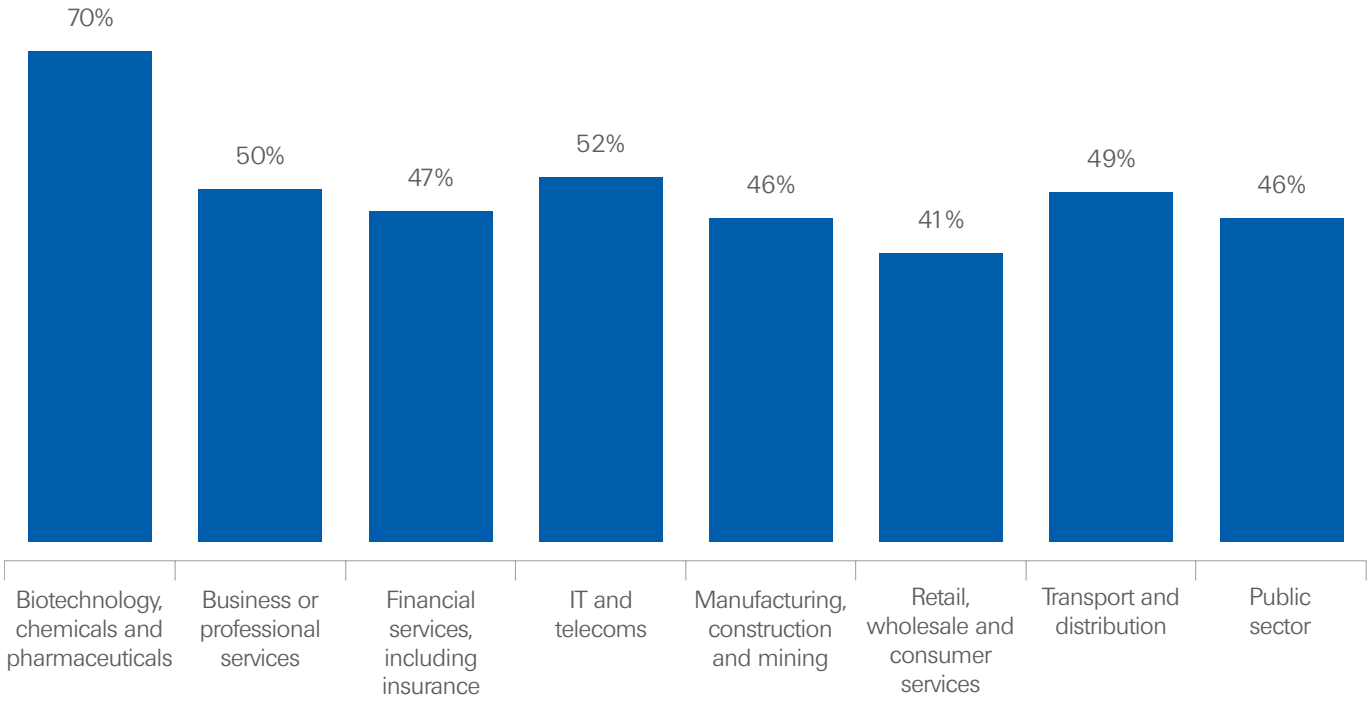


Third-Party Vendor Risk Management

Many third parties, including vendors, contractors, consultants and service providers have authorized access to networks, allowing them to change, alter or impact the operational service of the target organization. Nearly half (49%) of organizations allow third-party vendors (supply chain, IT management firms, etc.) remote access to their internal networks. The top three vertical industries allowing third-party vendor access are biotechnology/pharmaceutical (70%), IT and telecoms (52%) and business/professional services (50%). (figure 19)

In a strong example of organizations not learning their lessons from past breaches, according to this survey, the public sector has the least third-party vendor access controls in place with 21% not securing activity, and 33% not monitoring that activity. This comes only one year following the massive U.S. Office of Personnel Management (OPM) data breach, where social engineering was used to lead attackers to obtain credentials of a third-party contractor.

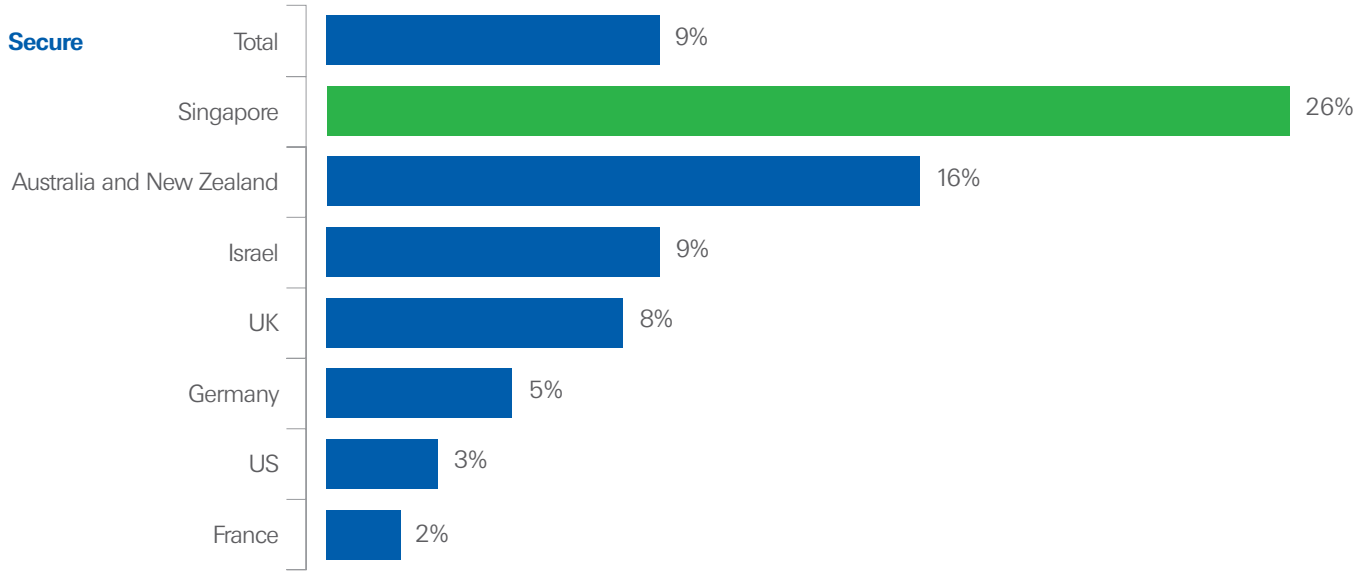
Fig. 19: **Which industries allow third-party vendors (supply chain, IT management firms, etc.) remote access to internal networks?**

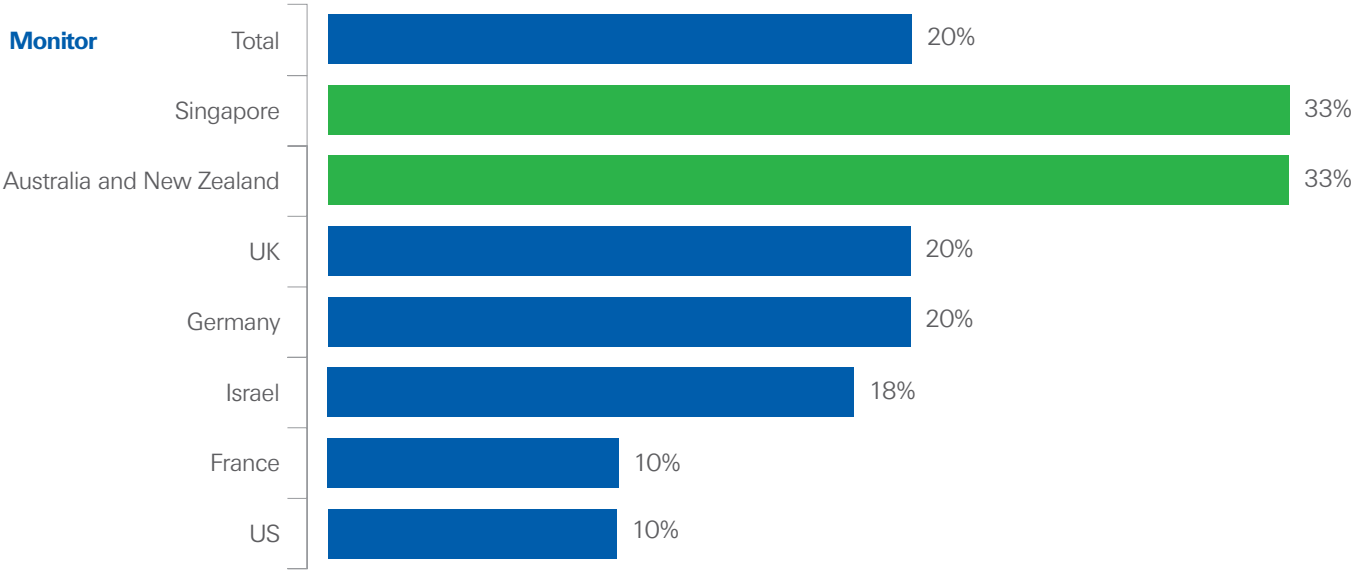


As organizations work to secure their networks, they often overlook remote access security controls, which can help to secure third-party access to privileged accounts. As a result, organizations are left with a very weak link in security, one that is all too often exploited by attackers to gain powerful access to the network.

While most global organizations are doing a good job of securing and monitoring that access, fewer best practice policies are apparent in Asia Pacific with 26% in Singapore neglecting to secure third-party access, and 33% in Singapore and 33% Australia and New Zealand saying they don't monitor that access. (figure 20)

Fig. 20: **Respondents whose organization is not securing or monitoring third-party vendor access.**





The High Cost of Non-Compliance

Legislation around cyber security continues to be introduced or strengthened globally, both at the nation state level as well as from politico-economic blocs such as the European Union. In the U.S., individual states require companies to notify their customers, immediately or without unnecessary delay, if personal data has been compromised. Other countries have introduced similar laws as well.

The survey asked specific questions around three pieces of legislation: European Union General Data Protection Regulation (EU GDPR), KRITIS in Germany, and the potential Mandatory Breach Notification amendment to Australia's Privacy Act. In this section, we examine preparedness for the introduction of more stringent security regulations as well as the perceived impact upon individuals and organizations.

EU GDPR

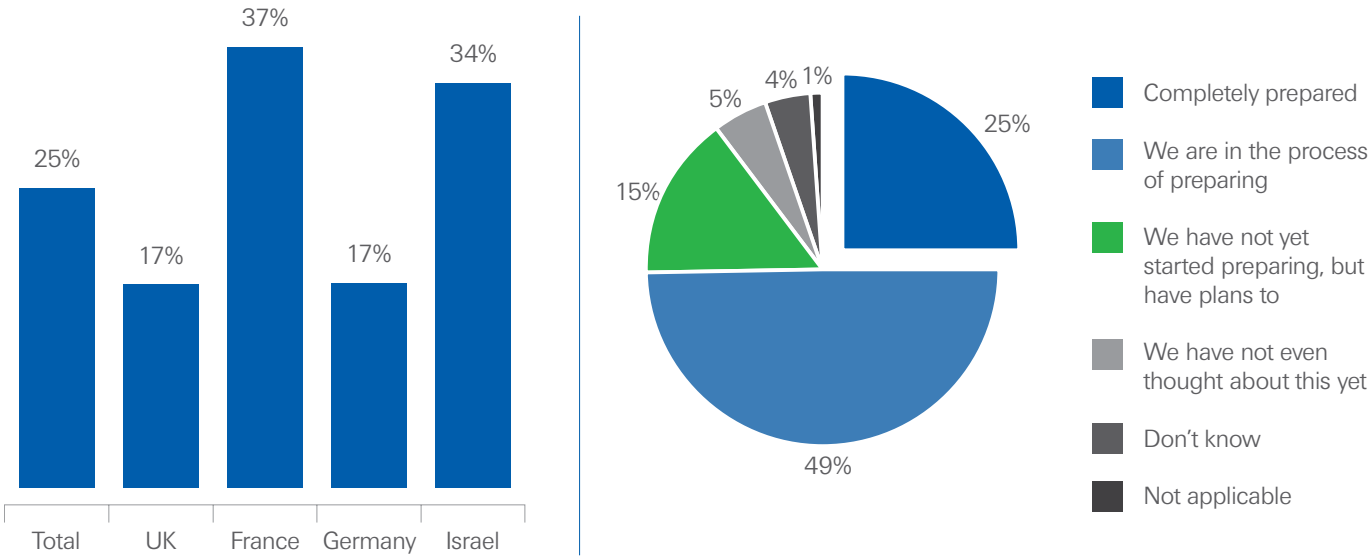
The EU GDPR is a directive that applies to all EU member states, adopted on April 14, 2016, after four years of drafting and negotiations. It will significantly affect businesses in all industry sectors. Broadly speaking, it makes data protection the responsibility of the entire organization, and organizations have until May 25, 2018 to become fully compliant. Failure to comply could result in fines of up to 4% of annual global turnover or €20 million – whichever is greater.

Worryingly, of respondents from EMEA, a fifth report that they have not started preparing for GDPR's requirements, and only a quarter (25%) report that their organization is completely prepared for its introduction. C-level respondents (38%) are twice as confident in their complete preparedness as managers (20%) or business/technical staff (20%). (figure 21)

Given the potential punitive fines for non-compliance, also interesting is the proportion (31%) of respondents who feel that this aspect of GDPR will be helpful in getting board-level attention of its requirements.

As with other, similar regulations such as the proposed amendment to the Australia Privacy Act, when asked about the likely impact of GDPR on an individual's role and organization, answers are starkly split between those seeing it as positive and having no impact at all. Only 10% feel it will have a negative impact on them as an individual, and only 12% feel it will have a negative impact on their organization. Respondents from France are the most positive about both these aspects, with 60% feeling GDPR will be positive for them and 59% for their organization.

Fig. 21: **How prepared is your organization for the introduction of GDPR (General Data Protection Regulation) compliance?**



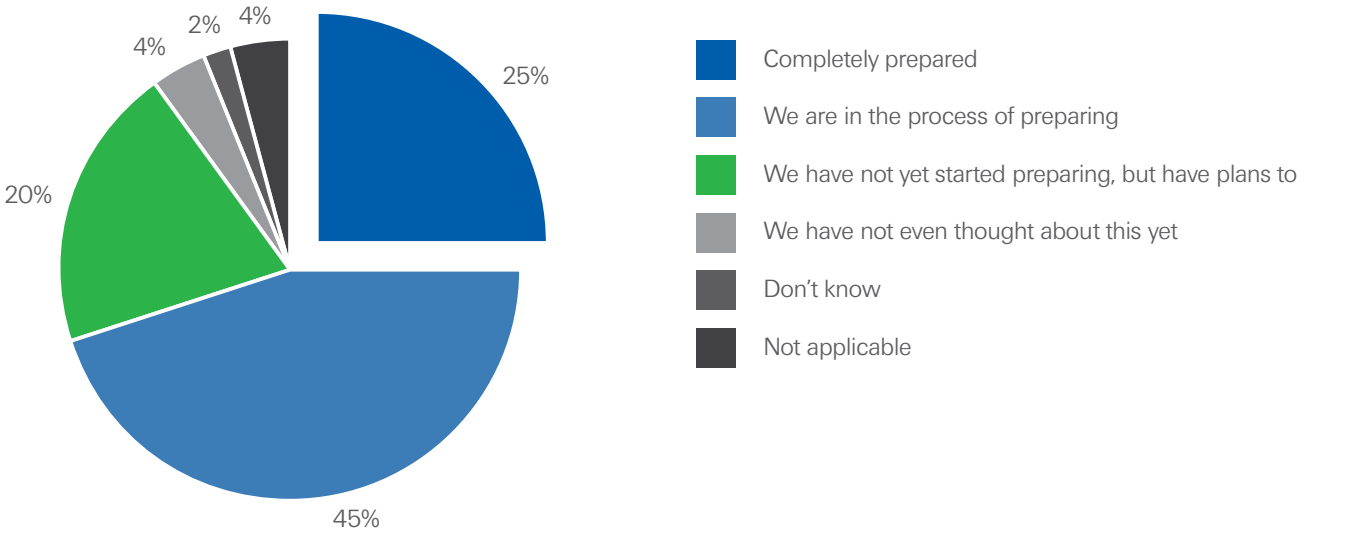
KRITIS

Germany's Implementation Plan for Critical Infrastructure Protection (KRITIS) is aimed at ensuring the ongoing readiness within the designated (and recently expanded) key industries of energy, information technology and telecommunications, transportation, health, water, nutrition, and finance and insurance. Not limited to technology issues, it nevertheless promotes IT resilience as well as joint assessment and evaluation of cyber security measures.

Of respondents from Germany, only a quarter (25%) report that their organization is completely prepared for the introduction of new KRITIS-related regulations. (figure 22) Half or more believe these new regulations will have a positive impact upon their role (57%) and organization as a whole (50%), while around four in 10 believe the change will have no impact on their role or organization (38% and 42% respectively).

The more senior a person is, the more likely they are to be positive about impending regulatory change. In fact, no C-level respondents think that there could be a negative impact from KRITIS regulations on either their role or their organization as a whole.

Fig. 22: **How prepared is your organization for the introduction of new KRITIS-related regulations?**



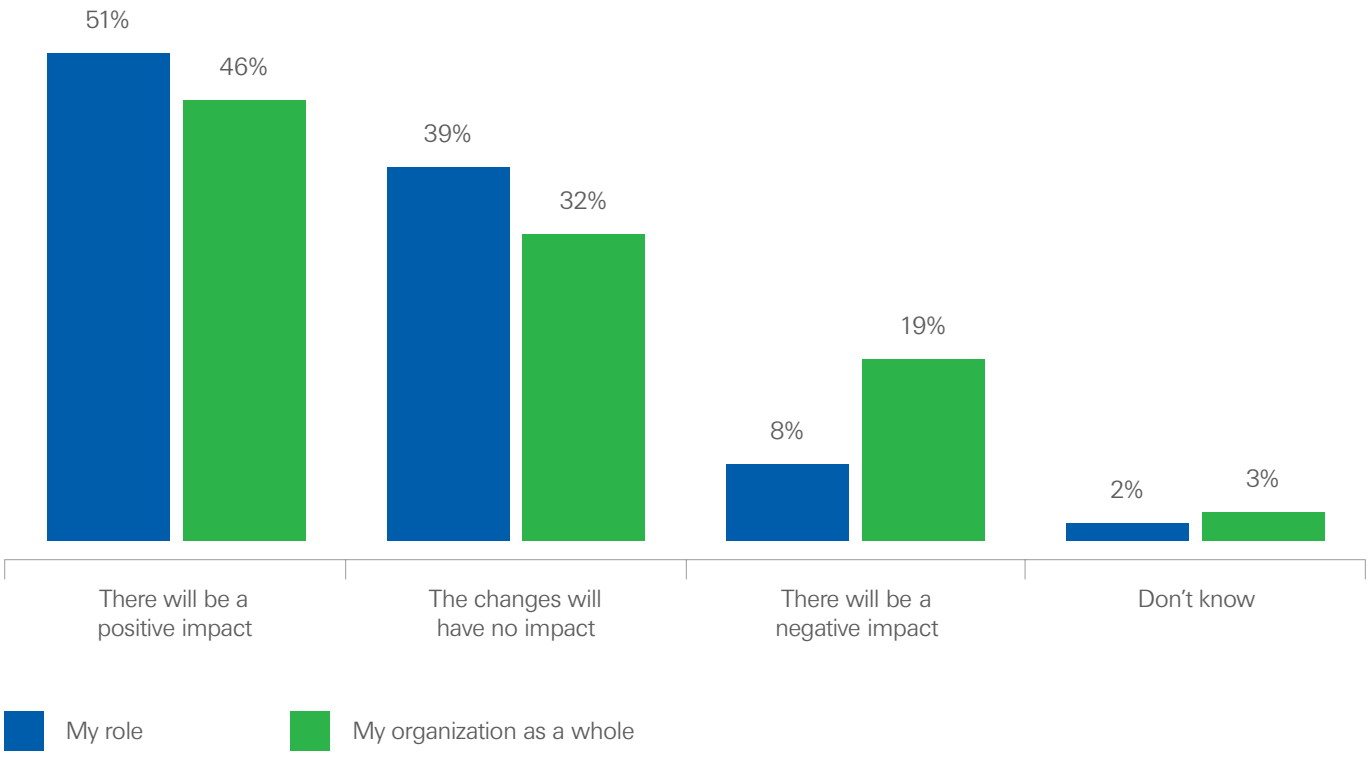
Australia Privacy Act

Currently, the Australian Privacy Act 1988 does not require an organization or agency to notify an individual of a data breach involving their personal information, but a suggested amendment to the Act means that this is likely to change by the end of 2017. Presuming such a requirement becomes law, respondents from Australian organizations were asked about their state of preparedness and the likely impact of a change.

Just over a third (34%) of surveyed IT decision makers in Australia report that their organization is completely prepared to handle mandatory breach notifications if passed as part of the Australia Privacy Act. It can be inferred, therefore, that there is a lack of confidence about either being able to identify a breach, or in existing emergency response plans – including providing the necessary information to the executive team, who would be responsible for the public breach notification.

Looking at how the new regulation is likely to impinge on individuals, half believe it will be positive for their role (51%) and a similar number feel it would be good for the organization as a whole (46%). (figure 23)

Fig. 23: **How will the new mandatory breach notification regulations affect both your role and your organization as a whole?**



Terminology

What Are Privileged Accounts?

Privileged accounts are valid credentials used to gain access to systems, providing elevated, non-restrictive access to the underlying platforms. These accounts are designed to be used by system administrators to manage network systems, run services or allow applications to communicate with one another. The most common privileged accounts are local admin, privileged user, domain admin, emergency, service and application. Privileged accounts can be found in any device with a microprocessor, including PCs, databases, networked devices like copiers, operating systems and more, and too often are 'secured' by default or hardcoded passwords easily found through basic internet searches.

The lack of accountability and protection of privileged accounts in corporate networks is the vulnerability most often exploited by cyber attackers. The benefits of protective controls and detection capabilities on privileged accounts and credentials should not be overlooked as part of a comprehensive security strategy.

About CyberArk

CyberArk (NASDAQ: CYBR) is the only security company focused on eliminating the most advanced cyber threats; those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world's leading companies – including 45 percent of the Fortune 100 – to protect their highest value information assets, infrastructure and applications. A global company, CyberArk is headquartered in Petach Tikvah, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout EMEA and Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.