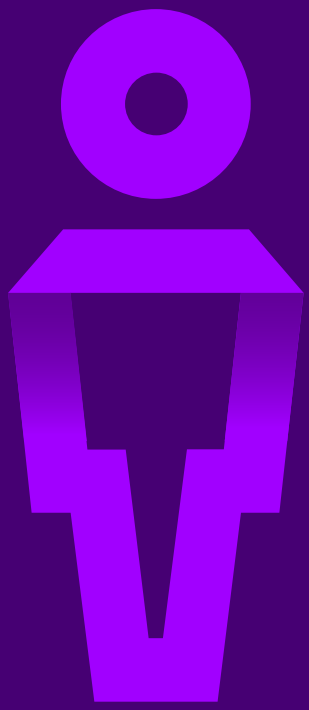
accenture

2018 State of Cyber Resilience in Software & Platforms

GAINING GROUND ON THE CYBER ATTACKER

In February 2018, Accenture conducted a global survey on cyber resiliency with 4,669 executives from companies with annual revenues of $1 billion or more, including 221 respondents from Software & Platforms companies.



Executive summary

- Software & Platforms companies are doing well with regards to cybersecurity with some room left for improvement
- Cybersecurity budget is approved by C-level and amounts to around 20 percent of Software & Platforms companies' IT budget and continues to rise
- New technologies, such as artificial intelligence (AI), machine or deep learning, user behavior analytics, and blockchain are essential to securing the future of these organizations
- Both internal and external focus is needed as attacks may come from outside or inside the organization and a company should protect its whole value chain, including internal assets, as well as their ecosystem of partners
- Around two percent of FTEs work with security at Software & Platforms companies versus the global average of around three percent
- Though Software & Platforms companies are generally highly confident in their cybersecurity capabilities and effectiveness, they seemed somewhat less confident in their cybersecurity effectiveness related to third-party partners and compliance

Introduction

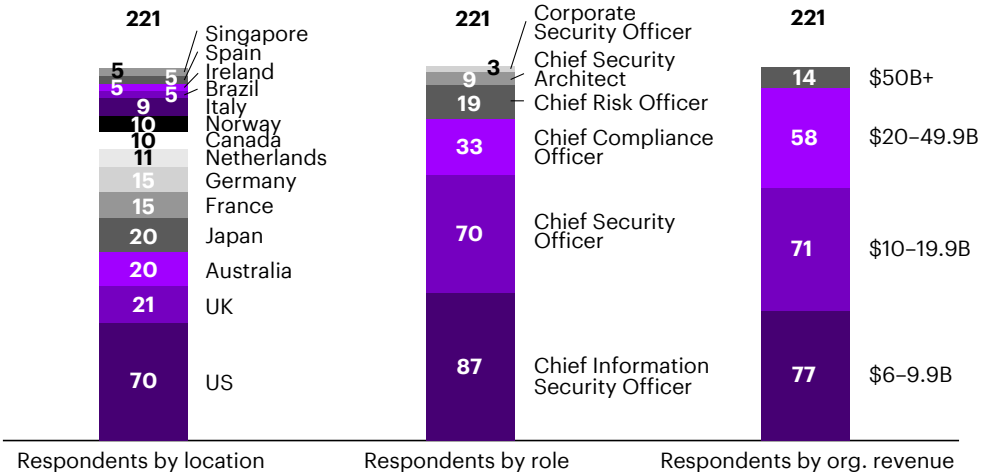
The **cyber-resilient business** brings together the capabilities of cybersecurity, business continuity and enterprise resilience. It applies fluid security strategies to respond quickly to threats, so it can minimize the damage and continue to operate under attack. As a result, the cyber-resilient business can introduce innovative offerings and business models securely, strengthen customer trust, and grow with confidence.

Cyber attacks take many forms and have different degrees of impact. The average organization is subjected to a daily deluge of hundreds—if not thousands—of speculative attacks, which are handled by mature security technologies, such as firewalls. For the purposes of this Accenture research, **we investigated targeted cyber attacks** which have the potential to both penetrate network defenses and cause damage to or extract high-value assets and processes from within the organization.

In 2017, Accenture Security surveyed 2,000 executives to understand the extent to which organizations prioritize security, how comprehensive their security plans are, what security capabilities they have, and their level of spend on security.

Just over a year later, Accenture Security undertook a similar survey, this time interviewing 4,669 executives representing companies with annual revenues of US$1 billion or more from 18 industries and 15 countries across North and South America, Europe and Asia Pacific. More than 98 percent of respondents were sole or key decision makers in cybersecurity strategy and spending for their organization. In this second survey, 221 executives represented Software & Platforms companies from 14 countries with annual revenues of US$6 billion or more (see Figure 1).

FIGURE 1: 221 executives represented Software & Platforms companies from 14 countries with annual revenues of US$6 billion or more in our survey carried out in Feb 2018

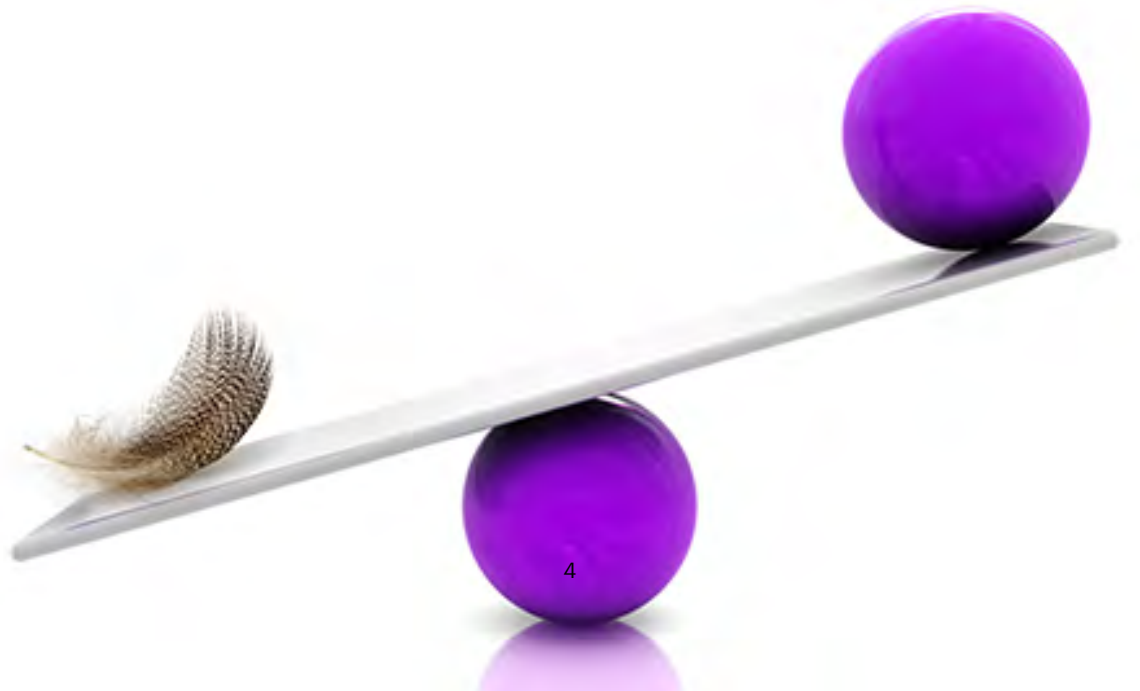


Software & Platforms companies doing well with some room left for improvement

We asked survey respondents to rank their performance based on a list of 33 cybersecurity capabilities across 7 domains (see Figure 2). On average, Software & Platforms companies performed high on 22 of these capabilities, outperforming the global average of 19 (see Figure 3).

FIGURE 2: Respondents were asked to rate their performance on 33 cybersecurity capabilities across 7 domains

Business Exposure	Cyber Response Readiness	Strategic Threat Context	Resilience Readiness	Investment Efficiency	Governance & Leadership	Extended Ecosystem
High Value Assets & Business Processes	Cyber Response Plans	What–If Analysis	Recovery Ability	Securing Future Architecture	High-Value Assets & Business Processes	Contractual Dependability
Physical & Safety Risks	Cyber Incident Escalation Plans	Business Relevant Threat Monitoring	Design for Resilience	Security in Project Funding	Physical & Safety Risks	Operational Cooperation
Cyber Attack Scenarios	Cyber Incident Communication	Peer Situation Monitoring	Exposure Driven Design	Protection of Key Assets	Actual IT Support	Contractual Assurance
IT Risk Support	Stakeholder Involvement	Threat Vector Monitoring	Continuous Improvement	Security in Investment Funding	Scenarios of Material Impact	Regulatory Compliance Focus
Cybersecurity Strategy	Recovery of Key Assets		Threat Landscape Alignment	Risk Analysis & Budgeting	Key Protection Assumptions	



An attack needs to be successful only once, whereas organizations' cyber resilience needs to be effective every time. The ability to detect an attack has significantly improved over the last year. Despite the increased pressure from targeted cybersecurity attacks more than doubling (232 on average in 2018 vs. 106 in 2017, see Figure 4), organizations are demonstrating far more success in heading them off with only one in eight (or around 13 percent) of focused attacks are getting through in 2018. This is much better than the one in three (or around 30 percent_ that caused disruption to organizations just over a year ago.

At the same time, the number of successful attacks stagnating globally at ~30 means that on average, organizations are facing 2-3 security breaches per month. This raises concerns, so there is more work to be done. In comparison, Software & Platforms companies faced on average 251 attacks in 2018, of which 33 (or around 13 percent) were successful, showing further room for improvement.

FIGURE 3: Software & Platforms companies performed high on 22 of 33 cybersecurity capabilities vs. the global average of 19

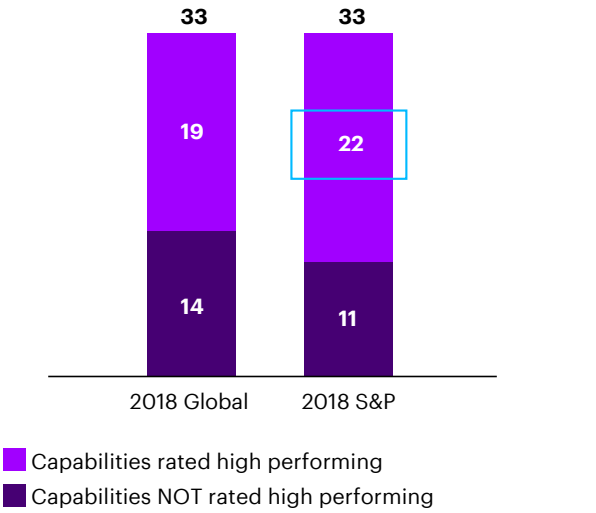
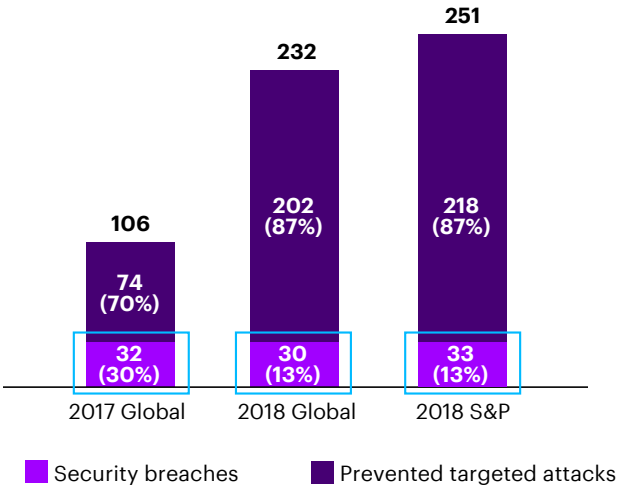
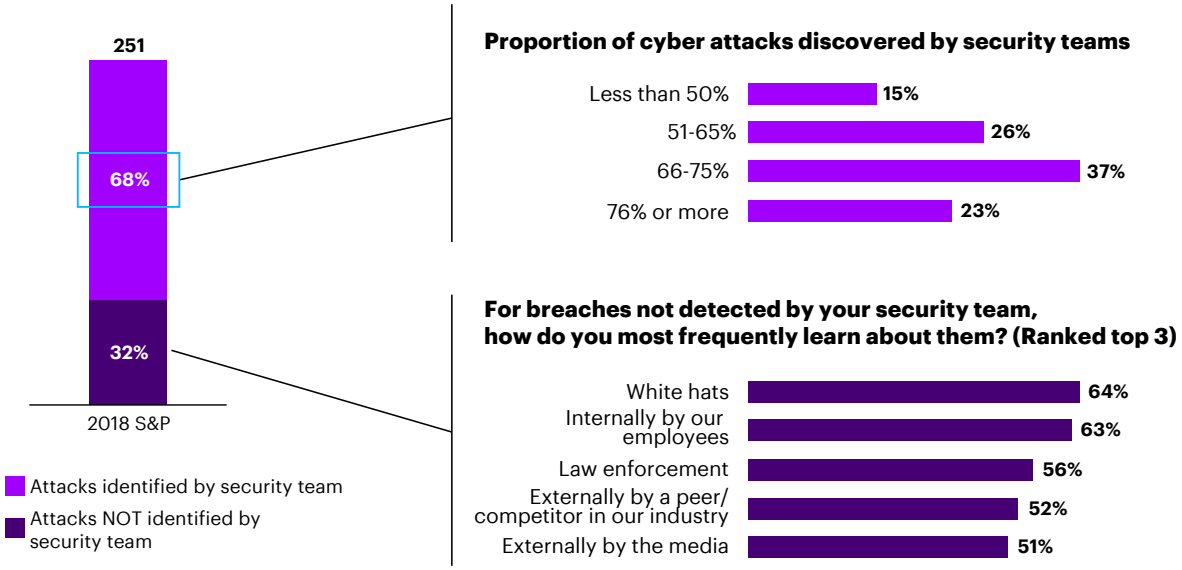


FIGURE 4: Room for improvement as companies face 2-3 security breaches per month



Despite the rising pressure of targeted cyber attacks, security teams at Software & Platforms companies continue to identify around two-thirds or 68 percent of all breach attempts on average (see Figure 5). However, this masks a divergence in performance among organizations. 23 percent of respondents were in the top category, i.e., able to identify between 76 percent and 100 percent of breach attempts, while 15 percent of respondents fell into the lowest category able to identify less than half of all breach attempts. So, while many organizations are performing well, some are clearly struggling with the increased pressure of attacks.

FIGURE 5: Software & Platforms security teams discovered on average 68% of breach attempts and get most help identifying the rest of the attempts from white hats, internal employees and law enforcement



Of course, security teams are not always the first to know about attacks. The insidious nature of cybercrime means that there are continually evolving ways to infiltrate an organization. But more collaboration is taking place for the attacks that security teams do not identify. When the survey asked how Software & Platforms companies learn about breaches undetected by their security teams, 64 percent said from white hats, 63 percent from their own employees and 56 percent said from law enforcement (see Figure 5). Such collaboration and threat information sharing is positive and needs to grow further as there is safety in numbers when defending against cyber attacks.

Cybersecurity budget approved by C-level and on the rise

Of those surveyed, 67 percent say their Board, CEO or Executive Committee authorizes their cybersecurity spend compared to the global average of 59 percent (see Figure 6). Consequently, budget authorization rests at the highest levels of companies.

This elevated status of cyber resilience within the business is helping to fuel improvements. Security spending reached 20 percent of the IT budget in Software & Platforms companies (see Figure 7).

FIGURE 6: 67% say their Board, CEO or Executive Committee authorizes their cybersecurity budget

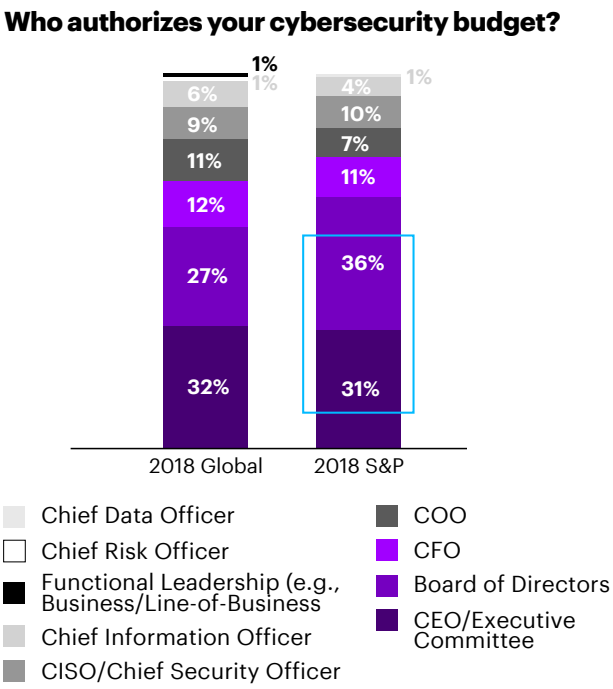
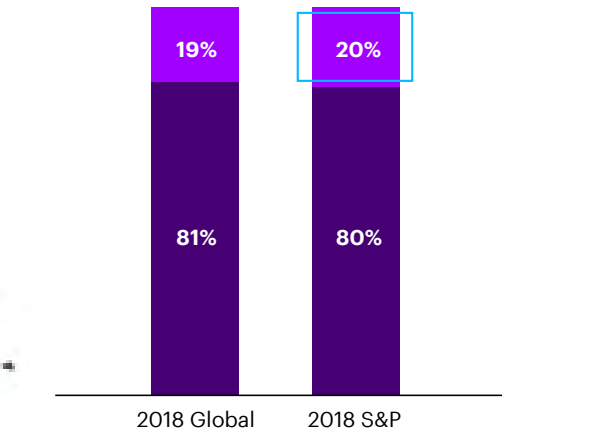
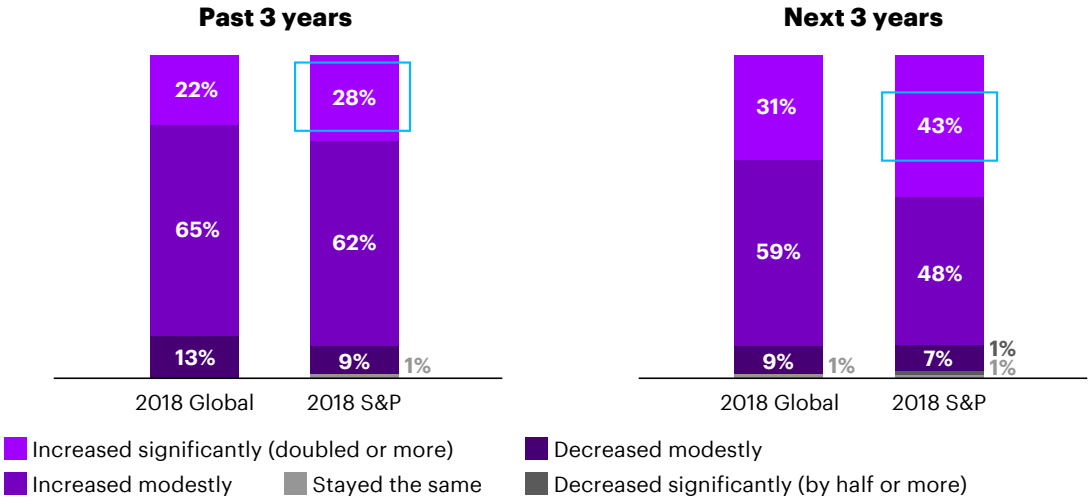


FIGURE 7: Software & Platforms companies spend 20% of their IT budget on cybersecurity



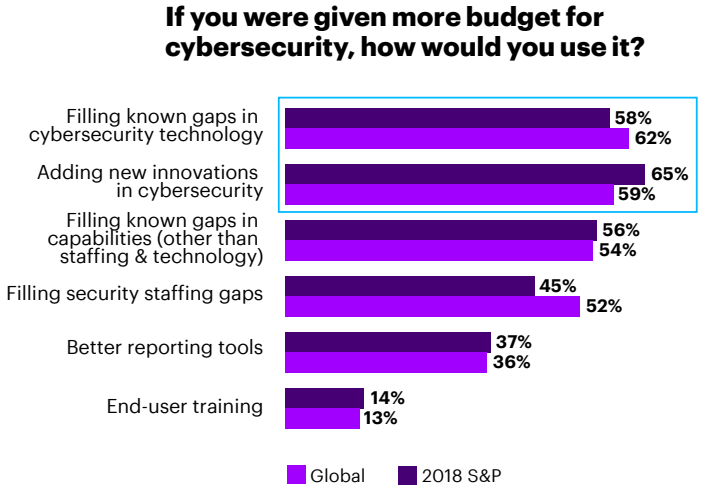
The general outlook for investment is positive with 90 percent of Software & Platforms respondents expecting their organization's overall investment in cybersecurity to stay the same or increase in the next three years (see Figure 8). At the same time, only 43 percent of them expect that increased investment to be significant (double or more)—hardly a fast-track to embedding security into the fabric of the organization. This, however, is still an increase compared to the 28 percent who claim they have significantly increased their cybersecurity budget over the past three years.

FIGURE 8: 43% of Software & Platforms companies expect to increase their cybersecurity budget significantly over the next three years while only 28% claim to have done so in the past three years



Given the additional budget, Software & Platforms companies would invest in breakthrough technologies: 65 percent of respondents would spend it on adding innovations in cybersecurity and 58 percent would spend it on filling known gaps in cybersecurity technology, but only 14 percent would spend it on end-user training (see Figure 9).

FIGURE 9: With more budget, security investments would be directed toward technologies and innovations over training



New technologies are important for the future

The evolution of digital technologies is a double-edged sword. It has been essential to organizations' success globally while increasing the risk of cyber threat. 89 percent of Software & Platforms respondents agree that the adoption of new innovative business models, ecosystems, liquid workforces, etc. can increase the attack surface and make organizations more vulnerable to the threat of cyber attacks (see Figure 10).

At the same time, the digital technologies that created market disruption and spawned the next wave of successful cyber attacks are also proving to be part of the solution to tackling cybersecurity. Our research shows that 90 percent of Software & Platforms respondents believe that breakthrough technologies, such as artificial intelligence (AI), machine or deep learning, user behavior analytics, and blockchain are essential to securing the future of their organizations (see Figure 11).

FIGURE 10: As companies adopt new innovative business models, ecosystems, liquid workforce, etc., the risk and security attack surface area increases exponentially

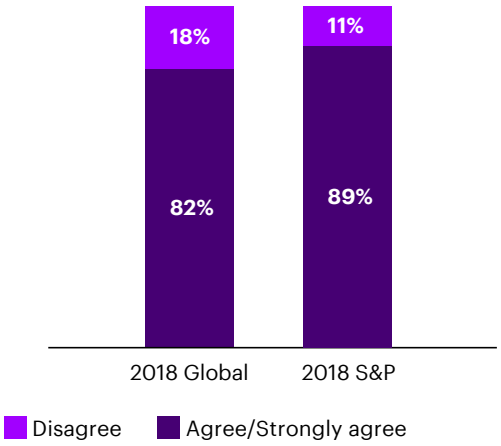
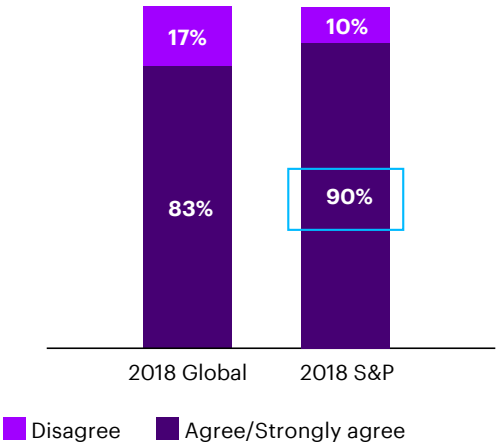
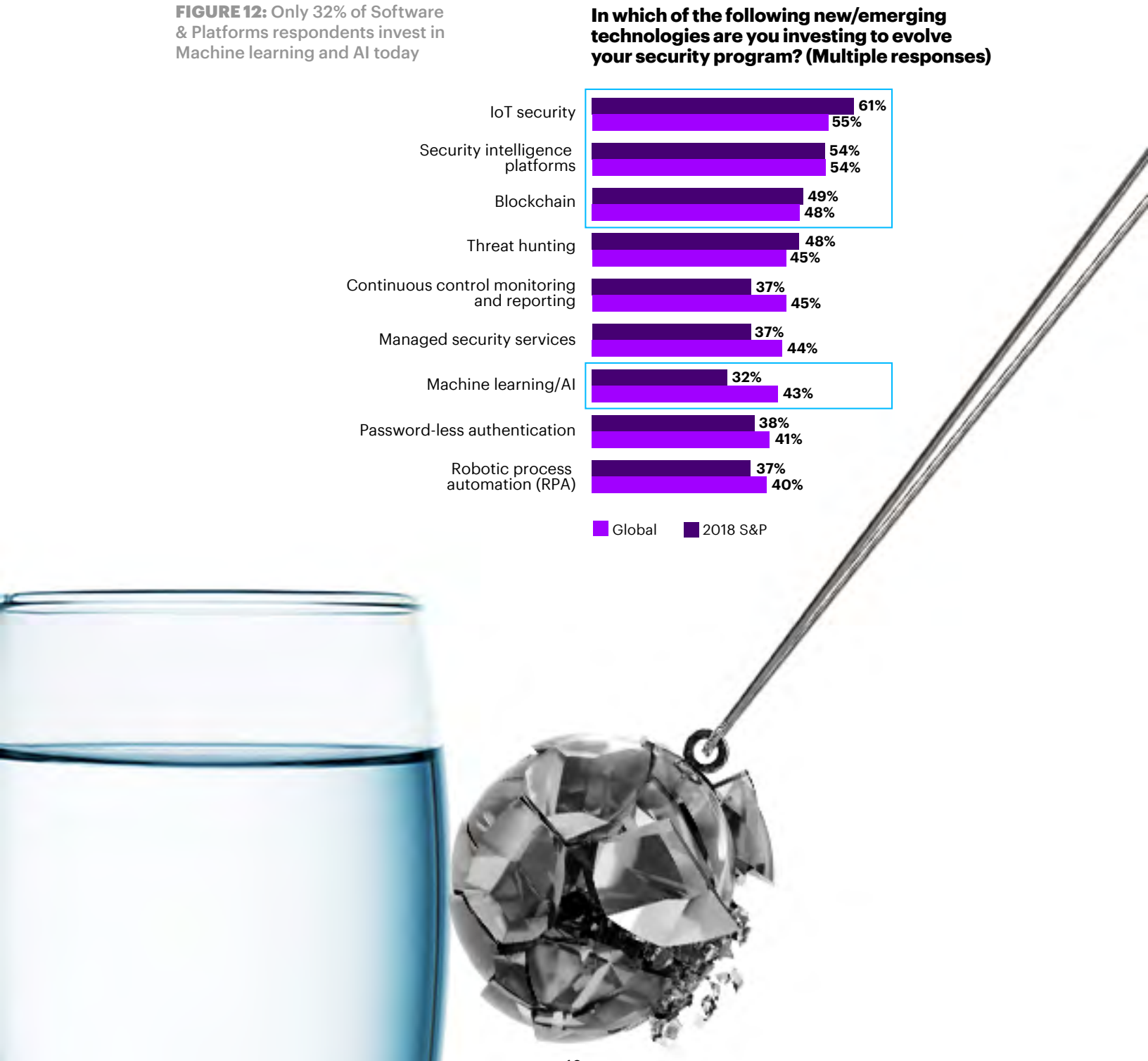


FIGURE 11: New technologies as AI, machine / deep learning, user behavior analytics, blockchain, etc. are essential to securing the future of the organization



Indeed, it is breakthrough technologies that will drive the next round of cyber resilience—although only one in three (or around 32 percent) of Software & Platforms business leaders are already investing in areas like machine learning/AI and automation as most of them instead invest in IoT security, security intelligence platforms and blockchain (see Figure 12).

FIGURE 12: Only 32% of Software & Platforms respondents invest in Machine learning and AI today

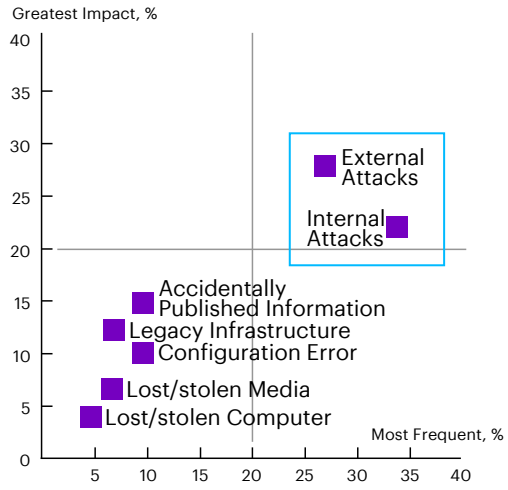


Both internal and external focus needed

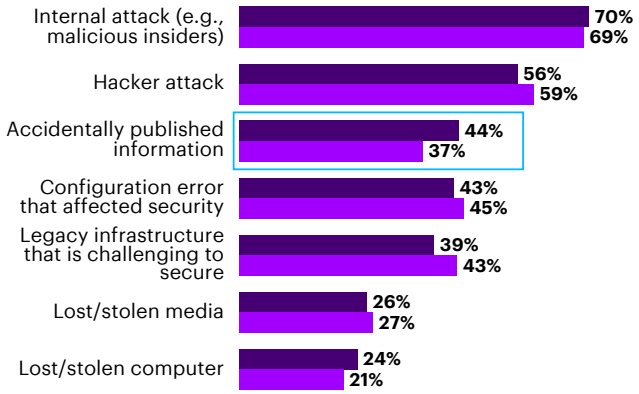
In terms of delivering the next wave of improvements, it is easy to focus exclusively on counteracting external attacks, but organizations should not neglect the enemy within. When looking at the incidents security teams fail to prevent, the top two attacks with the greatest impact are external attacks, such as hackers, and internal attacks, such as malicious insiders (see Figure 13). Furthermore, these two types of attacks are also the most frequent ones according to respondents. This serves as a timely reminder for organizations to protect themselves from the inside out against the equally damaging threats of internal and external attacks.

FIGURE 13: External attacks, such as hackers, and internal attacks, such as malicious insiders, are both the most frequent attacks and those with the greatest impact

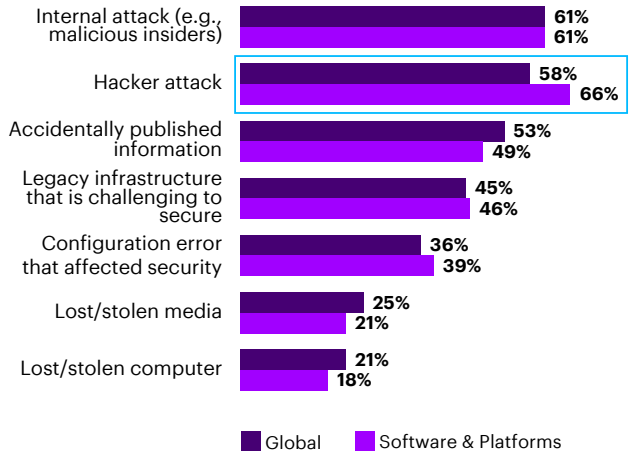
Most damaging breaches ranked by frequency & impact



Among the types of breaches your organization has experienced, please rank them from most to least frequent (Ranked top 3)



Among the successful breaches, please indicate which of the following causes had the greatest impact



On average, Software & Platforms respondents said a cybersecurity program does not protect one-quarter (27 percent) of their organization (see Figure 14), including corporate IT and the systems in the corporate office. Protection of third parties ranked lowest of all at only 36 percent.

Cybersecurity performance should also extend beyond the organizations' own four walls, but for many organizations, they are only as good as their weakest link. Subsidiary and third-party risk is top of mind, especially when 41 percent of Software & Platforms companies do not apply the same or higher cybersecurity standards to their extended ecosystem of partners as they apply to their own business (see Figure 15).

Consequently, Software & Platforms companies must do more to put the basics of cybersecurity in place to protect their most valuable assets—from the inside out—across their entire industry value chain.

FIGURE 14: On average, one-quarter of a Software & Platforms company is not protected by a cybersecurity program

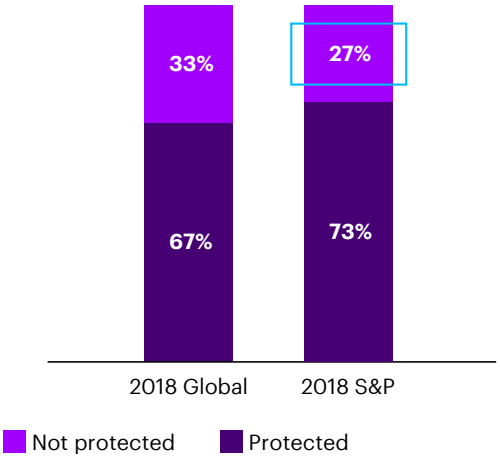
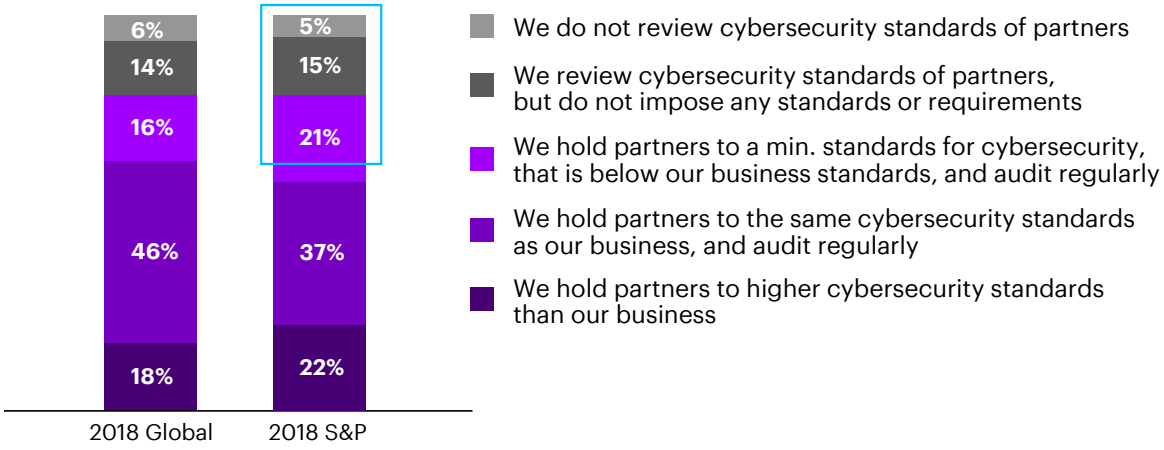


FIGURE 15: 41% of Software & Platforms companies do not apply the same or higher cybersecurity standards to their partners as to their own business

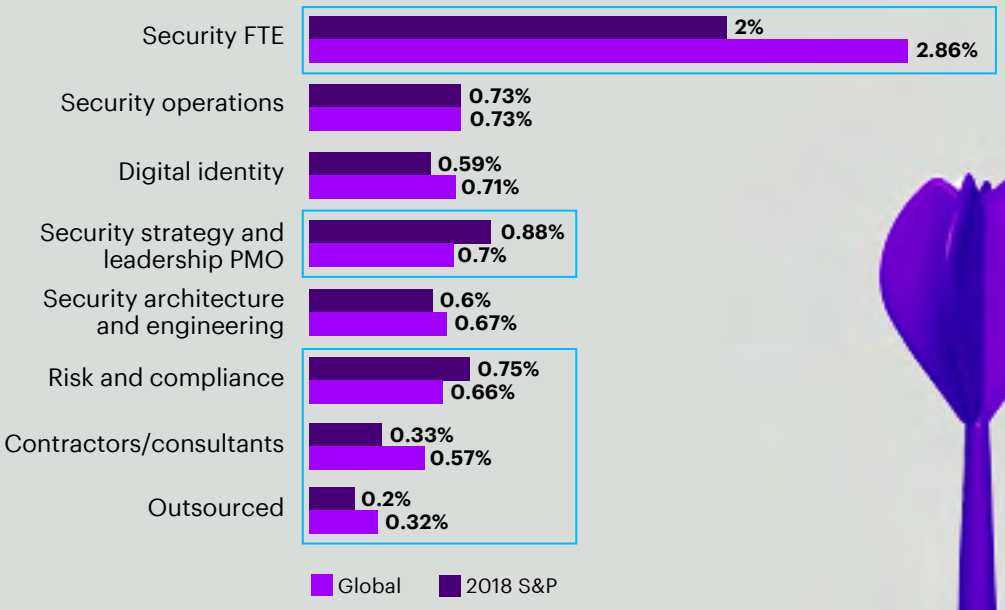
Which of the following best represents the degree to which you hold your ecosystem partners/strategic partners to cybersecurity standards?



2% of FTEs work with security at Software & Platforms companies

Organizations rely on their internal security workforce but also supplement it with contractors and outsourced staff. Software & Platforms companies have less of their total headcount, around 2 percent, work with security compared to the global average of almost 3 percent. At the same time, Software & Platforms companies have more employees working with "Security Strategy and Leadership" PMO and "Security Architecture and Engineering". On the other hand, Software & Platforms companies have fewer contractors and consultants, as well as fewer outsourced FTEs than the global average (see Figure 16).

FIGURE 16: Share of various internal security FTE, contractors/consultants and outsourced FTE as a percentage of total FTE

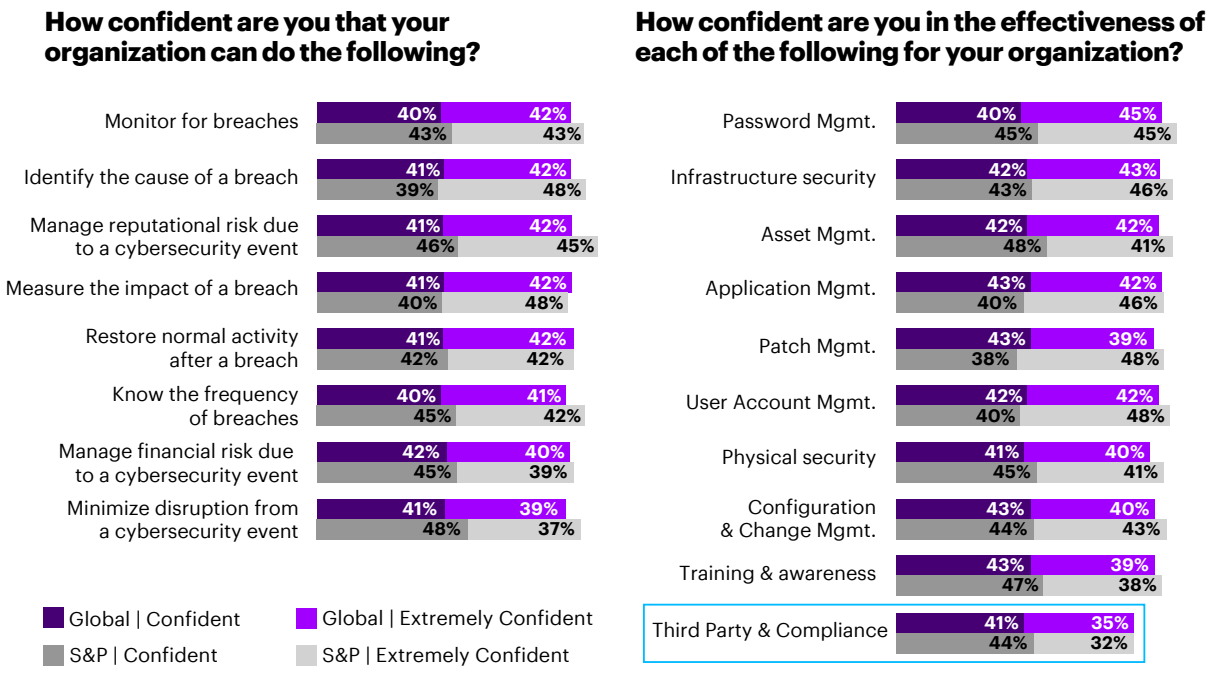


Software & Platforms companies rate themselves the least effective in Third Party & Compliance

Confidence is high amongst Software & Platforms respondents on all capabilities we asked them about. For example, 86 percent feel confident about their company's ability to monitor breaches, 87 percent feel confident about identifying the cause of a breach and 84 percent feel confident about restoring normal activity after a breach (see Figure 17).

Although confidence is also generally high amongst respondents in their organization's cybersecurity effectiveness, only 76 percent feel confident in their Third Party & Compliance-related effectiveness (see Figure 17).

FIGURE 17: Software & Platforms respondents feel least confident about their organization's effectiveness when it comes to Third Party & Compliance while they are generally confident about their cybersecurity capabilities and effectiveness



Five steps to cyber resilience

01

Build on a strong foundation: harden and protect your core assets. Important to identify the high-value assets of your company and then strengthen their security as Software & Platforms companies today do not protect on average a quarter of their organization with their cybersecurity program. Make sure to prepare for the worst and test those scenarios.

02

Pressure test your resilience: use coached incident simulation. As the red team / blue team model—where a red team is tasked with infiltrating your security system and a blue team is tasked with detecting it—has its limitations, we advise using a coached incident simulation, often referred to as purple teaming, which also uses threat intelligence and advanced adversary simulation techniques as well as coaching.

03

Employ breakthrough technologies: automate defenses. Use AI, big data analytics and machine learning to enable security teams to react and respond in nano- or milliseconds, not minutes, hours or days. Furthermore, implement multi-factor authentication, user behavior monitoring, AI-driven access provisioning and deprovisioning.

04

Use intelligence and data to be proactive: hunt threats. Use a data-driven approach and advanced threat intelligence to better anticipate potential attacks and develop a more proactive security posture for your business.

05

Evolve the role of the CISO. The next-generation CISO should be business adept and tech-savvy, someone who is equally at home in the boardroom as in the security operations center.

For more information, contact:

Kevin Collins
kevin.j.collins@accenture.com

Paul Johnson
paul.d.johnson@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 459,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**