Accenture Security

THE ACCENTURE SECURITY INDEX

REDEFINING SECURITY PERFORMANCE AND HOW TO ACHIEVE IT

by Kelly Bissell, Ryan LaSalle and Kevin Richards

REDEFINING SECURITY PERFORMANCE

It takes little more than a scan of the daily news to realize that cybersecurity is top of mind for business leaders and governments worldwide.

More than 70 percent of surveyed companies[1] confirmed that cybersecurity is a board-level concern supported by their highest-level executives, both financially and culturally. On average, organizations suffered two to three focused attacks that breached security each month; attacks they confirmed could take months or even years to detect.[2] This helps to explain why the protection of key digital assets and processes is on the C-suite agenda.

While the security performance of many organizations has improved over the last few years, the reality is that "the bad guys" have been getting better faster than companies are responding and, in the future, will likely do more damage than ever. Worldwide, organizations spent US$84 billion on cybersecurity in 2015; an amount that analysts expect to grow to US$125 billion by 2020.[3] A lot of money, but not when compared to the cost of cyberattacks, which some researchers believe could reach US$90 trillion by 2030.[4]

Consequently, leaders understand that it is not a matter of "if" but "when" they will face a serious security breach. The good news is that by taking proper measures, companies can substantially reduce the cybersecurity threat—but half measures will not do.

US$90tn

Potential cost of cyberattacks by 2030.

EMBRACING A NEW APPROACH

The current cybersecurity market is extremely fragmented, filled with many organizations focused on a wide array of "point solutions," none of which have meaningfully thwarted the growing number of attacks. Point solutions often prove effective for a specific application but at the enterprise level, they ultimately resemble attempts to plug individual holes in a sieve. This piecemeal approach, coupled with the high number of serious attacks organizations now endure and the extended length of time required to detect them, points to the need for a new attitude toward managing cybersecurity.

With the rise of the digital economy, companies can no longer remain safe within their corporate "walls." So instead of wasting time and resources attempting to "plug the sieve" with exterior defenses, companies need to develop a holistic cybersecurity strategy that protects the organization's most important assets from the inside out—and safeguards the enterprise across the entire industry value chain, such as from raw materials to consumption.

Executives should focus on business-aligned objectives, such as protecting the way their organization makes money and preventing financial losses that are specific to their operations. The goal is to imbue organizations, their extended ecosystems and their customers, with the confidence to drive their business forward and grow in a safe and secure environment. To that end, business leaders need to understand what higher levels of security performance looks like for them to be confident that they have taken the proper steps to protect themselves.

With the rise of the digital economy, **companies can no longer remain safe within their corporate "walls."**

BENCHMARKING PERFORMANCE

Defining high-performing security is not a simple task.

Companies can measure successful security outcomes, such as reductions in the number of breaches caused by targeted attacks, or the number of times fraud is committed against them, but defining high performance objectively requires a much broader view of capabilities. Using a comprehensive model, Accenture has assessed performance across 33 cybersecurity capabilities to help business leaders understand the current effectiveness of security measures both at a country level and globally across industries. The range of these cybersecurity capabilities is much broader and the focus more business-oriented than the typical audits or compliance tick-lists familiar to most organizations.

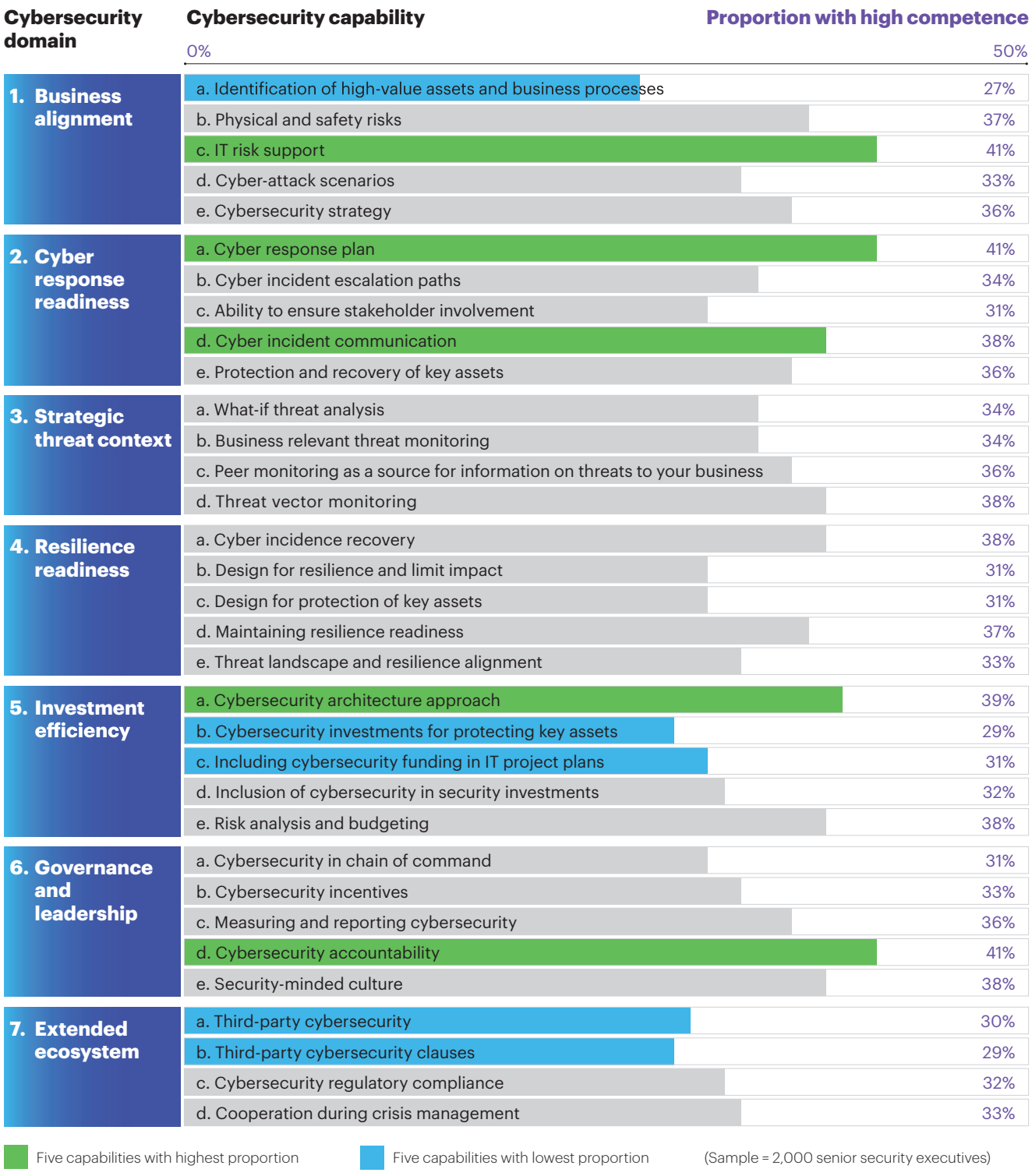
To capture a clear, objective measure of performance, the survey defined specific criteria to characterize three levels of competence: no or limited, average, or high. For example, one of the most important aspects of protecting any organization is the ability to identify high-value assets and processes in the business (Figure 1).

Figure 1. Example of defining performance levels for cybersecurity capabilities

Performance level	Performance criteria for the ability to identify high-value assets and processes in the business
No/limited competence	Organization fails to identify key assets and processes consistently.
Average competence	The company identifies key assets and processes, and regularly reviews their impact on security. Company policy also enforces the identification of key assets and processes across business units, and several new initiatives consider their potential impact on the organization's security strategy.
High competence	At this level, all new initiatives consider the potential impact on security. Critical cybersecurity trends automatically trigger reviews and the company ensures that it spreads awareness regarding key assets and processes throughout the organization. It also regularly reviews and improves the company policy.

By defining performance levels, senior security executives gain a clear measure of competence they can use to objectively rate the performance of their organizations for each cybersecurity capability (Figure 2).

Figure 2. The proportion of companies with high-performing cybersecurity capabilities



CYBERSECURITY WEAKNESSES

When asked about their cybersecurity strategies, business and government leaders worldwide may point to their budgets and the resources dedicated to protecting digital assets, and yet still feel unsure about the effectiveness of what they are doing.

Most also realize that throwing more money at the problem without understanding what good cybersecurity looks like can be a waste of time, resources and effort.

To provide the clarity companies need, we analyzed the responses from 2,000 senior security executives—with revenues in excess of US$1 billion—across 12 industries globally. The analysis defined ratings of high competence—against a specific set of criteria—as the benchmark for high performance in each cybersecurity capability.

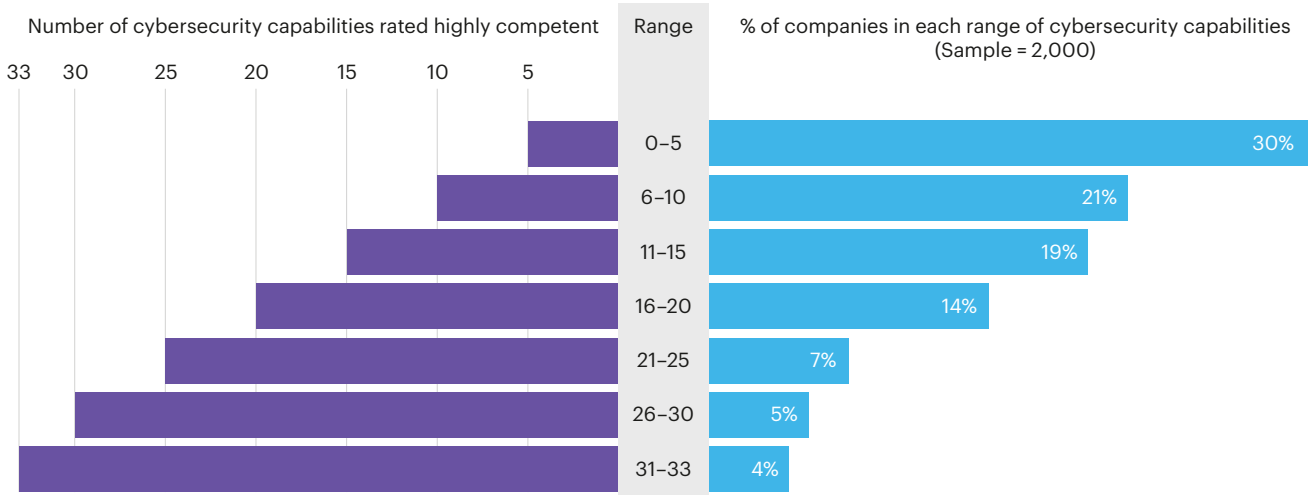
ROOM FOR IMPROVEMENT

At the global level, we found that, on average, senior security executives said their organization was highly competent in 11 of the 33 cybersecurity capabilities, suggesting significant room for improvement. At the top end of the scale, only 9 percent of organizations managed to achieve high competence in more than 25 of the 33 cybersecurity capabilities. Yet, at the other end of the scale, 30 percent of security executives said their organization had competent performance in, at most, five cybersecurity capabilities (Figure 3).

Of particular concern, the 'identification of high-value assets and business processes' and 'cybersecurity investments for key assets' were two of the lowest performing cybersecurity capabilities (27 percent and 29 percent respectively). This outcome appears related to the concept of business interlock—or the lack of it. For example, only 31 percent of organizations expressed high competence in the 'ability to ensure stakeholder involvement'. If the cybersecurity team does not engage fully with the business or really understand the business, it cannot realistically assess value.

With the rapidly expanding digital economy, many organizations should also consider addressing any weaknesses in protecting their extended business ecosystem where 'third-party cybersecurity' (30 percent) and agreeing active defense policies across business partners through 'third-party cybersecurity clauses' in contracts (29 percent) were among the five capabilities with the lowest proportion of competent performance (Figure 2). As extended ecosystems constantly change and grow, organizations must be able to adapt and re-align themselves to protect business priorities as they evolve.

Figure 3. Proportion of respondents in each range of cybersecurity capabilities rated highly competent



Source: Accenture Security and Oxford Economics

INDUSTRY PERFORMANCE

Industry-level performance includes a surprising degree of variation. Communications (45 percent), Banking & Capital Markets (44 percent) and High Technology respondents (44 percent) performed with higher levels of competence, with Life Sciences companies at the opposite end of the performance spectrum with a score of 19 percent (Figure 4).

Across all industries, Communications companies had the highest performance in 11 capabilities including the 'protection and recovery of key assets' (49 percent) and 'monitoring for business-relevant threats' (47 percent).

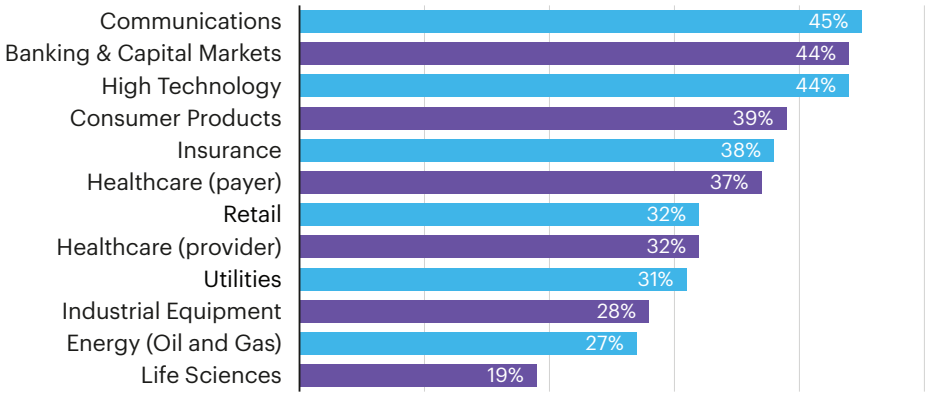
Banking organizations came second overall with a high rating in eight capabilities including "what-if" threat analysis (47 percent) and 'third-party cybersecurity' capabilities to help protect their extended business ecosystem (44 percent).

High technology companies came next in the rankings, with top scores in seven capabilities including the ability to 'create a security-minded culture' (54 percent) and 'recovering from cyber incidents' (48 percent).

Life Sciences organizations brought up the rear with an overall ranking of only 19 percent, with organizations exhibiting competence performance in only six capabilities on average. Life Sciences also ranked lowest in all but one of the 33 cybersecurity capabilities including the ability to 'ensure stakeholder involvement' (12 percent) and 'design for the protection of key assets' (13 percent).

Communications companies had the highest performance in **11 capabilities**.

Figure 4. Security Index Score by Industry
(% Share of high-performance security capabilities)



Source: Accenture Security and Oxford Economics

COUNTRY PERFORMANCE

The same variation emerges in country-level performance. The United Kingdom tops the country index along with France, as organizations in both countries have high competence in 15 out of 33 cybersecurity capabilities on average, compared with, for example, only nine out of 33 for a typical German company.

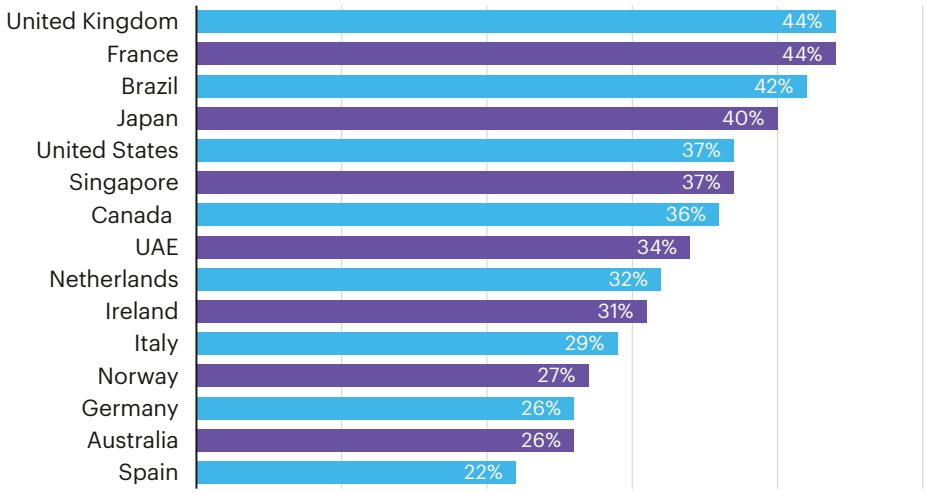
Compared with other countries, the UK ranked well in all capabilities and came top in 11 of them, including 'communication of cyber incidents' as part of business alignment (55 percent), 'cooperation during crisis management with third-parties' (52 percent) and 'measuring and reporting cybersecurity' (50 percent).

France also compared well with other countries and actually came top in 12 of the cybersecurity capabilities. This included the highest rating (40 percent) for the 'identification of high-value assets and business processes' and was joint-top with Japan for 'business-relevant threat monitoring' (44 percent). Both important capabilities for protecting organizations against cyber threats.

UK

came top in **11 out of 33** security capabilities.

Figure 5. Security Index Score by Country
(% Share of high-performance security capabilities)



Source: Accenture Security and Oxford Economics

The United States is fifth on the list, with the typical company having high competence in 12 of the 33 cybersecurity capabilities—slightly above the global average of 11. In line with its overall ranking, the US has average performance across the cybersecurity capabilities with the exception of governance and leadership where it ranked second overall—behind the UK—in 'creating a security-minded culture' (53 percent) and protecting the extended ecosystem with 'cooperation during crisis management with third-parties' (42 percent).

In contrast, Spain ranks at the bottom of the performance list with companies claiming competent performance in only 21 percent—or seven of 33 cybersecurity capabilities. Compared with the other countries, Spain was in the unfortunate position of being below average performance in all 33 capabilities (Figure 5).

ABOUT THE RESEARCH

Accenture Security surveyed 2,000 executives from 12 industries and 15 countries across North and South America, Europe and Asia Pacific. The survey objective was to understand the extent to which companies prioritize security, how comprehensive security plans are, how resilient companies are with regard to security, and the level of spend for security. The survey aimed to measure performance across 33 cybersecurity capabilities classified into seven cybersecurity domains: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem. More than 60 percent of respondents were senior security executives at director level and above with responsibility for cybersecurity strategy and spending at companies with revenues of US$1 billion or more.

For further information please visit:
www.accenture.com/cybersecurityreport

IMPROVING CYBERSECURITY

With organizations achieving competent levels of performance in only 11 out of 33 cybersecurity capabilities, many businesses may need to reassess their approach to cybersecurity and consider how they can improve their levels of performance in key areas of cybersecurity protection.

To build business confidence and drive secure growth, organizations can address areas of poor performance in key capabilities and reboot their approach to cybersecurity by following six key recommendations.

1. DEFINE CYBERSECURITY SUCCESS FOR THE ORGANIZATION

Barely one in three senior security executives we surveyed—34 percent—said their enterprise is sufficiently competent at `business-relevant threat monitoring'. However, another worrying statistic involves the cybersecurity capability with the lowest rank of all—the ability to identify the business's high-value assets and processes. Only 27 percent of organizations globally are highly competent in this area. This outcome appears related to the concept of business interlock (or the lack of it)—if the cybersecurity team does not really understand the business, it cannot realistically assess value. Associated with this finding, the third lowest-performing capability is the ability to invest in cybersecurity to protect key assets. In this case, low-end performance means that investments in cybersecurity do not consistently focus on high-value assets or processes.

To successfully define what good looks like in cybersecurity, organizations must:

- Improve the alignment of the company's cybersecurity strategy with its business imperatives, and enhance abilities to detect and repel more advanced attacks.
- Reframe cybersecurity perceptions and build a new definition of success based on business impact and using mitigated financial loss as a key metric.

27%

Competent in identifying high-value assets and processes in the business.

2. PRESSURE TEST SECURITY CAPABILITIES

Attack simulations help to build "muscle response" within the organization when its resilience is tested. Yet only one in three organizations (33 percent) are highly competent at defining cyber-attack scenarios that evolve with the changing threat landscape and have board-level involvement in their planning and execution.

To successfully pressure test security capabilities, organizations must:

- Engage in real-world attack simulations to establish a realistic assessment of internal capabilities in withstanding a targeted, focused attack. Similar in effect to military live-fire training programs, organizations can have benign external hackers engage in a real "sparring match" with their cybersecurity teams to assess preparedness and response effectiveness.
- Engage the CEO and board. There may be no better way to establish the business relevance of cybersecurity than to include them in cybersecurity crisis drills, simulations and exercises. Leadership will experience first-hand exactly what can go wrong, how bad the situation can be and their precise role in leading the company through the crisis.

3. PROTECT FROM THE INSIDE OUT

With the growth of the digital economy, businesses increasingly operate in an extended ecosystem that is becoming more complex, collaborative and networked. As the security footprint extends beyond the traditional boundaries of an organization, the business is exposed to even greater threats. One key area of concern involves the cybersecurity capabilities related to the extended ecosystem of suppliers, vendors and partners with which businesses increasingly interact. Our research reveals that the extended ecosystem cybersecurity domain sees the third and fourth lowest performing capabilities, with only 31 percent of organizations demonstrating competence or high competence in this area. Experience suggests that banks and government agencies have a head start with their third-party risk programs, but as approaches continue to evolve, opportunities for other players to leapfrog their progress continue to emerge.

Only 31%

demonstrate sufficient competence in protecting the extended business ecosystem.

To successfully protect from the inside out, organizations must:

- Prioritize the protection of key assets
- Focus on those internal incursions with greatest potential impact. Instead of attempting to anticipate a seemingly infinite variety of external breach possibilities, organizations can concentrate on the relatively fewer internal incursions that really matter.

4. KEEP INNOVATING

Despite their current subpar performance levels, the majority of organizations globally, given extra budget, would spend it on the same things they are doing now. Hardly a strong foundation for protecting the business in a rapidly evolving threat landscape. Especially when cybersecurity investment to protect key assets is the second poorest performing capability (29 percent) overall.

Anticipating future attacks through strategic threat intelligence was equally poor with barely one-third of organizations (34 percent) highly competent at developing and evaluating advanced threat scenarios through "what-if" analysis.

To keep innovating successfully, organizations must:

- Invest in state-of-the-art programs that enable the company to outmaneuver adversaries instead of spending more on existing programs.
- Refuse to stand still when it comes to cybersecurity; organizations need to innovate continually to stay ahead of potential attackers.

5. MAKE SECURITY EVERYONE'S JOB

On average, internal security teams discover only 65 percent of effective breaches, and 52 percent of global companies say their employees most often find breaches not detected by security team members. Fortunately, creating an environment where cybersecurity is embedded throughout the culture of an organization—with management demonstrating an understanding of cybersecurity threats and promoting cybersecurity as a key priority—is one of the higher performing capabilities on average (38 percent). Unfortunately, given extra budget, only 17 percent of organizations worldwide would invest in cybersecurity training, which could have an outsized impact on cybersecurity, given the roles employees play both formally and informally.

52%

of breaches not detected by security teams are discovered by employees.

To successfully make security everyone's job, organizations must:

- Prioritize training for all employees. Employees play a critical role in detecting and potentially preventing breaches, so represent a company's first line of defense. Appropriate training (for example, role-based training or instruction tied to their job functions) can pay disproportionate dividends.

6. LEAD FROM THE TOP

Globally, businesses do better when it comes to defining and managing cybersecurity accountability. Two out of five organizations (41 percent) feel they are competent or highly competent in this area—they have developed cybersecurity key performance indicators (KPIs) for M&As and other initiatives, have defined roles and responsibilities for cybersecurity, and collaborate across business units and subsidiaries on security. They also include cybersecurity in executive job descriptions across the organization, and regularly review and improve the process.

Less effective is the ability to ensure stakeholder involvement where only 31 percent feel their cyber response readiness is adequately developed, including pre-defined interactions between all main players during a cyber incident. While these examples highlight some areas with higher levels of competence, the overriding message concerns the potential for broad improvement across the organization.

To successfully lead from the top, organizations must:

- Help CISOs materially engage with enterprise leadership and make the case that cybersecurity is a critical priority in protecting company value.
- Encourage the unified leadership team to effectively communicate the issues to the rest of the company.

2 in 5

organizations feel they are highly competent in preparing and coordinating cyber response plans.

By embracing these steps, organizations can improve their cybersecurity capabilities and position their businesses to thrive, despite the rising cybersecurity threats.

GROWING CONFIDENCE

In a world of rising risk—where the threat landscape is evolving rapidly and organizations are subject to increasing levels of attack—it is time for organizations to consider a new approach to cybersecurity. One that evaluates a much broader range of cybersecurity capabilities across the business, using clearly defined criteria, to provide a new benchmark for cybersecurity success.

Based on current evidence, most companies could benefit from improving their performance levels across a wide range of cybersecurity capabilities. Nearly one-third of senior security executives (30 percent) confirm their organizations have adequate levels of competence in only one to five of the 33 capabilities assessed by the Accenture Security Index. By contrast, at the other end of the spectrum, barely 4 percent from our sample of 2,000 organizations had high levels of competence in 30 or more capabilities.

Once senior security executives and business leaders clearly understand where they need higher levels of cybersecurity performance, they can take the proper steps to protect the key assets and processes on which their success depends with greater certainty. And in doing so, they will help to create the environment and build the confidence needed for their business to grow securely.

CONTACT THE AUTHORS

Kelly Bissell
Global managing director, Accenture Security
kelly.bissell@accenture.com

Ryan M. LaSalle
Global managing director, Accenture Security—Growth & Strategy
ryan.m.lasalle@accenture.com

Kevin Richards
Global managing director, Accenture Security—Strategy & Risk
k.richards@accenture.com

REFERENCES

1 Accenture High Performance Security Research, August 2016.

2 Ibid.

3 Mega-Rounds to Cybersecurity Help Push Funding to New High In 2015, *CB Insights*. January 27, 2016

4 Atlantic Council and the Zurich Insurance, *Risk Nexus*, 2015

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 approximately 394,000 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.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.