THIRD ANNUAL STATE OF CYBER RESILIENCE

accenturesecurity

INNOVATE FOR CYBER RESILIENCE

LESSONS FROM LEADERS TO MASTER CYBERSECURITY EXECUTION

CONTENTS

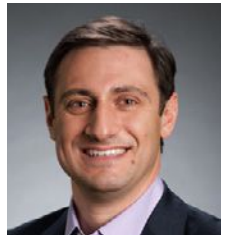
ABOUT THE AUTHORS

KELLY BISSELL
GLOBAL LEAD–
ACCENTURE SECURITY

kelly.bissell@accenture.com

Kelly leads the Accenture Security business globally. With more than 25 years of security industry experience, Kelly specializes in breach incident response, identity management, privacy and data protection, secure software development, and cyber risk management. His role as the Accenture Security lead spans strategic consulting, proactive risk management and digital identity to cyber defense, response and remediation services, and managed security services—across all industries. Kelly is also affiliated to OASIS, a non-profit consortium that drives the development, convergence, and adoption of open standards for the global information society.

Twitter: https://twitter.com/ckellybissell



RYAN M. LASALLE
MANAGING DIRECTOR–
ACCENTURE SECURITY

ryan.m.lasalle@accenture.com

Ryan leads the North America practice for Accenture Security. He is responsible for nurturing the talented teams that bring transformative solutions to better defend and protect our clients. Over the course of nearly two decades, He has worked with Accenture clients in the commercial, non-profit and public sectors helping them identify and implement emerging technology solutions to meet their business needs. Ryan is a Ponemon Institute Fellow and is active with the Greater Washington Board of Trade.

Twitter: https://twitter.com/Labsguy

PAOLO DAL CIN
MANAGING DIRECTOR–
ACCENTURE SECURITY

paolo.dal.cin@accenture.com

Paolo leads the Europe and Latin America practice for Accenture Security. He has 20 years of experience leading complex projects for Accenture clients. He is an expert in security strategy, business resilience, cyber defense and offense, cloud protection, security analytics, threat intelligence, application security, data protection and managed security services. He has authored several articles on security and is a frequent speaker at security events. Paolo taught information and communication technology (ICT) security at the Universities of Udine, Modena and Milan.

Twitter: https://twitter.com/Paolo_DalCin

SECURE INNOVATION

At first glance, the basics of cybersecurity are improving and cyber resilience is on the rise. Our latest research shows that most organizations are getting better at preventing direct cyberattacks. But in the shape-shifting world of cybersecurity, attackers have already moved on to indirect targets, such as vendors and other third parties in the supply chain. It is a situation that creates new battlegrounds even before they have mastered the fight in their own back yard. At the same time, cybersecurity cost increases are reaching unsustainable levels and, despite the hefty price tags, security investments often fail to deliver. As a result, many organizations face a tipping point.

There is good news for organizations wondering if they will ever move beyond simply gaining ground on the cyber attacker. Our analysis reveals there is a group of standout organizations that appear to have cracked the cybersecurity code for innovation. Detailed modeling of cybersecurity performance has identified two distinct groups: the first an elite group—17 percent—that achieve significantly higher levels of performance compared to the rest. These organizations set the bar for innovation and achieve high-performing cyber resilience. The second is the group forming the vast majority of our sample—74 percent—who are average performers, but far from being laggards in cyber resilience. This second group has lessons to learn from our leaders while leaders, too, have further room for improvement.

Being innovative in security is different to any other aspect of the business. Caution is necessary. After all, a fail fast approach is not an option for security where attack vulnerabilities could be catastrophic. Growing investments in innovation illustrate organizations' commitment to prevention and damage limitation. And it is here that leaders excel. By focusing on the technologies that provide the greatest benefit and sustaining what they have, they are finding themselves moving fast and first in the race to cyber resilience.

What is one key to secure innovation? Leaders show us that they scale, train and collaborate more. So, while non-leaders measure their success by focusing on the destination—improved cyber resilience—the leaders focus on how to get there using warp speed to detect, mobilize and remediate.

In the **Accenture Third Annual State of Cyber Resilience report** we take a deep dive into what sets leaders apart. Based on our research among 4,644 executives and backed by our knowledge and deep industry expertise, our findings aim to help organizations innovate securely and build cyber resilience to help grow with confidence.

In this cybersecurity report, we show how organizations are coping with cybersecurity demands since our last analysis and explore what our large sample of non-leaders can do to master cybersecurity execution and drive innovation success.

AT A GLANCE

State of Cyber Resilience

Innovation investment is growing

Cybersecurity basics are better

BUT...

- There are hidden threats
- Costs are unsustainable
- Investments are failing

A group of leading organizations are doing things differently

4x better at stopping attacks

4x better at finding breaches faster

3x better at fixing breaches faster

2x better at reducing breach impact

HOW DO THEY DO IT?

Invest for operational speed

Drive value from new investments

Sustain what they have

What is cyber resilience?

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.

THE STATE OF CYBER RESILIENCE

Investment in innovation grows (p.8)

The number of leaders spending more than 20 percent of IT budgets on advanced technology investments has doubled in the last three years.

The basics seem better (p.9)

Direct attacks are down 11 percent over the last year and security breaches are down by 27 percent.

Progress masks hidden threats (p.10)

Indirect attacks against weak links in the supply chain now account for 40 percent of security breaches.

Unsustainable cost increases (p.12)

Sixty-nine percent say staying ahead of attackers is a constant battle and the cost is unsustainable.

Security investments are failing (p.14)

Failures lead to gaps in protection, lower detection rates, longer business impact and more customer data loss.

WHERE ARE WE NOW?

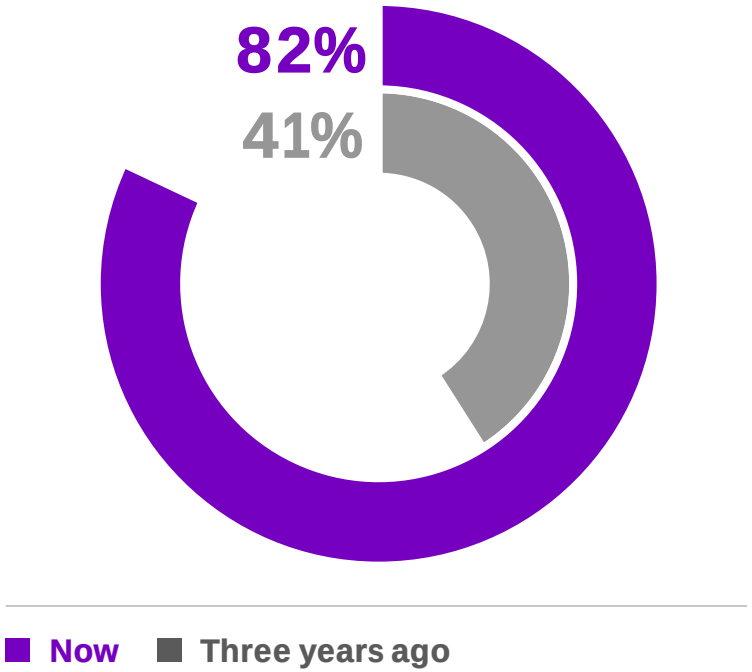
Investment in innovation grows

Increasingly, the online world has grown complex and threatening. Many organizations are finding it hard to reconcile the level of their cybersecurity innovation investments with the cyber resilience outcomes for their business. Even worse, choosing the wrong strategy to invest in cybersecurity technologies can cost the organization far more than wasted cash; it can damage an organization's brand, reputation, and future prosperity.

Both C-suite and security professionals should feel encouraged. Investment in innovation is increasing and managing the basics appears to be better. But scratch below the surface and there are hidden threats. Organizations face unsustainable costs, and security investments are often failing for the majority. With low detection rates and slow recovery times, it is important to find out what the leading organizations are doing differently to achieve cyber resilience.

The good news is that most organizations, on average, spend 10.9 percent of their IT budgets on cybersecurity programs. Leaders spend slightly more at 11.2 percent which is insufficient to account for their dramatically higher levels of performance. And their investments in advanced technologies, such as artificial intelligence, machine learning or robotic process automation, are rising substantially. Today, 84 percent of organizations spend more than 20 percent of their cybersecurity budgets on tools that use these three technologies as fundamental components. The finding represents a good step up from the 67 percent being spent three years ago. The increase is even more impressive with respect to the leaders. Three years ago, only 41 percent of leaders were spending more than 20 percent of their cybersecurity budgets on advanced technologies. Today, that has doubled, to 82 percent (Figure 1).

Figure 1. Percentage of leaders spending more than 20 percent of their IT budgets on advanced technology investments



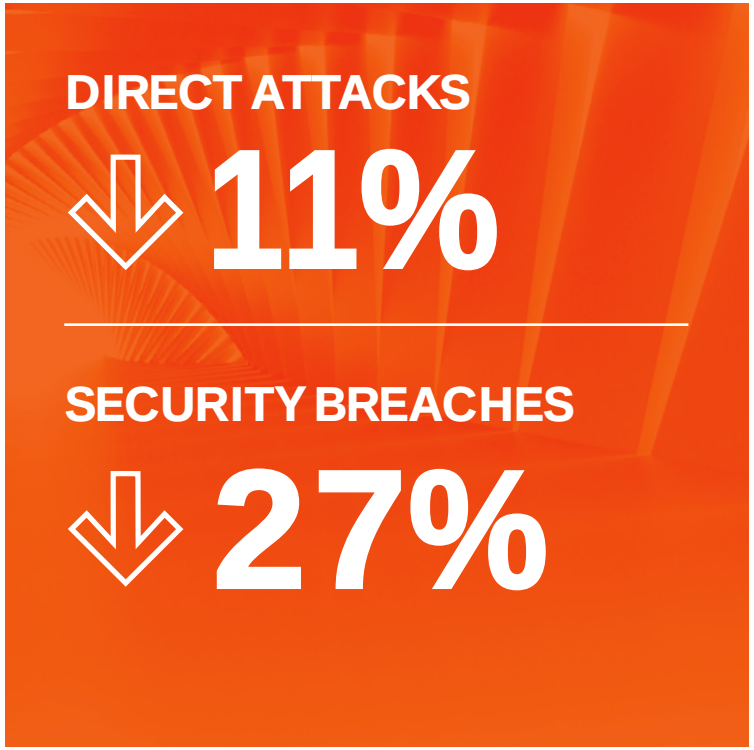
Source: Accenture Research; n=4,644

WHERE ARE WE NOW?

The basics seem better

The suggestion that organizations are making progress in cybersecurity is valid. In fact, more than four out of five respondents agreed that cybersecurity tools have advanced significantly over the past few years and are noticeably improving their organization's cyber resilience.

Improvements in basic security hygiene back up this finding. Being able to accurately assess the number of cyberattacks against an organization depends on the ability of each organization to detect them. On the other hand, security breaches are real events and likely to be more precisely recorded. With this in mind, cybersecurity teams across industries and geographies deserve recognition for the improved levels of cybersecurity protection over the past year. For example, the total number of cyberattacks dropped 11 percent, from 232 to 206 targeted attacks. At the same time, we have seen a larger drop of 27 percent in the number of security breaches which indicates the basics seem to be improving. On average, organizations now face 22 security breaches per year compared with 30 in the previous year.

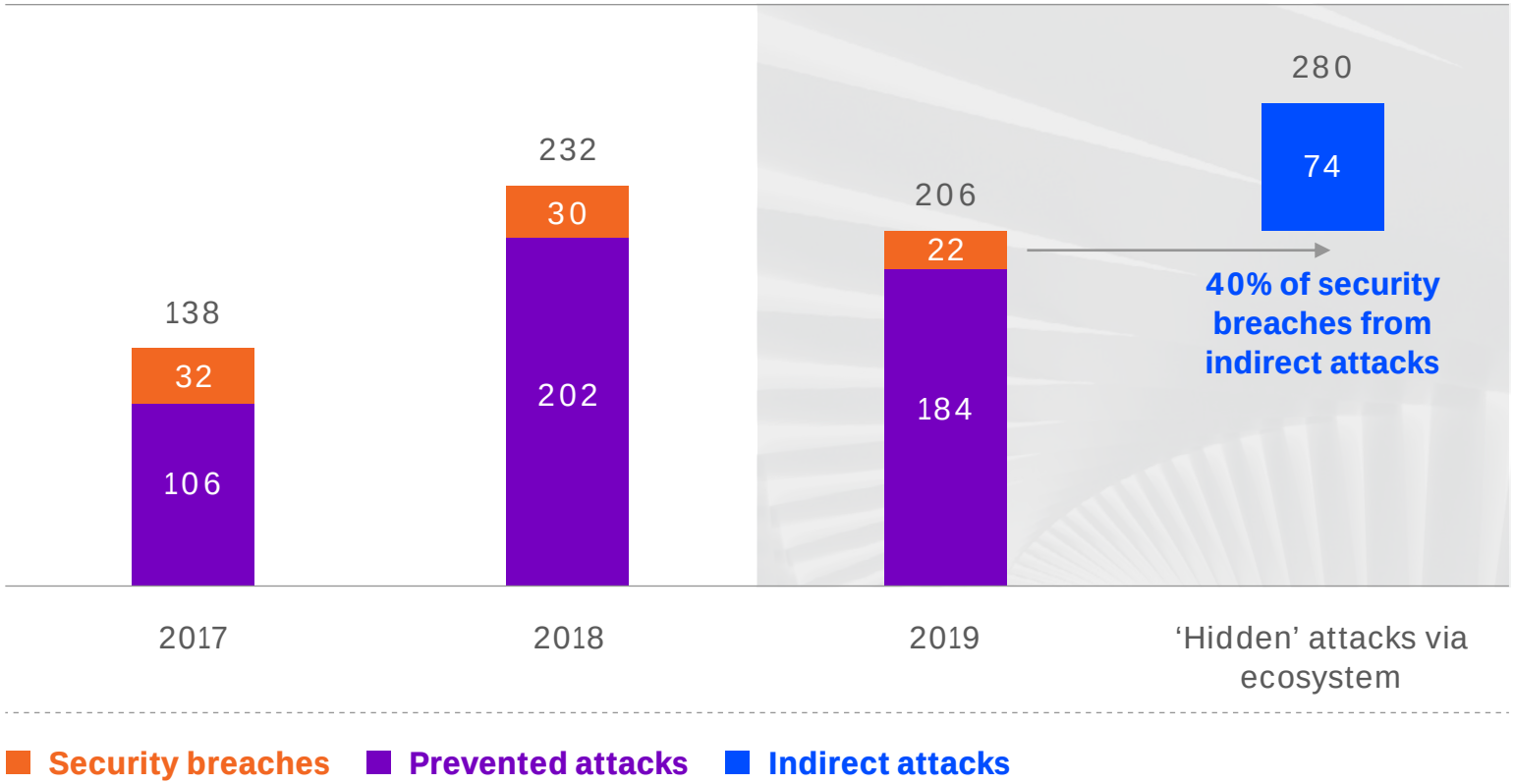


Progress masks hidden threats

A closer look at the sources of cyberattacks reveals 40 percent of security breaches are now indirect, as threat actors target the weak links in the supply chain or business ecosystem (Figure 2). This shift is blurring the true scale of cyberthreats. If we apply the same average number of security breaches to indirect cyberattacks, the total number—both direct and indirect—could jump to about 280, a potential increase of 20 percent over the prior year.

Organizations should look beyond their four walls to protect their business ecosystems and supply chains as well. On average, cybersecurity programs actively protect only about 60 percent of an organization's business ecosystem. That is an issue when 40 percent of breaches come via this route. In such an environment, few organizations have the luxury of standing still. Fully 83 percent of our respondents agreed that their organizations need to think beyond securing their enterprises and take steps to secure their ecosystems to be effective.

Figure 2. The danger of indirect attacks



Source: Accenture Research; n=4,644

Lock the front and back doors

As we have seen earlier, as soon as one breach avenue has been foiled, attackers are quick to find other means. With the growth in indirect attacks, the spotlight falls on protecting third parties and other partners. But there are enormous challenges in managing third-party cyber risks. Large volumes of data can overwhelm the teams responsible for managing compliance. The complexities of global supply chains, including the regulatory demands of various regions or countries, add to the strain. In our experience, many CISOs feel that the sizable number of vendors outstrips their capacity to monitor them.

Given finite security resources, there is value in a data-driven, business-focused, tiered-risk approach to secure the enterprise ecosystem. This may mean introducing managed services to help the organization tackle the wider scope and scale. By collaborating more broadly with others with the common goal of securing the enterprise and its ecosystem, organizations can not only play a responsible role in helping their smaller partners to beat cybercrime, but also they can be sure they are not bolting the front door from attackers while leaving the back door wide open.

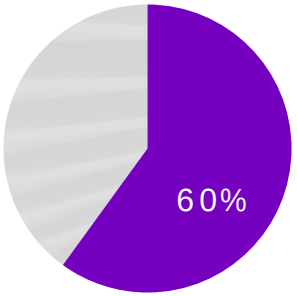
Unsustainable cost increases

Another threat is cost increases beginning to reach what many respondents consider unsustainable levels. Despite rising investments in new technologies for cybersecurity programs, our research highlights many areas where the cybersecurity technologies being purchased by this spending are failing.

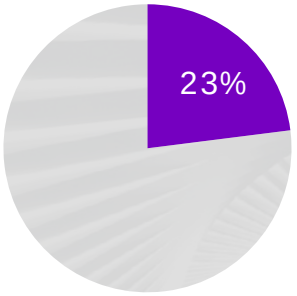
Looking at a broad range of 17 different components of cybersecurity protection, 60 percent of respondents reported cost increases on all 17 components over the last two years. A significant number, almost one quarter, reported cost increases of more than 25 percent a year across all 17 components. The three areas of cybersecurity protection with the largest increases in cost are network security, threat detection and security monitoring. Reflecting these trends, 69 percent of our respondents said staying ahead of attackers is a constant battle and the cost is unsustainable (Figure 3).

Figure 3. Cost increases across 17 components of cybersecurity protection over the last two years

Cost increases up to 25%



Cost increases more than 25%



SECURITY COMPONENTS RANKED BY BIGGEST COST INCREASES

1. Network security
2. Threat detection
3. Security monitoring
4. Cyber risk management
5. Firewalls
6. Threat intelligence
7. Application security
8. End-point detection and response
9. Incident response
10. Identity and access management
11. Vulnerability management
12. OT-related security
13. Privileged Access Management
14. Staffing (or People)
15. Remediation
16. Governance, Risk, and Compliance
17. SIEM and event consoles

Source: Accenture Research; n=4,644

How to help reduce the cost of a cyberattack

Cybersecurity is not an easy problem to solve for any business. As our research shows, just when one challenge has been met, another variable appears. But one of the areas where organizations can make a difference is in reducing cost—both in terms of the cybersecurity protection cost to the business and the wider economic impact. In short, they need to be clear what is at stake for average performance as well as measuring their existing investments.

Our research found that the current average cost per attack for non-leaders was US$380,000 per incident. If they could perform at the same level as leaders—that is, having the same proportion of attacks types and the same time to detect and fix responses as leaders—our detailed modeling indicates they could reduce the cost per attack by 72 percent (see About the Research, p.44). This is a potential saving of US$273,000 per security breach, reducing the average cost to US$107,000. With an average 22 incidents per year, this equates a potential saving of US$6 million per year for non-leaders.

Security investments are failing

More bad news is threatening organizations' cyber resilience in several areas and causing security investments to fail. Our research identifies serious gaps in protection, very low detection rates, much longer business impact and customer data being exposed. Yet, our leaders are, once again, proving the exception in many of these areas (Figure 4).

With only a little more than half of their organization covered by their cybersecurity programs, non-leaders are at risk of having many areas unprotected. This contrasts with leaders who are able to cover 85 percent of their organization with their cybersecurity programs. The difference reflects a substantial gap in protection between the two groups.

Figure 4. Comparison of failing security investments, leaders vs. non-leaders

FAILING INVESTMENTS	LEADERS (17%)	NON-LEADERS (74%)
Gaps in protection	**80% of organization is actively protected**	**55% of organization is actively protected**
Low detection rates	**83% of breaches found by security teams**	**54% of breaches found by security teams**
Longer breach impact	**55% say all breaches had an impact lasting more than 24 hours**	**97% say all breaches had an impact lasting more than 24 hours**
Customer data exposed	**15% had more than 500k records exposed in the last year**	**44% had more than 500k records exposed in the last year**

Source: Accenture Research; n=4,644

Building cyber resilience takes teamwork. Employees, third-party suppliers, alliance partners, law enforcement agencies and even competitors all have their parts to play. However, the first line of defense in an organization is the cybersecurity team. On average, our research shows the security teams of non-leaders discover 54 percent of cybersecurity breaches, while the security teams of leaders were able to find 83 percent. This level of detection enables leaders to respond quickly and start to fix security breaches sooner to reduce overall damage.

A failure to fully exploit advanced technology investments is also having an impact in terms of remediation. More than half of all security breaches (55 percent) for leaders had a business impact lasting more than 24 hours. For non-leaders, the figure was 93 percent. Reducing the impact on the organization to less than one day is a tough challenge, even for leaders, but this clearly is an area where non-leaders could improve their performance significantly.

Despite suffering from more frequent attempts to access customer records, only 15 percent of leaders have had more than 500,000 customer records exposed through cyberattacks in the last 12 months. But 44 percent of non-leaders admit that more than 500,000 customer records were exposed across all security breaches in the last year. The result is that 19 percent of non-leaders faced regulatory actions in the last 12 months compared with only 13 percent of leaders. Another outcome of this finding is that 19 percent of non-leaders faced financial penalties compared with only 9 percent of leaders. With potential fines in excess of US$100 million for violations of general data protection regulations (GDPR), regulatory fines may match, or even exceed, the overall cost of cybercrime for an organization.

WHY LEADERS ARE MORE CYBER RESILIENT

Stop more attacks (p.18)

4x

Leaders have nearly a fourfold advantage in stopping targeted cyberattacks.

Find breaches faster (p.20)

4x

Leaders have a fourfold advantage in detection speed.

Fix breaches faster (p.22)

3x

Leaders have nearly a threefold advantage in speed of remediation.

Reduce breach impact (p.24)

2x

Leaders have a twofold advantage in containing damage impact.

WHY LEADERS ARE MORE CYBER RESILIENT

Detailed modeling and statistical analysis of cybersecurity performance (see our methodology in "About the research" p.17) has identified a group of leaders that achieve significantly higher levels of performance compared with the non-leaders. The statistical analysis revealed that leaders were characterized as among the highest performers in at least three of the following four categories: stop more attacks, find breaches faster, fix breaches faster and reduce breach impact (Figure 5).

Even the leaders have room for improvement. Our modeling revealed that leaders were among the highest performers in three of the four categories. Clearly, they should look to understand any aspect of their approach that falls outside the highest levels of performance and aim to improve those areas, just as non-leaders are required to do.

Figure 5. The defining characteristics of leaders in cybersecurity performance

CHARACTERISTICS	LEADERS (17%)	NON-LEADERS (74%)
Stop more attacks	**1 in 27 attacks breach security**	**1 in 8 attacks breach security**
Find breaches faster	**88% detect breaches in less than one day**	**22% detect breaches in less than one day**
Fix breaches faster	**96% fix breaches in 15 days or less**	**36% fix breaches in 15 days or less**
Reduce breach impact	**58% of breaches have no impact**	**24% of breaches have no impact**

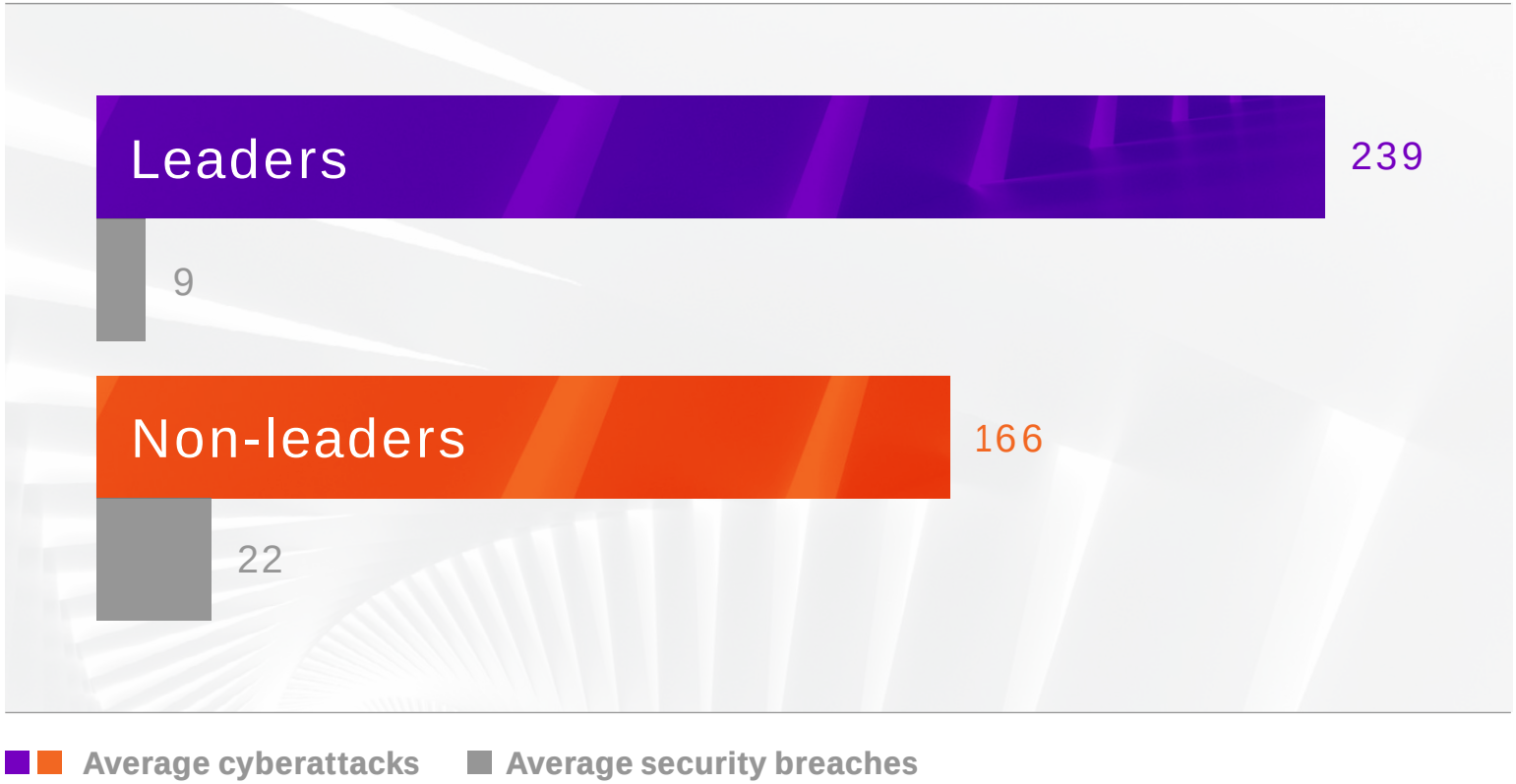
Source: Accenture Research; n=4,644

Stop more attacks

Calculating the total number of attacks against an organization depends on a number of factors—not least of which is the ability of security teams to detect them. Against this is the fact that security breaches are real incidents and more likely to be recorded accurately.

Keeping this in mind, leaders seem able to identify a higher number of direct attacks against them—an average of 239 cyberattacks compared with 166 for non-leaders—while having a much higher success rate in defending against them. These organizations see only nine security breaches per year compared with an average of 22 per year for non-leaders (Figure 6). The reduced number of security breaches compared with the total number of cyberattacks means leaders have nearly a fourfold advantage when dealing with security breaches.

Figure 6. Average number of security breaches and targeted cyberattacks for leaders and non-leaders



Source: Accenture Research; n=4,644

Leaders have nearly a fourfold advantage in stopping targeted cyberattacks

TAKE ACTION

The performance target for non-leaders is to reduce the number of cyberattacks that result in a security breach from 1-in-8 to 1-in-27 or better.

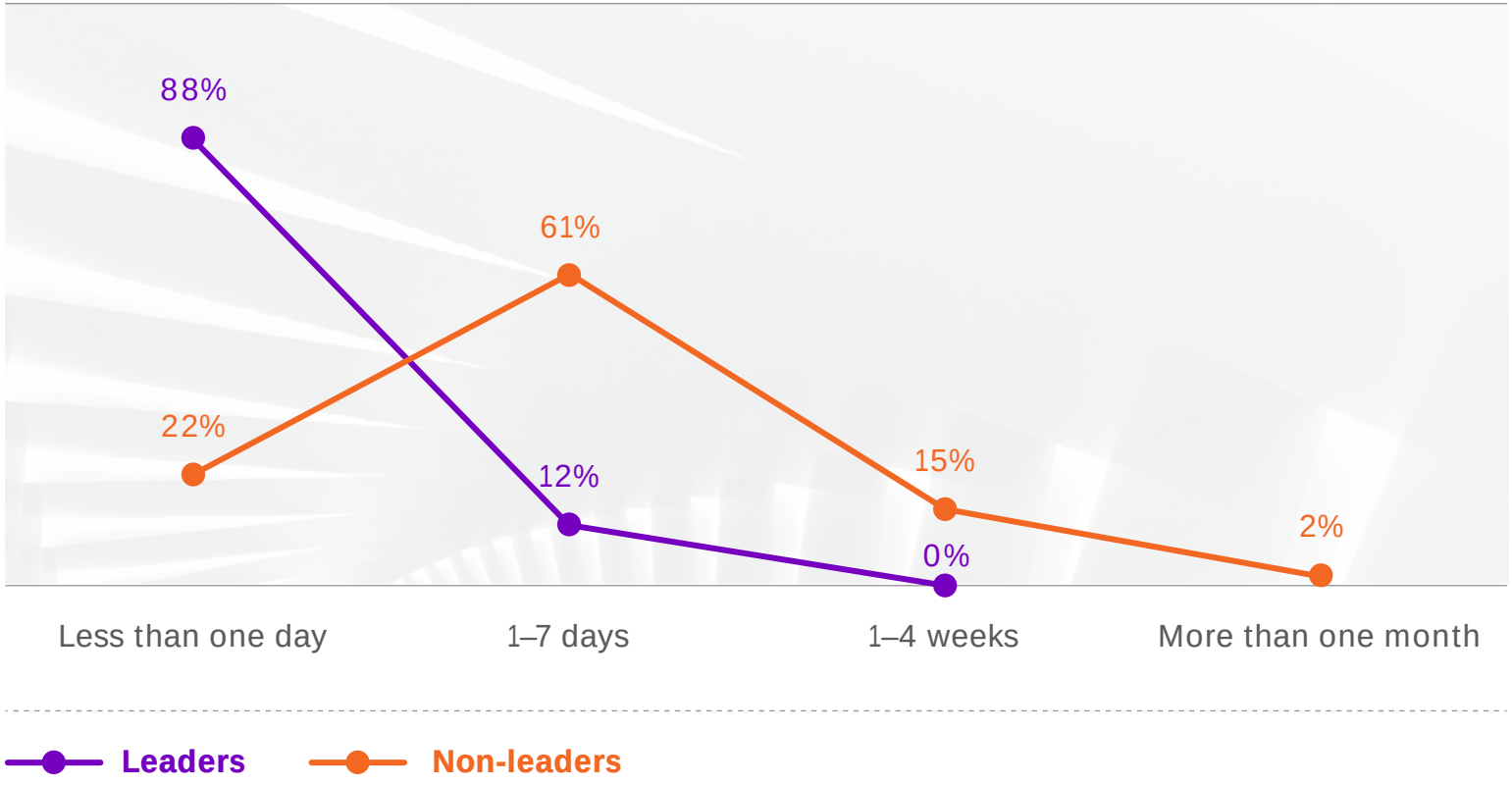
When attempting to reduce the number of security breaches, leaders say they benefit most from using the following three cybersecurity technologies: Next-Generation Firewall (NGF); Security Orchestration Automation and Response (SOAR) and Privileged Access Management (PAM). See page 26 for more on the specific technologies that benefit leaders.

Find breaches faster

Time is critical when it comes to detecting a security breach, and leaders have distinct advantages, with 88 percent able to detect a security breach in less than one day on average (Figure 7). The remaining 12 percent said they were able to detect security breaches in seven days or less.

Only 22 percent of non-leaders can detect security breaches with similar speed, while most (78 percent), take up to seven days or more.

Figure 7. Average time to detect a security breach



Source: Accenture Research; n=4,644

Leaders have a fourfold advantage in detection speed

TAKE ACTION

The performance target for non-leaders is to reduce the average detection rate for a security breach from up to seven days or more to less than one day.

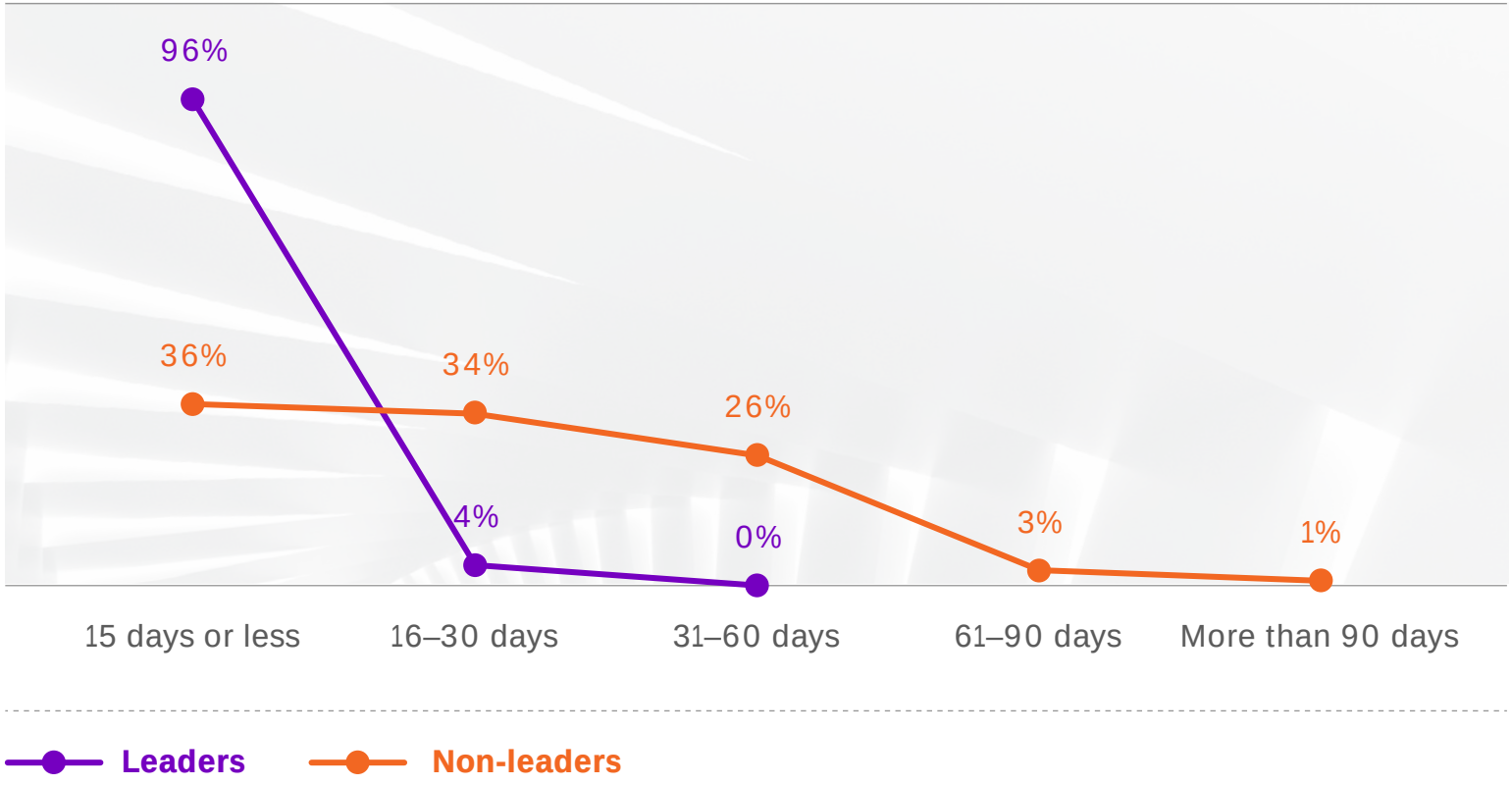
When attempting to find security breaches faster, leaders say they benefit most from using the following three cybersecurity technologies: Artificial Intelligence (AI), Security Orchestration Automation and Response (SOAR) and Next-Generation Firewall (NGF). See page 26 for more on the specific technologies that benefit leaders.

Fix breaches faster

Maintaining business continuity and rapid recovery speeds are other important aspects of cybersecurity resilience where leaders have clear advantages. Fully 96 percent of them plug security breaches in 15 days or less on average (Figure 8).

This majority response compares with only 36 percent of non-leaders able to remediate security breaches in the same amount of time. This means 64 percent take 16 to 30 days or more to remediate a security breach, on average.

Figure 8. Average time taken to remediate a security breach



Source: Accenture Research; n=4,644

Leaders have nearly a threefold advantage in speed of remediation

TAKE ACTION

The performance target for non-leaders is to reduce the average time to remediate a security breach from up to a month or more to 15 days or less.

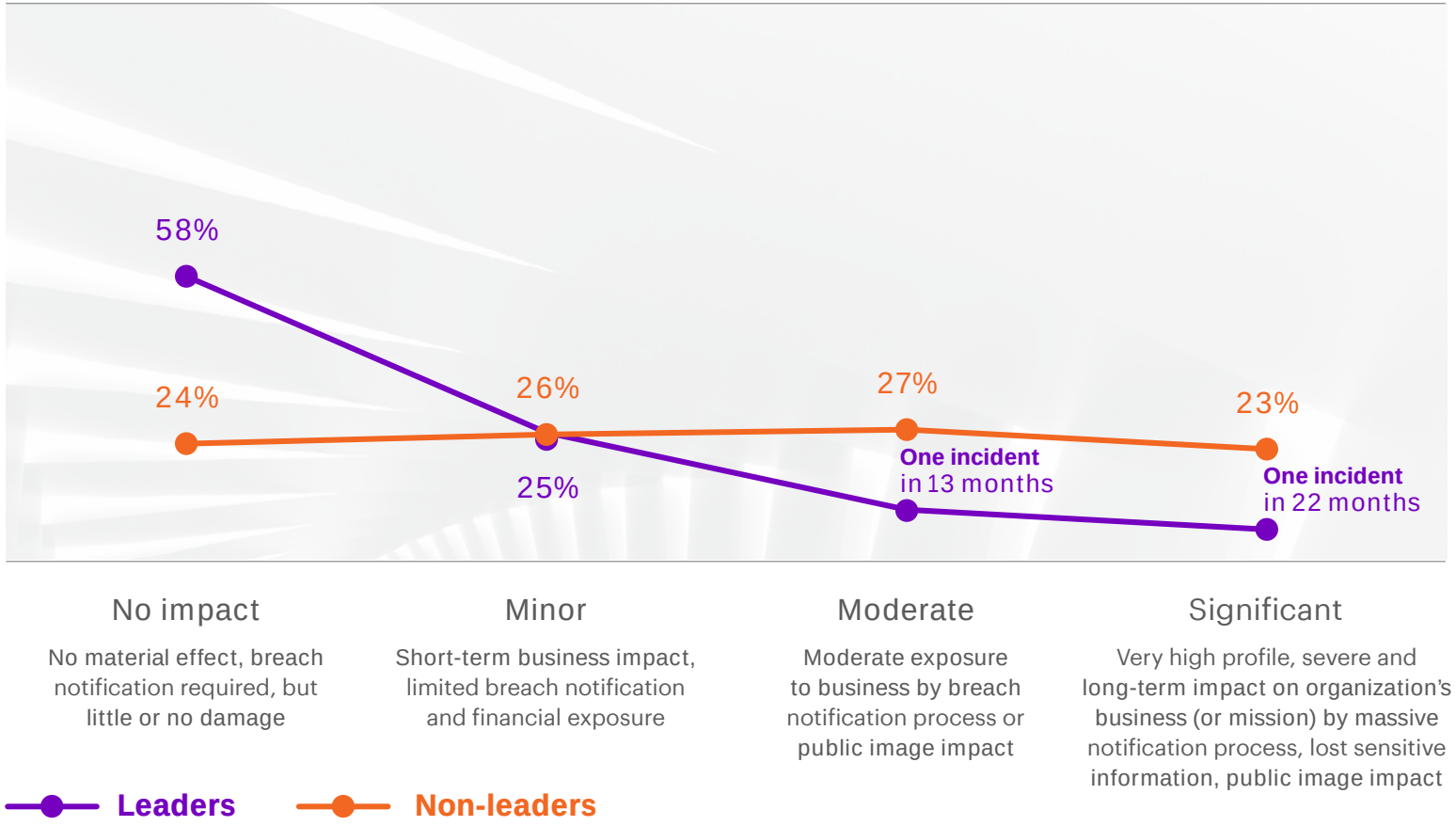
Leaders, when finding security breaches faster, say they benefit most from using the following three cybersecurity technologies: Security Orchestration Automation and Response (SOAR), Artificial Intelligence (AI) and Next-Generation Firewall (NGF). See page 26 for more on the specific technologies that benefit leaders.

Reduce breach impact

Speed of recovery is essential in minimizing the damage of a security breach and the level of impact on the organization is another important performance factor. Leaders stated that 83 percent of all security breaches resulted in either no impact or a minor impact (Figure 9). And when you look at the remaining security breaches, 10 percent are moderate impact and 6 percent are significant. In terms of timing, this translates to a moderate security breach every 13 months, on average, and a significant breach every 22 months or so, on average.

In comparison, non-leaders have lower levels of performance, with 50 percent of security breaches delivering a moderate or significant impact.

Figure 9. Security breaches by level of impact



Source: Accenture Research; n=4,644

Leaders have a twofold advantage in containing damage impact

TAKE ACTION

The performance target for non-leaders is to ensure at least three out of five security breaches have no impact or only a minor impact.

When trying to limit the impact of security breaches, leaders say they benefit most from using the following three cybersecurity technologies: Artificial Intelligence (AI), Next-Generation Firewall (NGF) and Security Orchestration Automation and Response (SOAR). See page 26 for more on the specific technologies that benefit leaders.

Filling the gaps in cybersecurity performance

Leaders know which technologies help to achieve a broader level of cybersecurity success. Non-leaders should consider refocusing their investment priorities toward the technologies which bring benefits that help to fill in some of the performance gaps and achieve a broader level of cybersecurity success.

Technology benefits	SOAR	AI	NGF	RBA	RPA	PAM
Fewer successful attacks	#2		#1	#4		#3
Reduced breach impact	#3	#1	#2			#4
More precise incident detection	#1	#2	#3		#4	
Reduced inherent risk/Shrink the attack surface	#1		#3	#2		#4
Cost reduction	#1	#2		#3	#4	
Consistent quality of response	#2	#1		#4	#3	

AI Artificial Intelligence (Machine Learning/Natural Language Processing)
NGF Next-Generation Firewall
PAM Privileged Access Management
RBA Risk-Based Authentication
RPA Robotic Process Automation
SOAR Security, Orchestration, Automation, Response

Source: Accenture Research; n=4,644

WHAT MAKES LEADERS SUCCESSFUL

Invest for operational speed (p.28)

Leaders prioritize moving fast and choose turbo-charging technologies to help them get there.

Drive value from new investments (p.32)

Leaders scale more, train more and collaborate more to increase the value from innovative technology.

Sustain what they have (p.38)

Leaders place more emphasis on maintaining existing investments and perform better at the basics of cybersecurity.

INVEST FOR OPERATIONAL SPEED

Prioritize moving fast

In the current environment of rising costs and growing third-party threats, security investments must work more effectively and efficiently than ever to prove their worth. So, what do leaders do differently to become more resilient? We found they invest for operational speed, drive value from new investments and sustain what they have.

While non-leaders focus on measuring their cyber resilience, leaders focus their speed of travel toward this final destination. The top three measures of cybersecurity success for leaders emphasize speed. We found that leaders prize how quickly they can detect a security breach, how quickly they can mobilize their response and how quickly they can get operations back to normal (Figure 10). Beyond these priorities, leaders also measure the success of their resiliency—how many systems were stopped and for how long—and precision—improving the accuracy of finding cyber incidents.

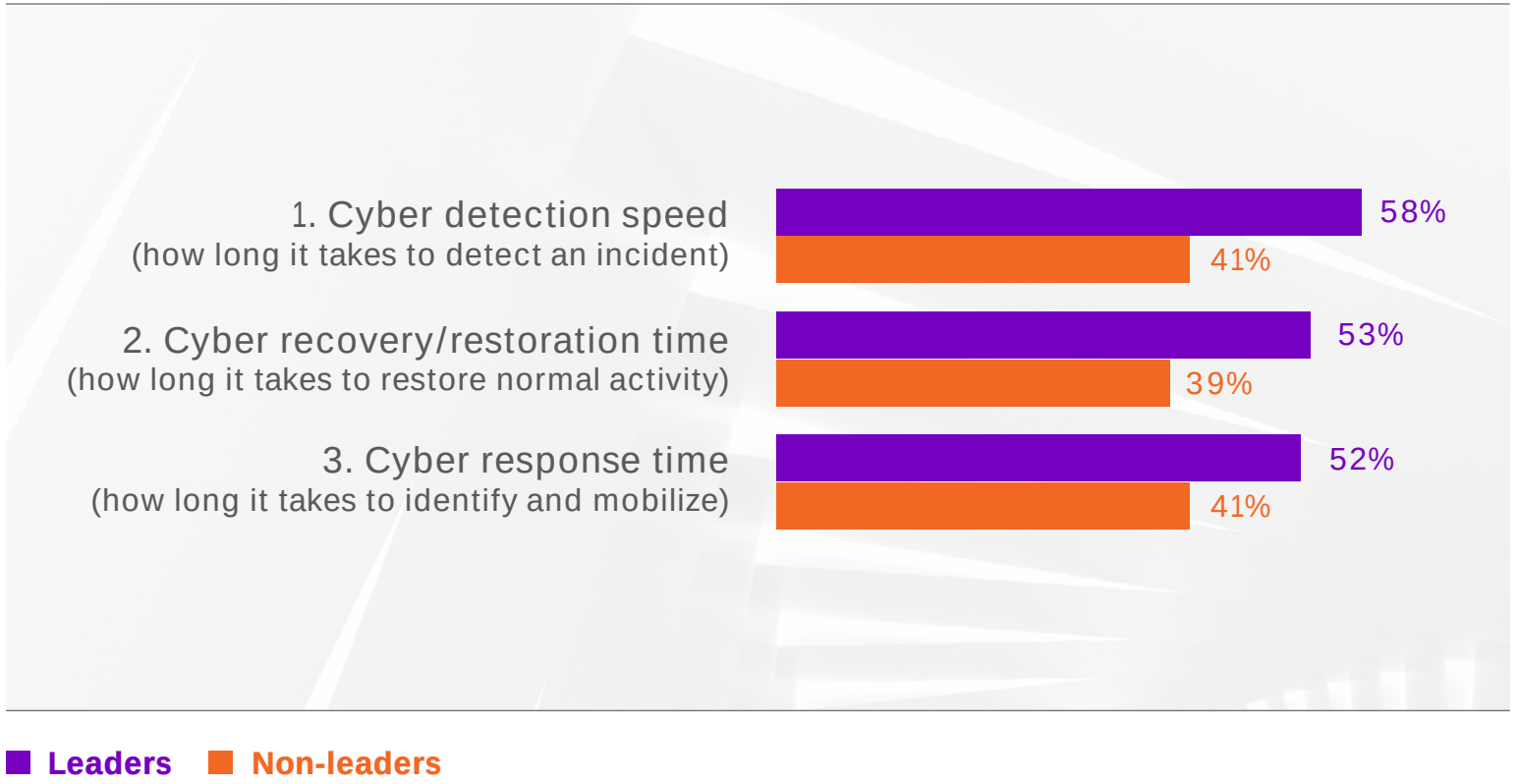
Where leaders value their speed of detection, response and recovery, the top three measures of cybersecurity success among non-leaders concern the outcomes they want to achieve: cyber operational technology (OT) resiliency; repetition (the portion of breaches that come from repeated attempts of the same type); and cyber IT resiliency.

TAKE ACTION

Non-leaders should consider refocusing their priorities to measure and improve their speed of detection, response and recovery. They should emulate the way leaders measure their cybersecurity performance to achieve greater levels of cyber resilience.

Prioritize moving fast

Figure 10. Top three ways leaders measure the success of their cybersecurity program



Source: Accenture Research; n=4,644

Choose turbo-charging technologies

We analyzed six advanced technologies to understand which ones provided the greatest contribution toward achieving each of the measures of cybersecurity success for leaders (Figure 11). Analysis of the technologies that benefit leaders helps to focus investment resources on the areas of greatest value. Artificial Intelligence (AI) and Security Orchestration Automation and Response (SOAR) technologies form the backbone of leaders' investment strategies. As we can see from Figure 11, Leaders have ranked the technologies that their companies align with and provide the greatest benefit in helping them achieve their main measures of cybersecurity success—speed of detection, speed of recovery and speed of response. They have also ranked the same range of technologies according to the benefits they derive from using them to achieve other measures of cybersecurity success—like fewer successful attacks, reduced breach impact and cost reduction (see p.26). The result of these findings creates a useful heatmap of which security technologies help the most in achieving a range of beneficial outcomes for cybersecurity success to guide security technology investments.

TAKE ACTION

Non-leaders should consider refocusing their investment priorities toward the technologies which benefit the ways leaders measure their cybersecurity performance: faster detection, faster response, and shorter recovery times.

INVEST FOR OPERATIONAL SPEED

Choose turbo-charging technologies

Figure 11. Security technologies ranked by leaders' priorities in achieving cybersecurity success

Leaders' priorities	SOAR	AI	NGF	RBA	RPA	PAM
Faster incident detection	#2	#1	#3	#4		
Faster incident response	#1	#1		#4	#3	
Shorter recovery times	#1	#2		#3	#4	

AI Artificial Intelligence (Machine Learning/Natural Language Processing)
NGF Next-Generation Firewall
PAM Privileged Access Management
RBA Risk-Based Authentication
RPA Robotic Process Automation
SOAR Security, Orchestration, Automation, Response

Source: Accenture Research; n=4,644

Scale more

The rate at which organizations scale investments across their business has a significant impact on their ability to defend against attacks. The leaders best at scaling technologies—defined as 50 percent or more tools moving from pilot to full-scale deployment—perform four times better than their counterparts (Figure 12). For the leaders best at scaling, only 5 percent of cyberattacks resulted in a security breach. For the non-leaders, 21 percent of cyberattacks resulted in a security breach.

Better security team detection

Security teams are also more effective for organizations who scale more of their technology investments. For those best at scaling, security teams discovered almost three-quarters of cybersecurity attacks against their organizations compared with only one-half of all cyberattacks for their counterparts.

Protect more key assets

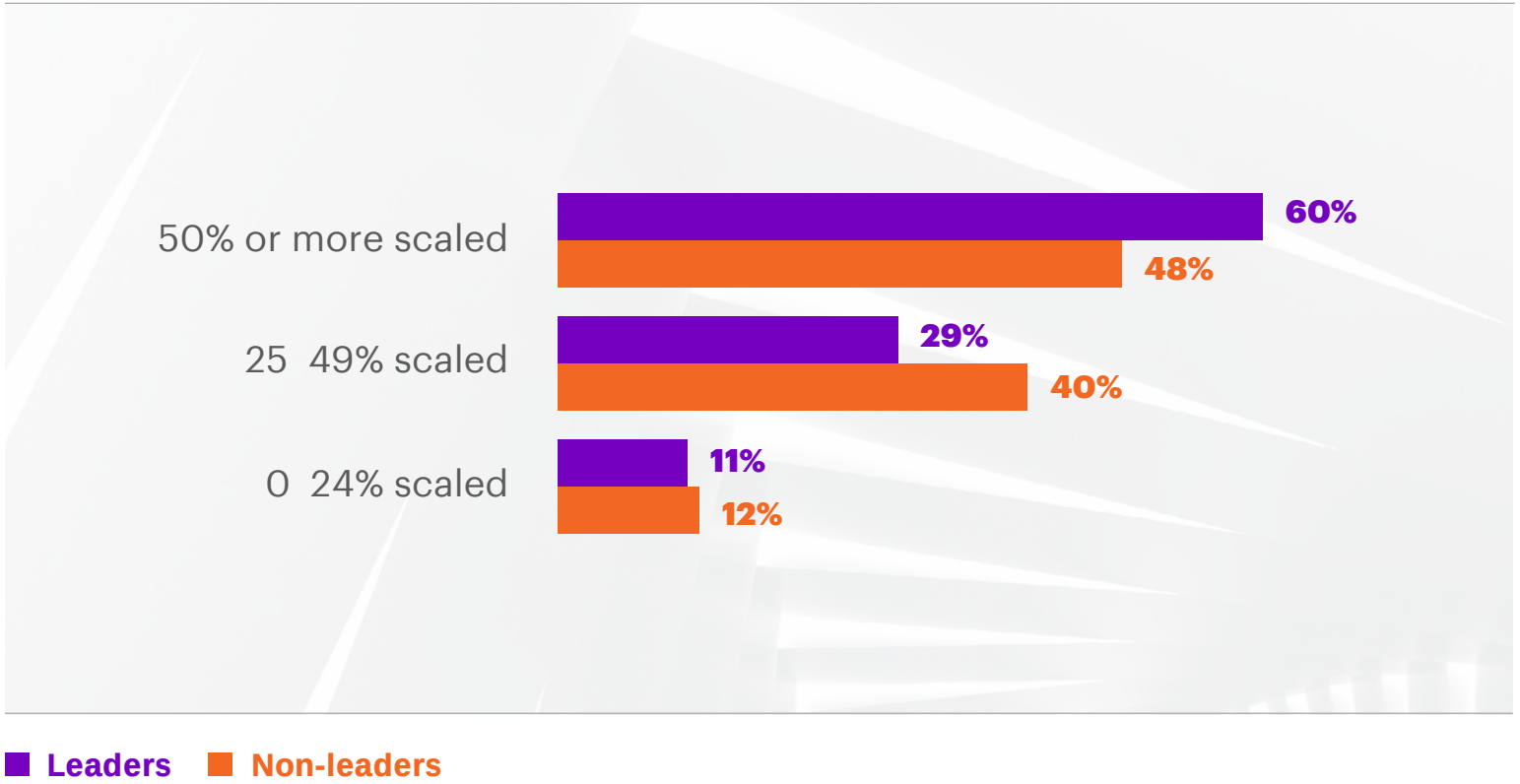
The ability to scale is an important factor in the reach of security programs. The cybersecurity programs for the best at scaling actively protect three-quarters of all key assets in the organization. The rest cover only one-half of their key assets. It is little surprise that 86 percent of leaders agreed new cybersecurity tools are increasing the reach of cybersecurity coverage for their organizations.

TAKE ACTION

Non-leaders should consider scaling fast, like the leaders, to realize how effective investments in new security technologies can be in improving security team detection rates and protecting more key assets—but only when they are fully deployed across the enterprise.

Scale more

Figure 12. The percentage of the security tools piloted then scaled and used throughout the enterprise



Source: Accenture Research; n=4,644

Train more

Training is another area where most organizations can make significant improvements. When asked about security tools adopted by their organization that require training, 30 percent of leaders provided training for more than three-quarters of users when it was needed, versus just 9 percent of non-leaders (Figure 13). For the best at training, only 6 percent of cybersecurity attacks resulted in a security breach compared with an average of 11 percent for the rest. Clearly, there is room for leaders and non-leaders to improve their performance by training more.

Faster at discovering and fixing breaches

The speed with which organizations find security breaches is faster for those who provide higher levels of training. The best at training found 52 percent of security breaches in less than 24 hours, compared with only 32 percent for the rest. How long it takes to remediate a security breach is also an aspect of better training. For the leaders in training, 65 percent of all security breaches are remediated within 15 days.

Protect more key assets

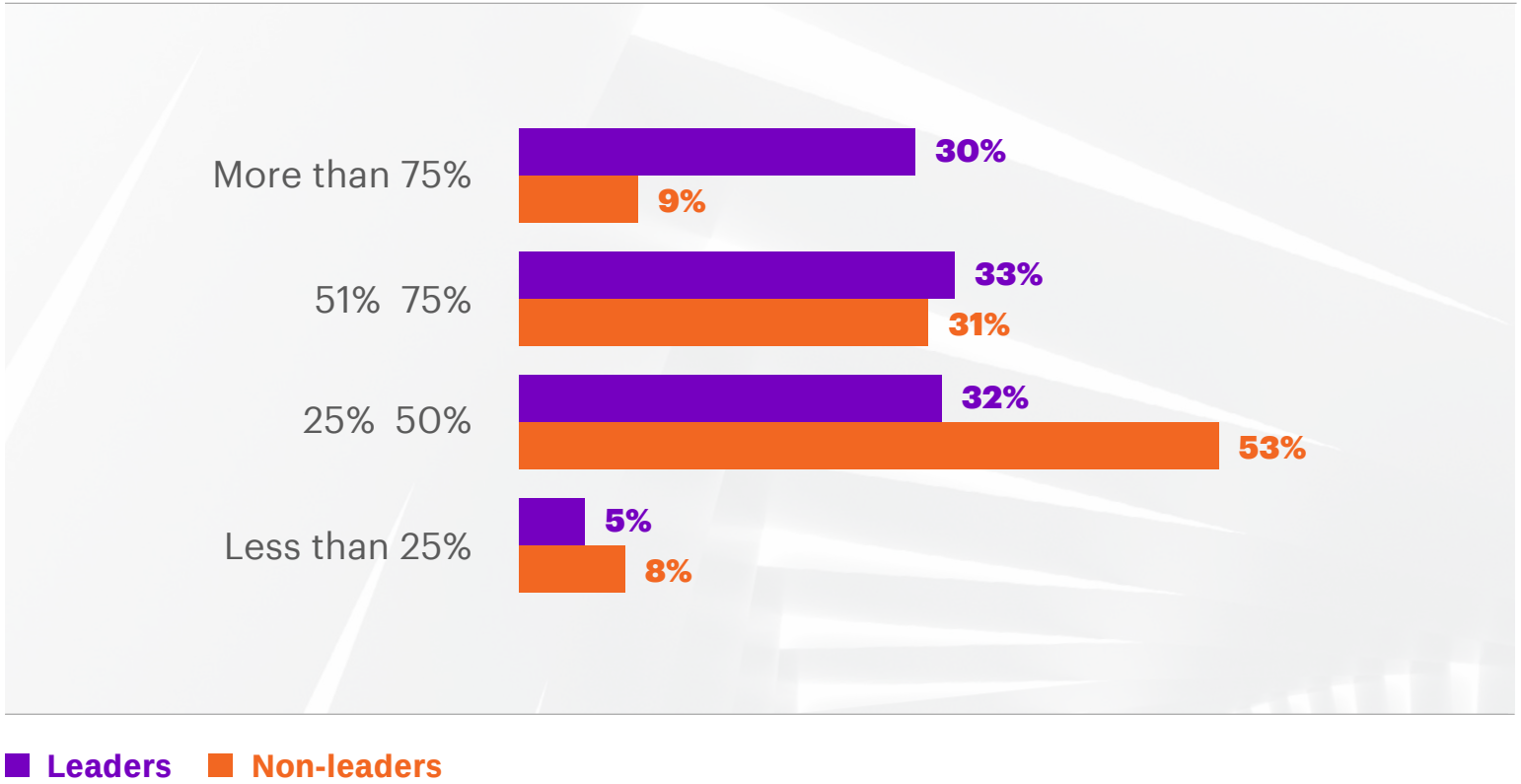
Introducing new tools means that training is essential to get the best out of them. For the best at training, 85 percent of their organization is actively protected by their cybersecurity program. The rest protect only 56 percent of their organization through their cybersecurity program.

TAKE ACTION

Non-leaders should consider training more, like the leaders, to make security tools more effective. They could benefit from better protection of more key assets along with faster discovery and remediation of breaches.

Train more

Figure 13. The percentage of users who receive training when needed for new security tools adopted by an organization



Source: Accenture Research; n=4,644

Collaborate more

When asked about the importance of collaboration, 79 percent of respondents agreed collaborations with other organizations, government bodies and the wider security community will be one of the essential weapons organizations will need to combat cyberattacks in the future. The organizations best at collaborating—the ones using more than five methods to bring together strategic partners, security community, cybersecurity consortiums, and an internal task force to increase understanding of cybersecurity threats—are two times better at defending against attacks than others. Organizations that collaborate more have a breach ratio of 6 percent against an average of 13 percent for the rest.

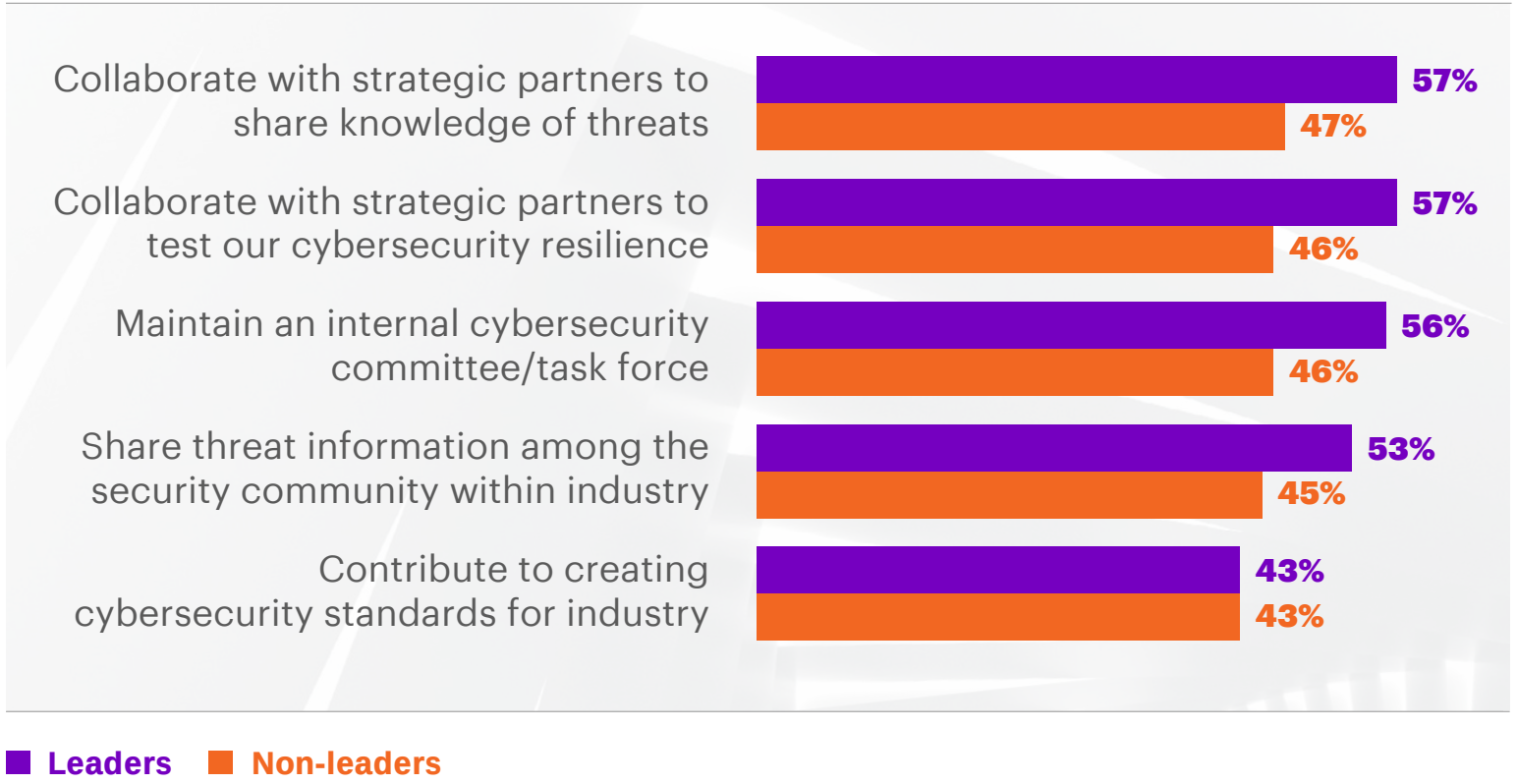
Threat intelligence plays a key role in ways to collaborate for leaders. Leaders focus more on knowledge sharing with partners and sharing threat information among the security ecosystem in their top five ways of collaborating with partners (Figure 14).

TAKE ACTION

Non-leaders should consider collaborating more, like the leaders. They could realize a better return on technology investments with a better containment of business impact and greater protection for key assets and the extended ecosystem.

Collaborate more

Figure 14. Main ways that organizations that are best at collaborating work with partners



Source: Accenture Research; n=4,644

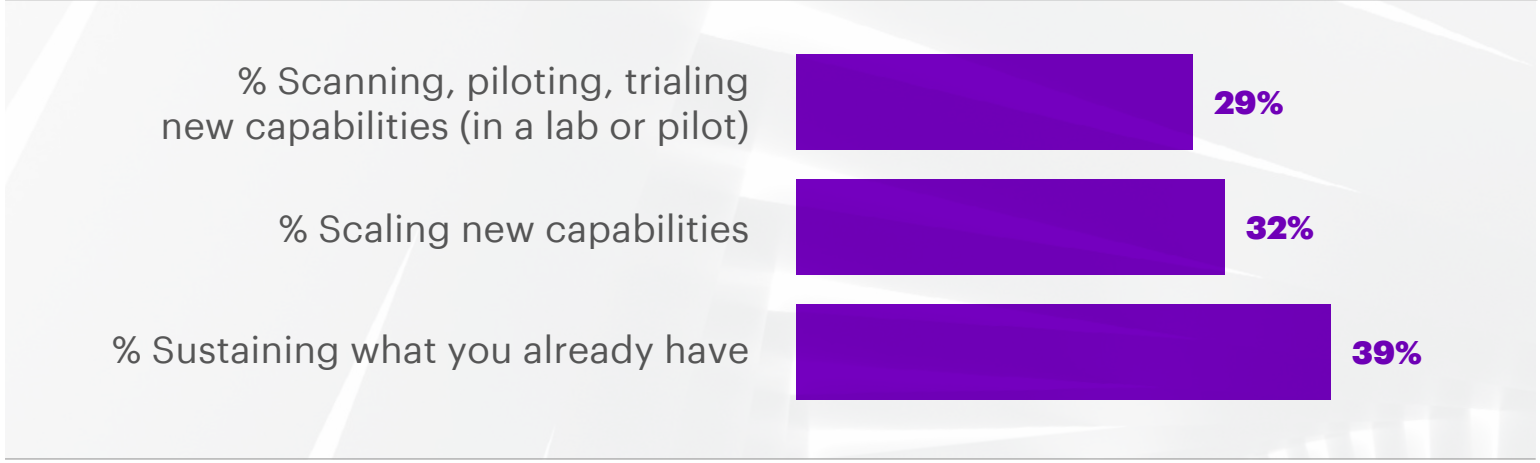
SUSTAIN WHAT THEY HAVE

Maintain existing investments

Despite recent improvements in the basics of cyber resilience—with security breaches down 27 percent in the last 12 months—non-leaders still have a long way to go if they are to match the cybersecurity performance of leaders. Leaders understand the need to be brilliant at the basics.

They focus more of their budget allocations on sustaining what they already have compared with non-leaders who place more emphasis on piloting and scaling new capabilities (Figure 15). In fact, non-leaders tend to spread their spending evenly across all three of these activities.

Figure 15. Budget allocation by leaders



TAKE ACTION

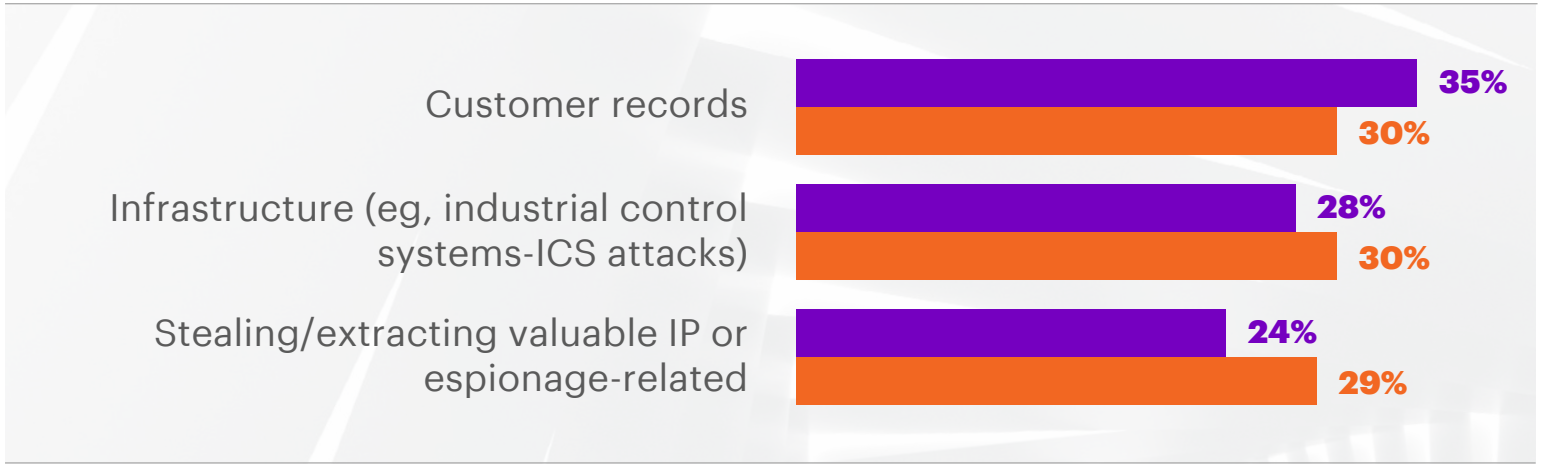
Non-leaders should consider placing more emphasis on sustaining what they already have to enable them to perform better at the basics just as the leaders do. They should also try to move more quickly from piloting new capabilities to scaling them across the enterprise.

Source: Accenture Research; n=4,644

Perform better at the basics

Security breaches most often happen when organizations fail at fundamental aspects of their protection practices. Which is a challenge when the highest proportion of cyberattacks against leaders—35 percent—target customer records (Figure 16). Yet with only 15 percent of leaders having more than 500,000 records exposed in the last year—compared with 44 percent of non-leaders—it is clear they are significantly better at the basics of cybersecurity protection. Now, more than ever, it is vital for organizations to make sure the basics of data-centric security are in place. It is not only the right thing to do, but also critical if organizations are serious about protecting their customer data and protecting their most important assets.[1]

Figure 16. The primary target of cybersecurity attacks against leaders



Source: Accenture Research; n=4,644

TAKE ACTION

Non-leaders should consider placing more emphasis on the basics of cybersecurity by putting steps in place to fortify their data-centric security and better protect their most important assets.

1 www.accenture.com/us-en/insight-data-achieving-centric-security-2017

MASTERING CYBERSECURITY EXECUTION

A core group of leaders has shown that cyber resilience is achievable and can be reproduced. By investing for operational speed, driving value from these investments, and sustaining what they have, they are well on the way to mastering cybersecurity execution.

Leaders often take a more considered approach to their use of advanced technologies by choosing those which help deliver the speed of detection and response they need to reduce the impact of cyberattacks. And once they do decide to invest, they scale fast—the number of leaders spending more than one-fifth of their budget in advanced technologies has doubled in the last three years. The combined result is a new level of confidence from leaders in their ability to extract more value from these investments—and by doing so, exceed the performance levels of the non-leaders.

With two out of five cyberattacks now indirect, organizations must look beyond their own four walls to their broader ecosystems. They should become masters of cybersecurity execution by stopping more attacks, finding and fixing breaches faster and reducing breach impact. In this way, they can not only realize security innovation success, but also achieve greater cyber resilience.

Test your own cybersecurity leadership

Ask your Accenture contact if you would like to undertake the Accenture Security Diagnostic to benchmark your organization's cybersecurity program capabilities against those of your peers in a personalized report.

ABOUT THE RESEARCH

ABOUT THE RESEARCH

In a continuation of our study started in 2017, Accenture Security surveyed 4,644 executives to understand the extent to which organizations prioritize security, how comprehensive their security plans are, and how their security investments are performing. The executives represent organizations with annual revenues of US$1 billion or more from 24 industries and 16 countries across North and South America, Europe and Asia Pacific.

The first step of our approach was to determine the characteristics of high-performance cybersecurity. We developed a list of dimensions that set leaders apart and which help leaders have a positive impact on reducing the overall cost of cybercrime. Our analysis determined leaders as those companies that exhibit high-performance in at least three of these dimensions:

Stop more attacks
Find breaches faster
Fix breaches faster
Lower breach impact

1 STOP MORE ATTACKS

The ratio of security breaches over attempted attacks received by each group.

2 FIND BREACHES FASTER

The percentage of the group that detect a breach in less than one day.

3 FIX BREACHES FASTER

The percentage of the group that fix a breach in less than 15 days.

4 LOWER BREACH IMPACT

The percentage of no impact and minor impact attacks received by each group.

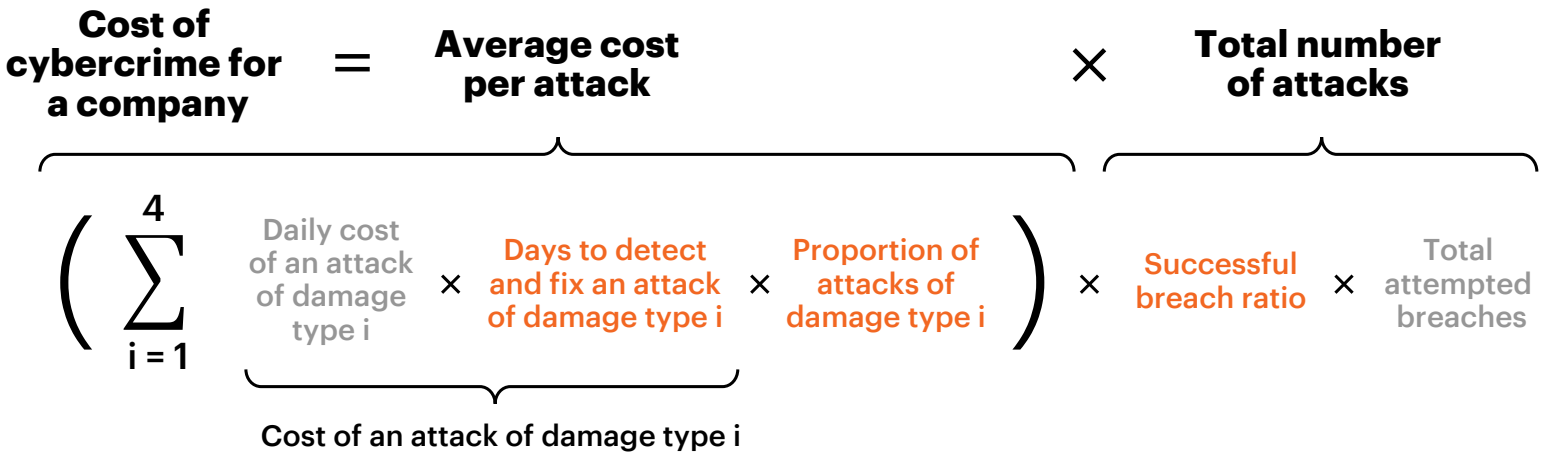
Our methodology

We then conducted a series of "what if" experiments to explore the return on investment of improving these cybersecurity practices. We created a formula to assess the cost of cybercrime for a company: the average cost per attack, multiplied by the total number of attacks.

The average cost per attack was the total of the daily cost of an attack by damage type, by the days to detect and fix an attack of this damage type, by the proportion of attacks for this damage type. The total number of attacks consisted of the security breach ratio by the total attempted breaches.

The average cost per attack was the total of the daily cost of an attack by damage type, by the days to detect and fix an attack of this damage type, by the proportion of attacks for this damage type. The total number of attacks consisted of the security breach ratio by the total attempted breaches (Figure 17).

Figure 17. A formula to assess the cost of cybercrime

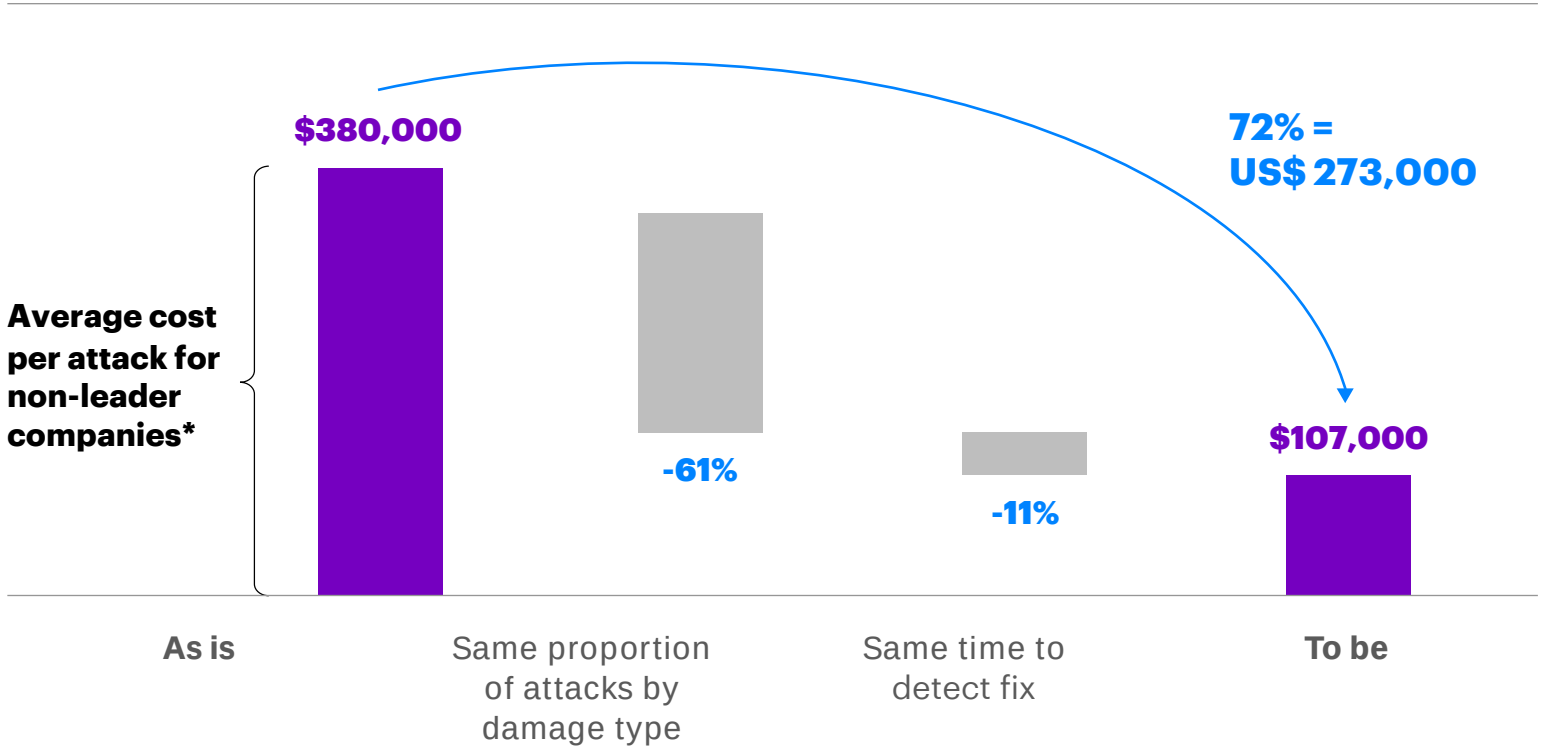


Note: all variables come from our survey comprising data for 4,644 organizations.
We assume variables in grey to remain constant. Damage type includes attacks that are: (1) Significant, (2) Moderate, (3) Minor and (4) No impact.

Our methodology

Our modeling simulations estimate the value to non-leaders of improving cybersecurity performance to the level of a leader could reduce the cost per incident by 72 percent. This equates to US$273,000 potential savings on average (Figure 18).

Figure 18. Cost reduction per attack if non-leaders perform as leaders



* As reported in our survey comprising data for 4,644 organizations, 83% of which were classified as non-leaders

ABOUT THE RESEARCH

Demographics

3RD ANNUAL RESEARCH STUDY

16 Countries

- Australia
- Brazil
- Canada
- France
- Germany
- Ireland
- Italy
- Japan
- Kingdom of Saudi Arabia
- Netherlands
- Norway
- Portugal
- Singapore
- Spain
- United Kingdom
- United States

US$1B+ Revenues

24 Industries

- Aerospace
- Automotive
- Banking
- Biotech
- Capital Markets
- Chemicals
- Consumer Goods
- Energy
- Health Provider
- Health Payer
- High Tech
- Industrial
- Insurance
- Life Sciences
- Media
- MedTech
- Metals & Mining
- Pharma
- Retail
- Telecom
- Travel
- Software
- US Federal
- Utilities

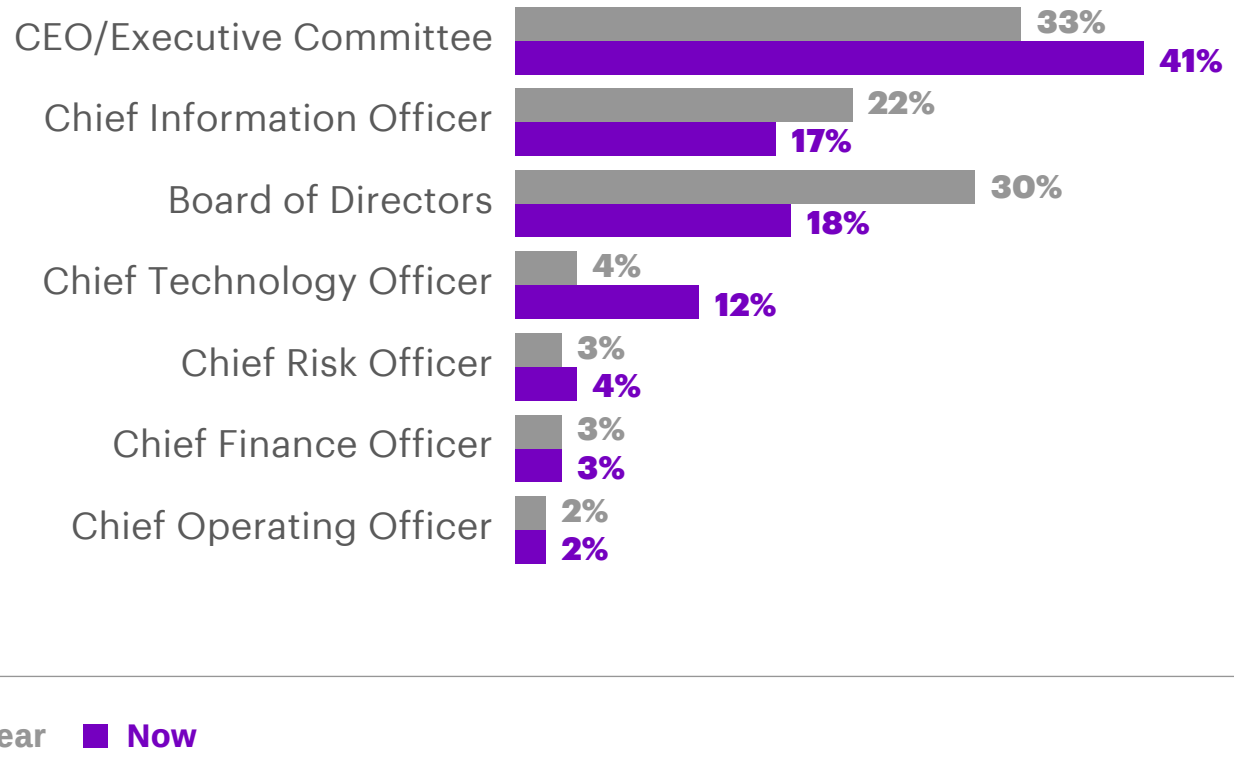
4644 Security executives

Reporting structure

The reporting structure, the influence of the C-suite and Board and who manages the budget have always been important considerations in any cybersecurity program. Our 4,644 executives highlighted that:

The CEO and executive team continue to expand their governance of cybersecurity programs but there is a drift away from board involvement in terms of reporting. Reporting to the CEO is up by 8 percentage points, while Board reporting is down by 12 percent. Direct reports to the CIO are down about 5 percent year-on-year with a general drift to the CTO of about 10 percent over the same period (Figure 19).

Figure 19. Direct reports for research respondents

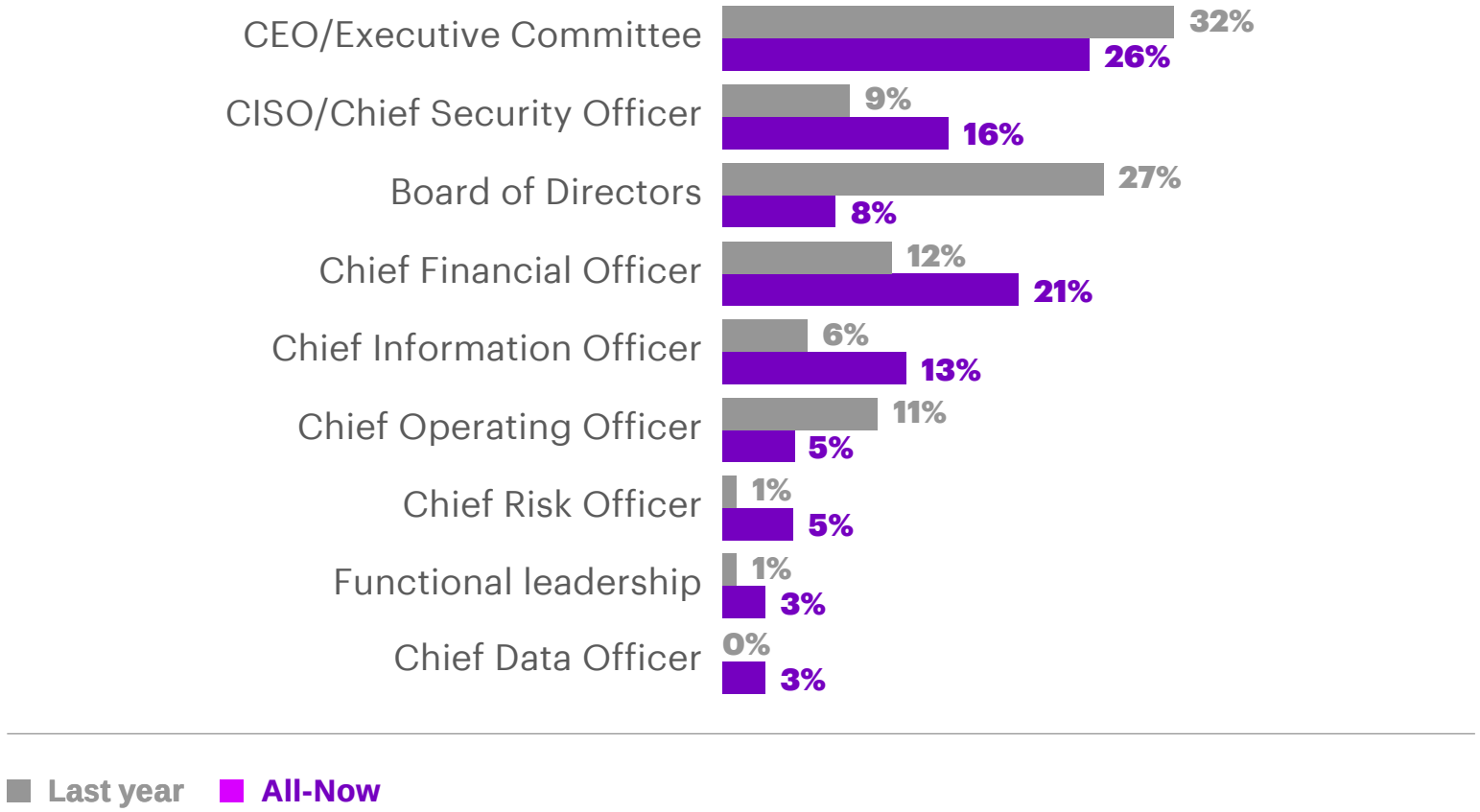


Source: Accenture Research; n=4,644

Budget authorization

The impact of budget approval continues to vary. The CEOs/Executive team's influence is steady, nudging down just a few points from last year's findings. The Board, however, is at around one-third of the level of participation in budget approval compared with last year. To compensate for this, CISO, CFO and CIO budget authorization is up by 5 to 10 points each over the year. While CEOs and the executive committee continue to be actively involved in cybersecurity governance; for many, this suggests budget approvals seem to be moving toward more of a business-as-usual activity (Figure 20).

Figure 20. Cybersecurity budget authorization for research respondents



Source: Accenture Research; n=4,644

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 505,000 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 the Accenture Security blog.

About Accenture Research

Accenture Research shapes trends and creates data driven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research—supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard—guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients. For more information, visit **www.accenture.com/research.**