2019 STATE OF CYBER RESILIENCE

accenturesecurity

INVEST FOR CYBER RESILIENCE

SCALE. TRAIN. COLLABORATE.
ACHIEVE BETTER RESULTS FROM CYBERSECURITY INVESTMENTS

FOREWORD

Welcome to the first of our 2019 State of Cyber Resilience reports—a guide to help C-suite leaders and their Boards understand how their security investments can be optimized to better protect their organizations.

Following on from last year's report, and as part of our extensive and ongoing body of research, we surveyed 4,644 security leaders with annual revenues of US$1 billion or more from 24 industries and 15 countries. We wanted to understand the extent to which organizations prioritize security, how comprehensive their security plans are, and how their security investments are performing.

It's clear that this is no time to stand still. We found 38 percent of organizations admit to having 500,000 records or more exposed in the last year—that's a lot of data and a potential loss of trust that is likely to have a long-term impact on the organizations involved. Coupled with the wake-up call of potential fines in excess of US$100 million for violations of GDPR, this kind of risk is unsustainable.

We did, however, discover some good news along the way, too. Yes, the threat landscape may be changing, with cost increases accelerating alongside evolving threats. But organizations are investing, particularly in new security technologies, and seeing clear benefits from doing so.

In fact there is a group of organizations that we identify as leaders who seem to have cracked the secret code behind making security work. These leaders demonstrate three key ways that enable their organizations to focus their efforts and drive better results from their security investments—they scale more, they train more and they collaborate more.

I hope you enjoy reading these research highlights and can join with the leaders in benefitting from successful security efforts. I welcome the opportunity to discuss any of these important issues with you.

KELLY BISSELL
GLOBAL LEAD—
ACCENTURE SECURITY

Kelly leads the Accenture Security business globally. With more than 25 years of security industry experience, 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.

NEW RISKS, HIDDEN THREATS

Indirect attacks mask the true scale of cyberattacks

Recent high-profile takedowns by law enforcement agencies lift the lid on the level of sophistication and maturity of cybercriminals. With attempts to steal US$100 million from US-based targets alone, the global GozNym malware hacker group comprised a complex supply chain of distributed attackers using advanced technologies—with each specialized freelancer of that supply chain responsible for a single step in the exploitation of victims. Effectively, it "was a supermarket of cybercrime services".[1]

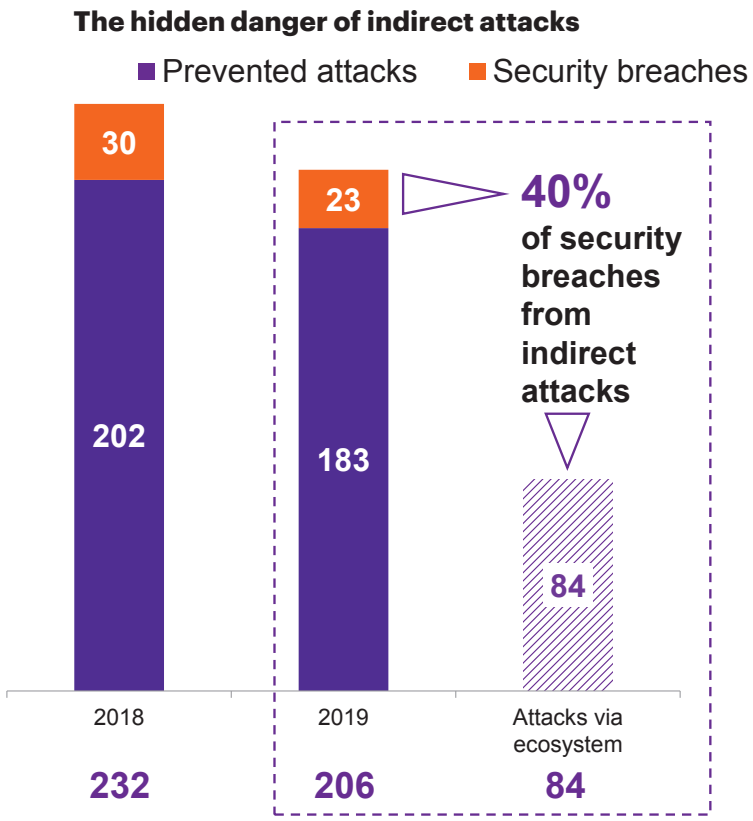
As financially-motivated cybercrime and politically-motivated cyber espionage groups evolve, organizations face new risks and hidden threats, such as:

Big game hunting—focusing a smaller number of cyberattacks against financially attractive organizations.

Regional attacks—exploiting domestic knowledge of local language, culture and technology to improve the chance of success.

Indirect attacks—where the entry point is through weak links in the supply chain or from compromises in cloud and managed service providers in the ecosystem.

While the reported number of cyberattacks* has reduced from 232 to 206 in the last year—in line with these trends—indirect attacks represent a hidden danger that masks the true scale of cyber threats. Since 40 percent of security breaches originate from weak links in the supply chain or business ecosystem, attacks against these ecosystem partners are 'hidden'. Applying the same breach ratio to ecosystem partners enables us to estimate the average number of cyberattacks targeting an organization may be closer to 290—an increase of 25 percent this year.



*See definition of cyberattacks page 4

FAILING INVESTMENTS

Despite pouring money into security efforts, investment returns often fail to live up to expectation

Investment in new technologies is leading to a proliferation of tools for most organizations—yet they are seeing only 53 percent returns on average for these investments. One reason may be down to the fact that these tools are not being tested or fully used throughout the enterprise—only one quarter of all security tools adopted are piloted and scaled across the organization.

Of course, tackling cybersecurity means adapting to a shifting landscape. To do so, security teams should keep pace with attack groups by embracing advanced technologies. And, with the number of indirect attacks, organizations should also focus on protecting their ecosystem as well as internal assets. According to our research, only 60 percent of an organization's business ecosystem is actively protected—an issue when 40 percent of breaches come through this route.

Failing to optimize investments is also having an impact in terms of protection and remediation. Our research shows only 59 percent of assets are actively protected by cybersecurity programs on average. While more than half of security breaches (54 percent) take more than 16 days to remediate—and one quarter take more than a month.

Targeted cyberattacks

For the purposes of this research, we investigated targeted cyberattacks. These have the potential to both penetrate network defenses and cause damage or extract high-value assets from within the organization. This excludes the deluge of hundreds—if not thousands—of speculative attacks organizations face on a daily basis.

CYBERSECURITY LEADERS

Leaders stop more attacks and resolve breaches faster with less damage

To assess cybersecurity performance, metrics must be presented in the language of the business to better engage the C-suite and Board. But to evaluate the performance of security technology investments, a more direct set of security-related metrics is necessary.

One of the primary purposes of new technology tools is to help fuel an organization's resilience—not only preventing attacks, but also aiding quick and efficient recovery from security breaches.

Our research finds that some organizations achieve significantly better results from their cybersecurity technology investments. These cybersecurity leaders perform better than the rest in relation to the number of security breaches, how quickly breaches are identified, the time taken to remediate an attack and the level of damage caused by those attacks.

CHARACTERISTICS OF LEADERS:	LEADERS	THE REST
LOW BREACH RATIO The percentage of cyberattacks that result in a security breach.	4%	13%
FAST DETECTION SPEED The percentage of the group that detect a breach in less than one day.	88%	22%
FAST REMEDIATION SPEED The percentage of the group that fix a breach in 15 days or less.	96%	36%
MINIMAL DAMAGE The percentage of security breaches with no impact and minor impact.	83%	50%

WHAT DO LEADERS DO DIFFERENTLY?

Leaders scale more, train more, and collaborate more

Of the 4,600 organizations we studied, 17 percent seem to have cracked the secret code behind making security work that sets them apart from the rest. These leaders do things differently to get the best results from their cybersecurity technology investments.

LEADERS SCALE MORE

Organizations best at scaling technology investments are 4X better than the rest at defending attacks

LEADERS TRAIN MORE

Organizations best at training are 2X better than the rest at defending attacks

LEADERS COLLABORATE MORE

Organizations best at collaborating are 2X better than the rest at defending attacks

LEADERS SCALE MORE

Organizations best at scaling technology investments are 4X better than the rest at defending attacks

Better at stopping cyberattacks

The rate at which organizations scale investments across their business has a significant impact on their ability to defend against attacks. Those best at scaling technologies perform four times better than their counterparts. For the best at scaling, only 5 percent of cyberattacks resulted in a security breach. For the rest, 21 percent of cyberattacks resulted in a security breach.

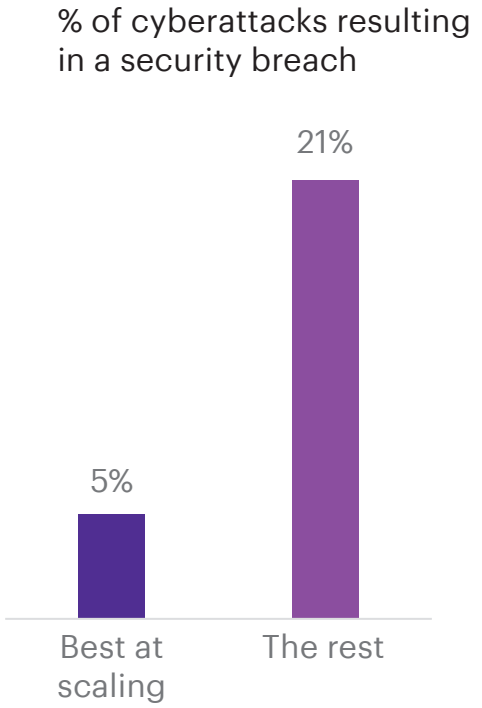
Faster at discovering breaches

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 half of all cyberattacks for their counterparts.

Protecting 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 half of their key assets.

The ability to scale more shows how effective investments in new security technologies can be—but only when they are fully deployed across the enterprise.



81% said new cybersecurity tools are increasing the reach of cybersecurity coverage for my organization

Definition of best at scaling: 50% or more of tools move from pilot to full-scale deployment

LEADERS TRAIN MORE

Organizations best at training are 2X better than the rest at defending attacks

Better at stopping cyberattacks

Training is another area where most organizations can make significant improvements. When asked about security tools adopted by their organization that require training, the best organizations provided training for more than three-quarters of users when it was needed. For these organizations, only 6 percent of cybersecurity attacks resulted in a security breach compared with an average of 11 percent for the rest.

Faster at discovering breaches

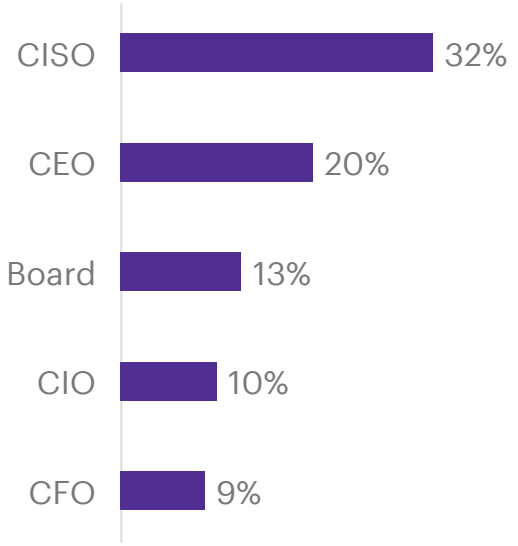
The speed with which organizations find security breaches is faster for those who provide higher levels of training. The best at training found 52 percent of security breaches in less than 24 hours, compared with only 32 percent for the rest.

Protecting 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 cybersecurity program.

The ability to train more makes security tools more effective—but organizations may be failing to prioritize training when CEOs and Boards authorize security budgets.

Who authorizes the budget for the best at training?



Definition of best at training: 75% or more of users receive the education they need in security tools

LEADERS COLLABORATE MORE

Organizations best at collaborating are 2X better than the rest at defending attacks

Better at stopping cyberattacks

Organizations that collaborate more experience more benefits, including a lower breach ratio: the breach ratio is 6 percent for those who use five or more methods to collaborate, against an average of 13 percent for the rest.

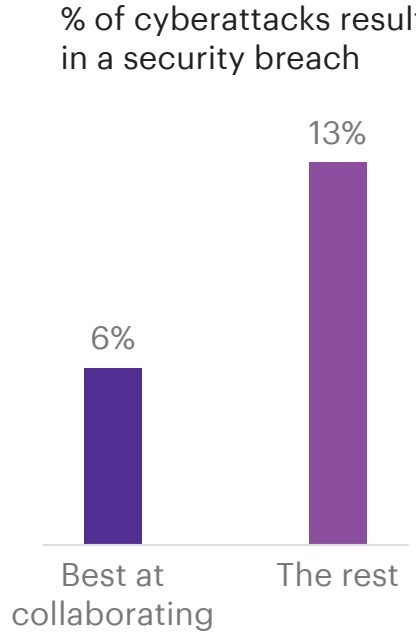
Protecting more key assets

Organizations that collaborate more are significantly better protected by their cybersecurity program, including their ecosystems. For those who collaborate more, 67 percent of their organization is actively protected by their cybersecurity program. The rest protect only 58 percent of their cybersecurity program.

Improved regulatory alignment

Regulatory alignment is important with increasing demands for audit compliance and substantial fines emerging from data privacy protections like the General Data Protection Regulation (GDPR). For the best at collaboration, 54 percent state improved alignment with regulatory requirements a direct result of collaboration compared with only 25 percent for the rest.

The ability to collaborate more realizes a better return on technology investments with a better containment of business impact and greater protection for key assets and the extended ecosystem.



79% said collaboration with other organizations, government bodies and the wider security community will be one of the essential weapons organizations will need to combat cyberattacks

Definition of best at collaborating: using 5+ methods to bring together strategic partners, security community, cybersecurity consortiums, and an internal task force to increase understanding of cybersecurity threats.

MAKING INVESTMENTS WORK

When it comes to cybersecurity investments, spending more does not always equate to better performance. And as the costs of cybersecurity continue to rise, investments need to work harder to prove their worth.

In the last two years, the ratio of cost to investment is rapidly becoming unsustainable. C-suite leaders and their Boards should act to be sure that their investments are protecting their organizations for today and tomorrow.

By understanding the effective strategies used by leaders—scaling, training, and collaborating more keenly—organizations can not only optimize security investments but potentially achieve better outcomes.

Ask yourself:

1. Have we gone beyond piloting to scale our cybersecurity technology investments effectively across the organization—and among suppliers and partners in our ecosystem?

2. Are we regularly updating the training and education programs for our people based on existing and planned security tools and techniques?

3. Are we working closely with strategic partners, security communities, cybersecurity consortiums—and do we have an internal task force to enhance our overall understanding of cybersecurity threats?

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 companies with annual revenues of US$1 billion or more from 24 industries and 15 countries across North and South America, Europe and Asia Pacific.

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.

References

1 GLOBAL TAKEDOWN SHOWS THE ANATOMY OF A MODERN CYBERCRIMINAL SUPPLY CHAIN, Wired, May 16 2019. https://www.wired.com/story/goznym-takedown-cybercrime-supply-chain/

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 482,000 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.