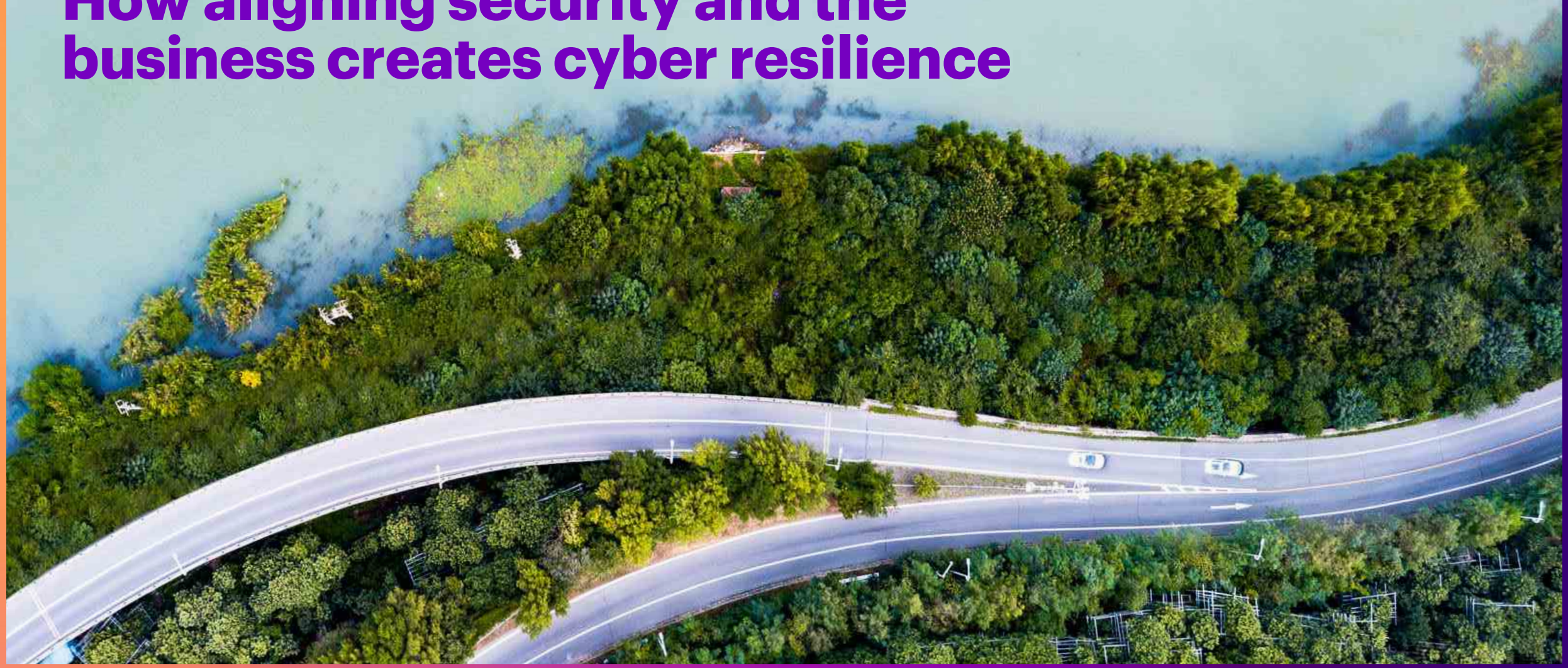
accenture

State of Cybersecurity Resilience 2021

# How aligning security and the business creates cyber resilience



# Table of contents

# About the authors


**Kelly Bissell**
**Global Lead**
**Accenture Security**


Kelly leads the Accenture Security business globally. With more than 25 years of security industry experience, Kelly has served governments and the private sector across all areas of cybersecurity. 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.


**Jacky Fox**
**Group Technology Officer**
**Accenture Security**


Jacky leads the Accenture Security practice in Ireland and serves on the global leadership team as Group Technology Officer. With more than 20 years of experience in technology and cybersecurity consulting, Jacky has worked across multiple industry sectors, specializes in helping organizations to understand and treat their cyber risk and has experience in investigating many national and international breaches. She is also Vice-Chair on the board of Cyber Ireland and is an adjunct lecturer for University College Dublin on forensics and security. She is a frequent public speaker, contributing to the World Economic Forum, Interpol and the United Nations.


**Ryan M. LaSalle**
**Senior Managing Director**
**Accenture Security**


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.


**Paolo Dal Cin**
**Senior Managing Director**
**Accenture Security**


Paolo leads the Europe 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 security at the Universities of Udine, Modena and Milan in Italy.


## Acknowledgements

The authors would like to thank Edward Blomquist, Julia Malinska, Anna Marszalik, Eileen Moynihan, Vincenzo Palermo and Ann Vander Hijde for their contributions to this report.

# Championing cybersecurity

## Championing cybersecurity

In our annual survey among 4,744 global respondents around the current state of cybersecurity resilience, we found that many CISOs feel recognition for their role in fulfilling the business strategy is well overdue—85% agree or strongly agree that the cybersecurity strategy is developed with business objectives, such as growth or market share, in mind.

Yet, most business executives (78%) said that they don't know how or when a cybersecurity incident will affect their organizations. It's a sentiment that continues to increase from our 2020 report when it was still high at 69%.

A majority of respondents (81%) say that "staying ahead of attackers is a constant battle and the cost is unsustainable" compared with 69% in 2020. In fact, we found that respondents experienced a 32% increase over 2020 in the number of successful cyber attacks, while some attacks, such as ransomware, have seen a much higher increase.

This year, we continued our exploration of leaders in cyber resilience. Due to the rapid increase in high-profile attacks and sheer complexity of handling cybersecurity demands, we also tested what difference it made to cyber resilience if there was a stronger alignment between cybersecurity practices and the business strategy.

### What is cyber resilience?

The cyber-resilient business brings together the capabilities of cybersecurity, business continuity and enterprise resilience. It embeds security across the business ecosystem and 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 across the entire value chain, strengthen customer trust and grow with confidence.

Our research identified four levels of cyber resilience (Figure 1). At the head of the pack is a group of Cyber Champions—organizations that strike a balance, not only excelling at cyber resilience, but also aligning with the business strategy to achieve better business outcomes. They are successful in at least three out of four cyber resilience performance criteria—better at stopping attacks, finding and fixing breaches faster and reducing their impact.

We also identified two new groups that reflect different approaches to cyber resilience: Business Blockers who put cybersecurity first over alignment with the business strategy and Cyber Risk Takers who put business strategy first over alignment with cybersecurity. The fourth level of cyber resilience we've identified as The Vulnerable.

It matters where organizations fall within this cyber quadrant—there's money on the table. Business Blockers stand to reduce their cost of breaches by 48%, Cyber Risk Takers by 65% and The Vulnerable by 71% if they increased their performance to Cyber Champion levels.

## The cyber quadrant

**Figure 1. Four levels of cyber resilience**


**Our report shows what a difference a year makes and how leading organizations are demonstrating cybersecurity resilience.**

# Where are we now?

**Cyber attacks are up**

**Security investment continues to rise**

**Cloud still has a complex relationship with security**

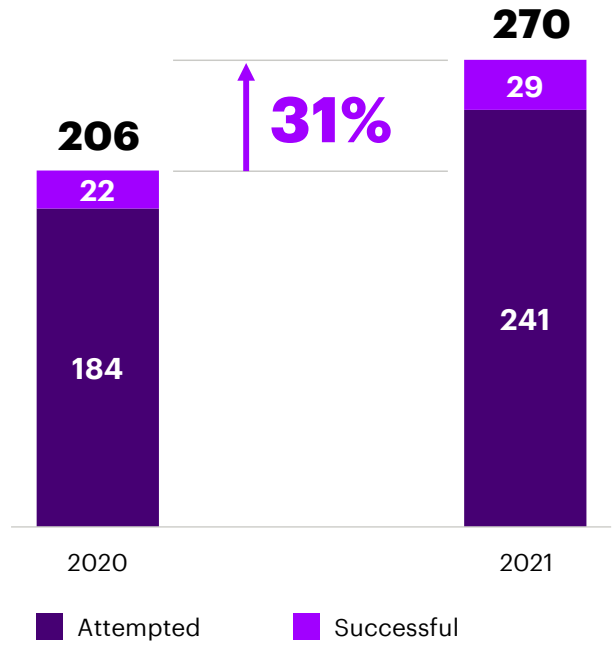
# Cyber attacks are up

**Even a global pandemic can't stop cyber criminals—if anything, the vulnerability and uncertainty was a breeding ground for new attacks. There were on average 270 attacks (unauthorized access of data, applications, services, networks or devices) per company over the year, an increase of 31% compared with 2020 (Figure 2).**

Third-party risk continues to dominate. Indirect attacks—by which we mean successful breaches to the organization through the supply chain—have increased from 44% to 61%.

And the impact of cybersecurity has hit hard in the boardroom; in an analysis of more than 500 companies' 2020 earnings reports, there's an increase in legal (23%), economic (16%) and internal (10%) discussions around cybersecurity consequences compared with 2019, suggesting an elevation in prioritizing the subject.[1]

**Figure 2. Average attacks per company up 31%**




Source: Accenture State of Cybersecurity surveys
Wave 3 report published in January 2020 (N=4,644)
and Wave 4 report published in November 2021 (N=4,744)

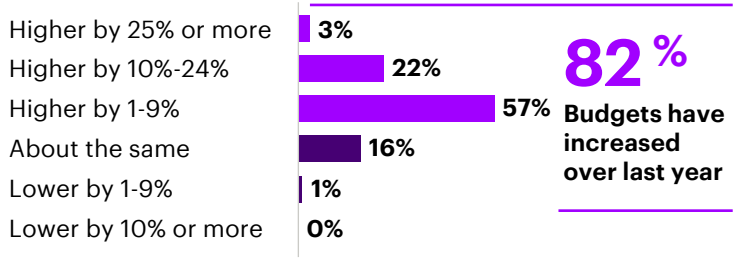
# Security investment continues to rise

**IT security budgets are increasing, with more than 82% of our survey respondents saying their budgets have increased in the last year (Figure 3). IT security budgets are now up to 15% of total IT spend, 5 percentage points higher than the spend reported in 2020.[2]**

This may be the COVID-19 change event—the massive and rapid shift in how they ran their businesses and increased security demands; we won't know until next year if this kind of investment will continue but we do know that budgets are always under scrutiny. Rapid cloud adoption may also contribute to this investment increase since many security tools have to be updated to accommodate cloud or more robust security is needed in a digital world.

Perhaps this increased spend has encouraged optimism. On average, 70% believe their organization is actively protected by their cybersecurity program, compared with 60% in 2020. While they are also more confident about the wider picture—67% believe their ecosystems to be secure, compared with 60% in 2020.

**Figure 3. 2021 Cybersecurity spending increase compared with 2020**




Source: Accenture State of Cybersecurity Resilience 2021 (N=4,744)

"During my four year tenure, we tripled, maybe quadrupled the security budget. We were starting from ground zero, so we had to overinvest in security systems and infrastructure to get it up to where it needed to be."

Global Head of IT, Pharmaceutical Company

# Cloud still has a complex relationship with security

**Over the next three to five years, more than two-thirds of workloads will shift to the cloud, with about one-third of organizations moving more than 75% into the cloud across most regions of the world.[3]**

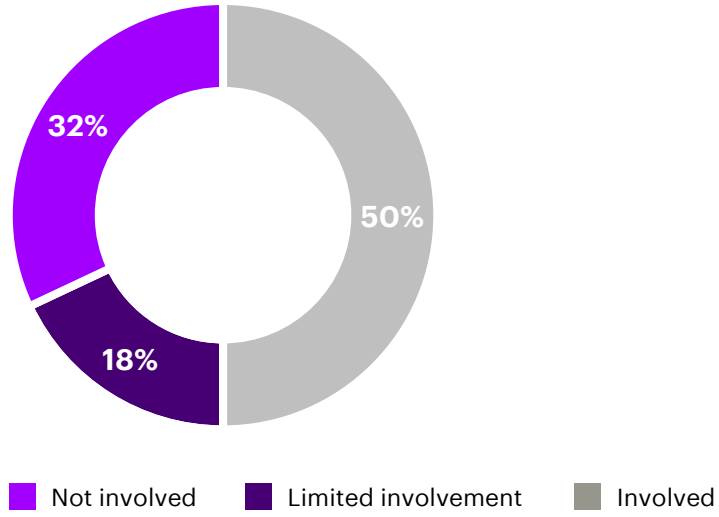
This is echoed in our recent technology innovation strategies research which found that the top 10% of respondents doubled down on technology investment during the pandemic —72% accelerated investment in security.[4]

Our cyber resilience survey respondents have moved their operations to the cloud because they recognize the benefits such as lower costs, more resilient operations and access to more advanced technology.

Yet, despite most of our survey respondents believing that cloud applications and operations are more secure than those hosted on-premise, nearly one-third (32%) say security is not part of the cloud discussion from the outset and their organization is trying to catch up (Figure 4).

And reasons preventing the take up of the cloud revolve around security issues: about one-third of all respondents say poor governance and compliance practices around cloud security are a problem, that cloud security is too complex and that they do not have the skills internally to structure a proper cloud security framework.

**Figure 4. Nearly one-third of respondents say security is not part of the cloud discussion**




Source: Accenture State of Cybersecurity Resilience 2021 (N=4,744)

# Why alignment matters

## Why alignment matters

**This year's research continued to explore how winning organizations tackle cyber resilience, evaluating their responses based on the following key measures of cyber resilience: they stop more attacks, find and fix breaches faster and reduce breach impact.**

We also looked at the impact on cyber resilience from being aligned with the business strategy and identified four levels of cyber resilience: Cyber Champions, Business Blockers, Cyber Risk Takers and The Vulnerable (Figure 5).

Let's examine the differences in the cyber quadrant positions and the implications for business performance and cyber resilience.

**Figure 5. Key measures of cyber resilience**

| | Cyber Champions | Business Blockers | Cyber Risk Takers | The Vulnerable |
|---|---|---|---|---|
| **Stop more attacks:** Number of attacks that breach security | **1 in 6** | **1 in 4** | **1 in 2** | **1 in 2.3** |
| **Find breaches faster:** % breaches found in < 1 day | **55%** | **50%** | **11%** | **15%** |
| **Fix breaches faster:** % fixed in 15 days or less | **100%** | **96%** | **30%** | **30%** |
| **Reduce breach impact:** % breaches with no impact | **72%** | **64%** | **23%** | **24%** |

Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

# Business Blockers

**Business Blockers take a security-first approach and place less emphasis on alignment with the business strategy. They are sometimes seen as an impediment to business objectives.**

## Why alignment matters

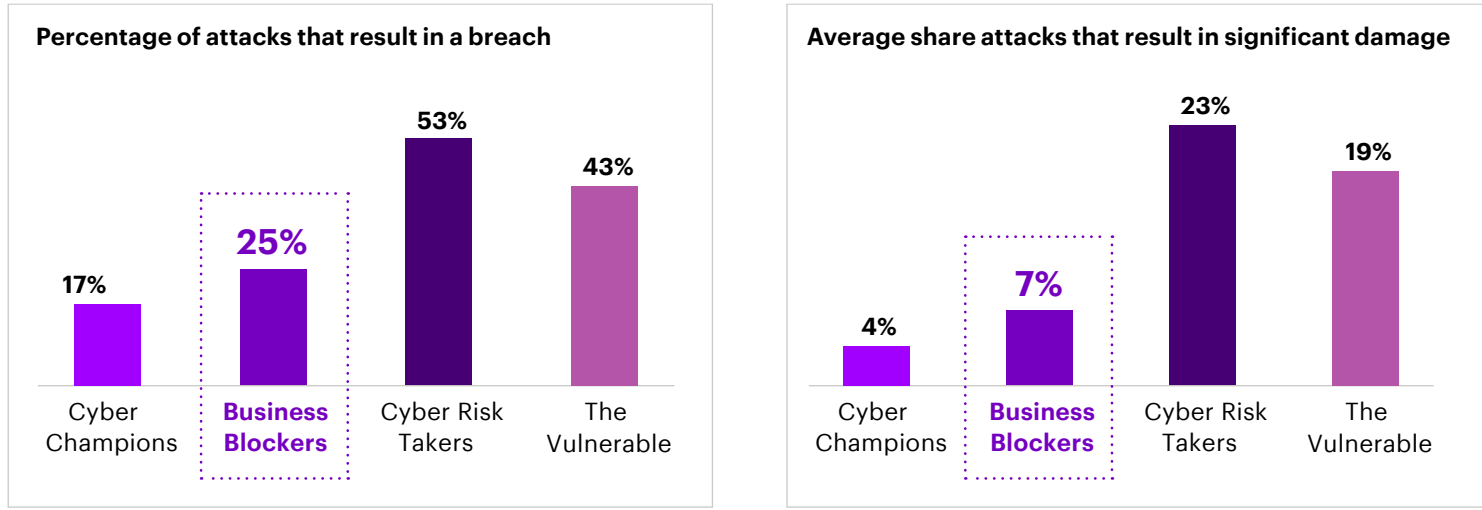
Business Blockers outperform Cyber Risk Takers and The Vulnerable, but lag Cyber Champions across all key measures of cyber resilience. As illustrated in Figure 6, they experience fewer breaches than Cyber Risk Takers and The Vulnerable, but 8 percentage points more than Cyber Champions (17%).

When it comes to the average share of significant attacks—with high-profile, severe and long-term impact on the organization's business or mission—they experience fewer than Cyber Risk Takers or The Vulnerable, but nearly 2X more than Cyber Champions.

And when attacks get through, Business Blockers detect and remediate them more quickly than Cyber Risk Takers and The Vulnerable, but lag Cyber Champions by a day on both measures.

Business Blockers also have the highest percentage of CISOs with full authority to approve budgets (32%) versus Cyber Champions (21%), Cyber Risk Takers (21%) and The Vulnerable (16%). This CISO-driven spending autonomy may explain the increased focus on cybersecurity over business strategy.

**Figure 6. Impact of breaches on Business Blockers**



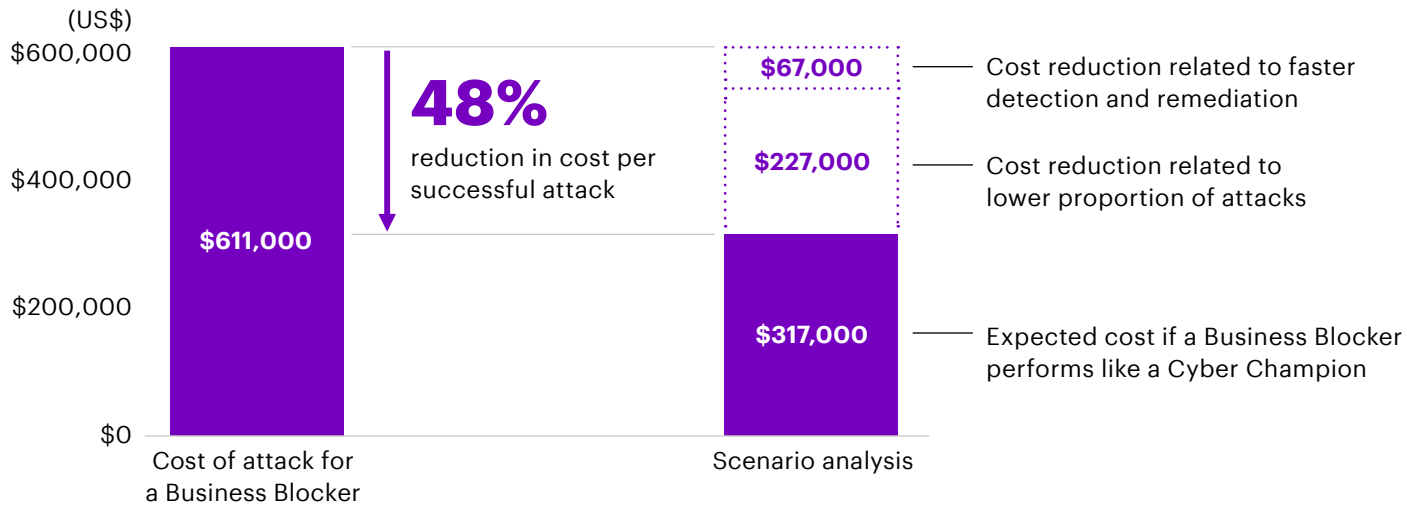

Source: Accenture State of Cybersecurity Resilience 2021, security executives
(N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

## Why alignment matters

If Business Blockers add alignment to their already-robust cybersecurity foundation, they will have even stronger cyber resilience, without sacrificing business outcomes.

Business Blockers could reduce costs by 48% per successful attack if they increased their performance to Cyber Champion levels, with savings of about US$294,000 per attack (Figure 7).

**Figure 7. Value at stake if Business Blockers perform like Cyber Champions**




Note: We assign the same level of performance to Business Blocker companies as the Cyber Champion companies across metrics of cyber resilience such as speed of detection/remediation and proportion of significant attacks and simulate the cost outcomes. N=522

# Cyber Risk Takers

**Cyber Risk Takers take a business-first approach and place less emphasis on alignment with the cybersecurity strategy. They report higher probability of meeting or exceeding their business objectives, but their business focus comes at the expense of cybersecurity success.**

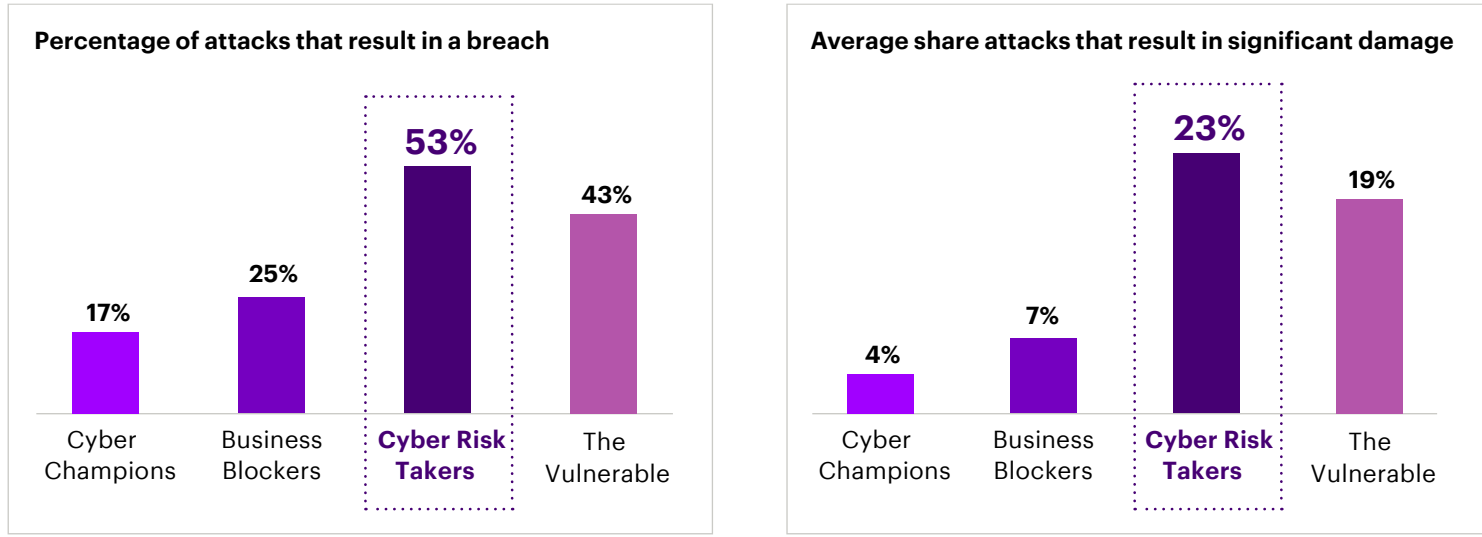
## Why alignment matters

Cyber Risk Takers lead in achieving business outcomes in eight business areas in our survey including cost reduction, business growth, faster time to market, gaining market share, developing new products/services, entering new markets, improved customer satisfaction and frictionless user experiences.

Significantly, Cyber Risk Takers secure a higher cyber budget—and yet successful breaches are still twice as high as Business Blockers and 10 percentage points higher than The Vulnerable. Securing more budget doesn't translate to better cyber resilience.

Despite being focused on business objectives, Cyber Risk Takers' performance is among the poorest when it comes to average share of successful breaches and the average share of significant attacks (Figure 8).

**Figure 8. Impact of breaches on Cyber Risk Takers**




Source: Accenture State of Cybersecurity Resilience 2021, security executives
(N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

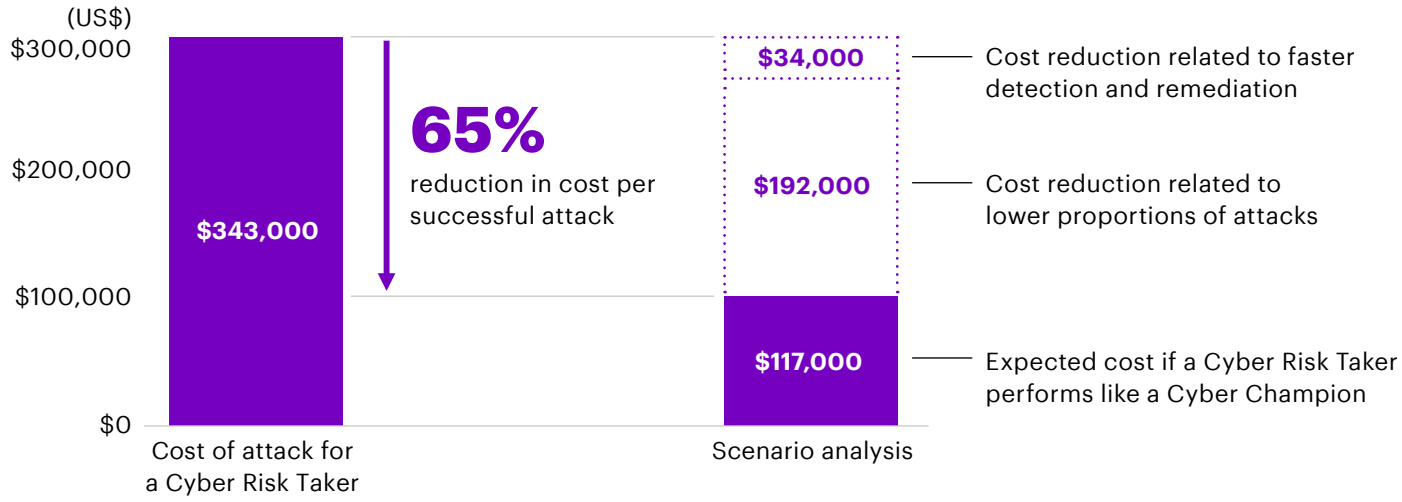
## Why alignment matters

And they have a resource allocation problem —they lack visibility, unclear metrics delay investment decisions and they demonstrate a poor allocation of funds. With fewer CISOs authorizing the security budget it may be that these Cyber Risk Takers are cash rich but expertise poor when it comes to how to spend their cybersecurity budgets.

While a focus on alignment alone may enable potential for meaningful business benefits, without a foundation for cyber resilience companies will be at greater risk and have higher costs of cybersecurity.

Cyber Risk Takers could reduce costs by 65% per successful attack if they increased their performance to Cyber Champion levels, with savings of about US$226,000 per attack (Figure 9).

**Figure 9. Value at stake if Cyber Risk Takers perform like Cyber Champions**




Note: We assign the same level of performance to Cyber Risk Taker companies as the Cyber Champion companies across metrics of cyber resilience such as speed of detection/remediation and proportion of significant attacks and simulate the cost outcomes. N=885

# Cyber Champions

**Cyber Champions are the cream of the crop. Like Business Blockers, Champions are among the top 30% in at least three of the four cyber resilience criteria. What sets them apart is their close alignment to the business strategy.**

## Why alignment matters

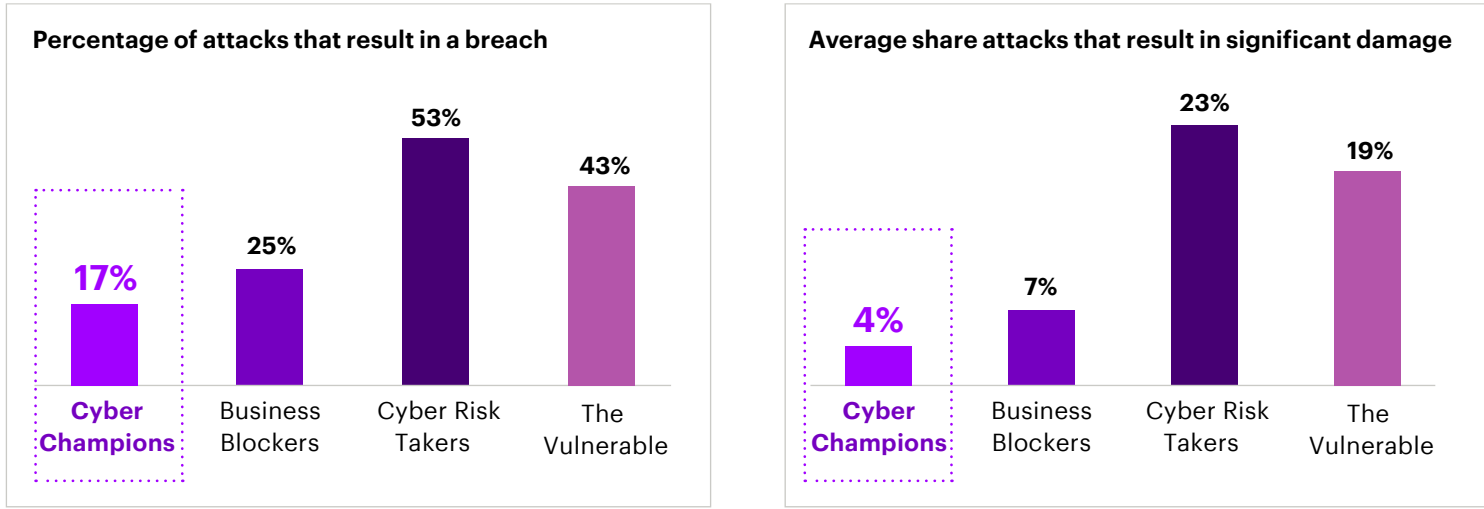
The number of successful breaches experienced by Cyber Champions is 8 percentage points lower than Business Blockers and 36 percentage points lower than Cyber Risk Takers and they experience the fewest significant attacks (Figure 10).

Cyber Champions have a speedier response to detection and remediation—a day extra of being fully operational can make all the difference to the bottom line.

Cyber Champions are better able to protect themselves from loss of data—about 4% of Cyber Champions lose more than 500,000 records—6.5X less than Cyber Risk Takers at 27%.

Some of the Cyber Champions' success in aligning with the business could be as a result of the fact that they have a higher share of business unit leads responsible for cybersecurity —nearly twice (1.9X) that of Cyber Risk Takers.

**Figure 10. Impact of breaches on Cyber Champions**

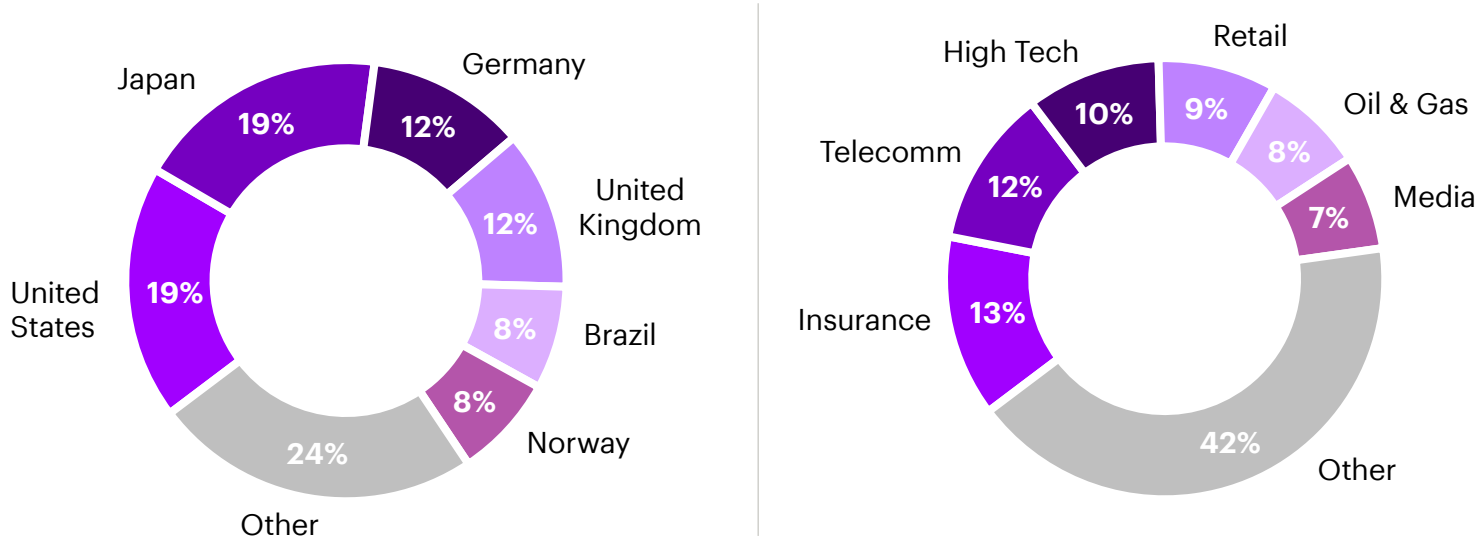



Source: Accenture State of Cybersecurity Resilience 2021, security executives
(N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

## Why alignment matters

Top countries and industries represented in Cyber Champions include the United States, Japan, United Kingdom and Germany and insurance, telecommunications, high tech and retail respectively (Figure 11).

**Figure 11. Cyber Champions—top countries and industries represented**



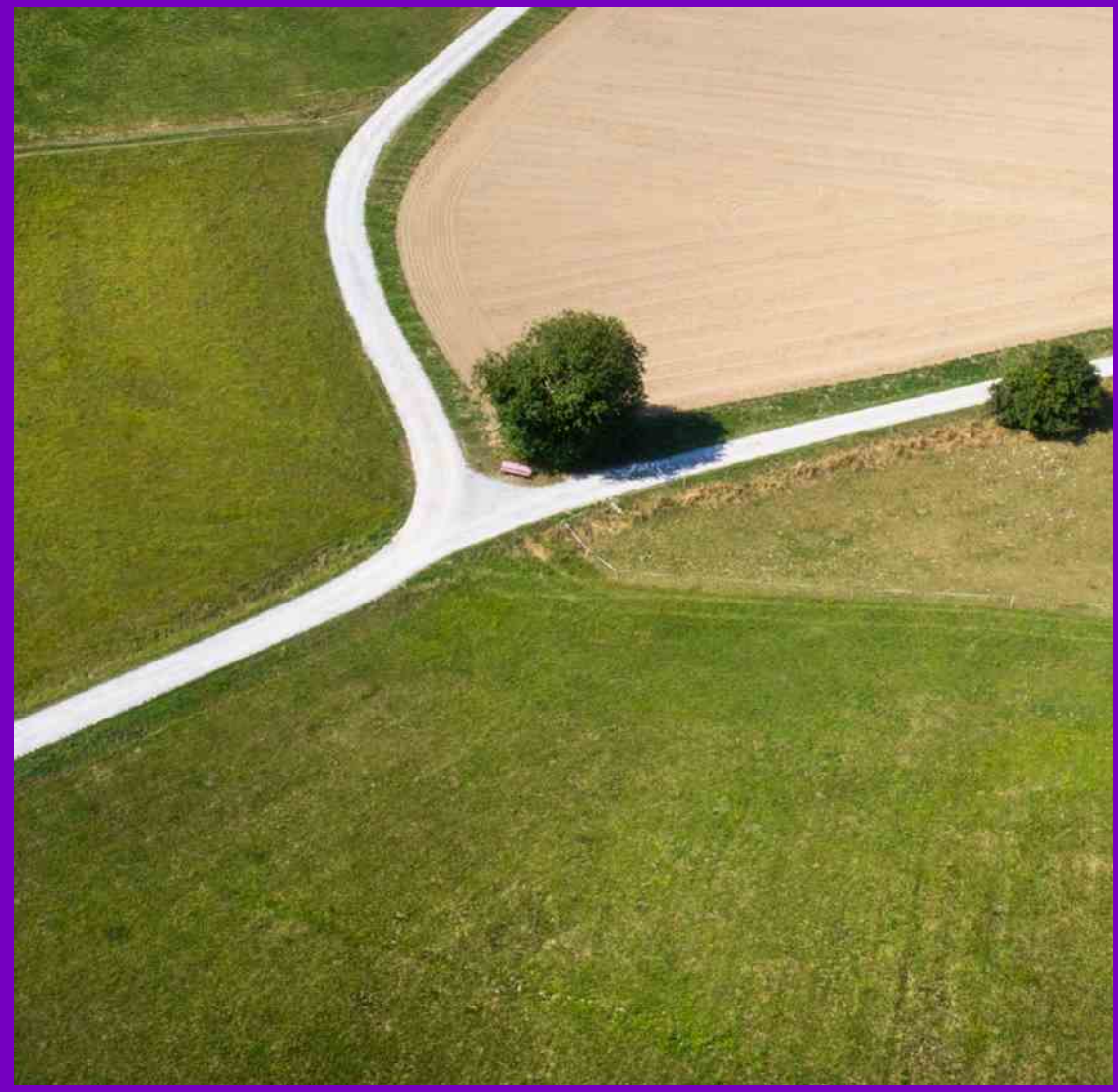

Source: Accenture State of Cybersecurity Resilience 2021, Cyber Champions (N=172)

# How to be a Cyber Champion

**Give CISOs a seat at the top table**

**Be threat-centric and business aligned**

**Get the most out of secure cloud**



# Give CISOs a seat at the top table

CISOs must move away from security-focused silos and collaborate with the right executives in the organization to understand business risks and priorities. By drawing on the experience and insights of the wider leadership team, CISOs can gain a broader perspective that serves the whole business well.

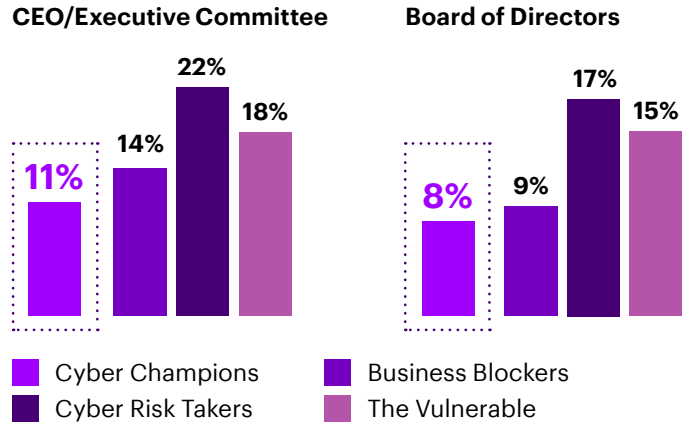
We found that Cyber Champions set themselves apart in terms of their reporting structures. Around 70% of the group report to the CEO and Board and they demonstrate a far closer relationship with the CFO—reporting is 7X higher than the other groups.

And Cyber Champions tap into these relationships when it comes to defining the strategy. They consult most with CEOs (51%) and CFOs (49%) when developing their organization's cybersecurity strategy—almost twice as much as the Business Blockers.

When it comes to budget authorization, only 19% of Cyber Champions have their budgets authorized by the CEO or Board, compared to 23% for Business Blockers and 39% for Cyber Risk Takers (Figure 12). This suggests that Cyber Champions have more autonomy when it comes to the purse strings and are less reliant on the CEO and Board for approval.

> "The business is heavily aligned with the CISO: The reason is very simple. Cyber is one of the top three priorities communicated by our chairperson and by top management... but if you don't have the okay from cyber, the product simply doesn't move on."
>
> CISO, Regional US Bank

**Figure 12. Cyber Champions have more autonomy: only 19% have their budget authorized by the CEO or board**




Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

# Be threat-centric and business aligned

CISOs only have to reflect on the 160% year-on-year increase in ransomware events in 2020 to recognize that cyber attacks are prompting a "prevention is better than cure" approach.[5]

Given remediation can be 30X the cost of prevention, once a ransomware attack happens, one of the biggest challenges when it takes down an enterprise environment is understanding priorities. What is the most important system to recover in your network? What does your revenue rely on? What's most critical to your operations?

Keeping attackers out of your environment depends on security leaders closely aligning with the business as partners in driving down risk. This alignment helps to embed security into the business priorities.

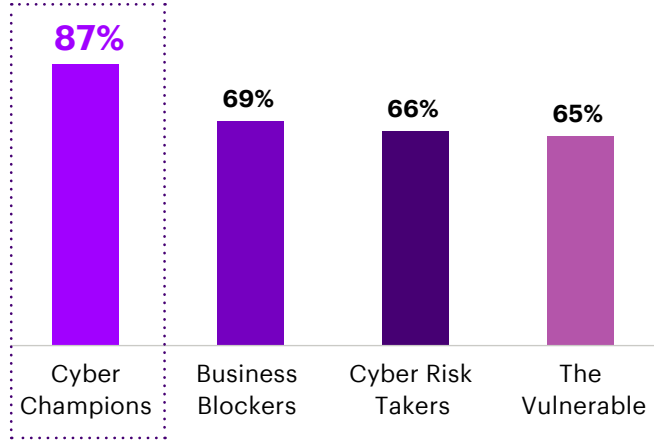
Cyber Champions understand the importance of balancing security and the business—they measure and monitor often to continuously improve their security function and enable the business to manage risk.

We found nearly 90% of Cyber Champions measure the maturity of their cybersecurity program at least annually or more frequently, 18% more than the Business Blockers (Figure 13). This indicates that Cyber Champions clearly understand the risks while Business Blockers may be blind to them.

By measuring and monitoring their risk profiles and making that data available to leadership, CISOs can better align with the business.

> "We track data in four areas: cybersecurity effectiveness, the company's cyber culture, cybersecurity readiness and cybersecurity resilience. We monitor how well we align our plans with core processes and what's going on in the business."
>
> CISO, Large Mining Company

**Figure 13. Cyber Champions measure cybersecurity maturity frequently**




Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

# Get the most out of secure cloud

Security should be embedded consistently in the cloud. Too often, it is added at the end of the cloud-first journey and can delay business outcomes—or result in having to do the costly work all over again.

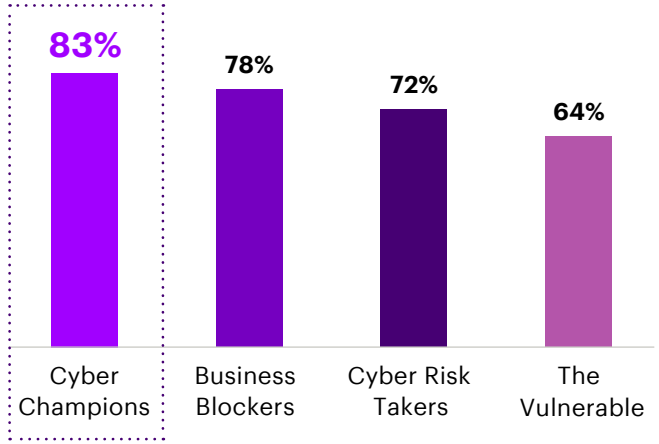
Cloud security can enable better business outcomes by being fast, frictionless, scalable, proactive and cost effective.[6]

With an accelerated shift toward using the cloud, it is important to drive full value from it. When moving to the cloud, organizations should seize the opportunity to reset their security posture, earlier and more effectively —like our Cyber Champions do.

Most Cyber Champions (83%) say that security is a major consideration when moving operations to the cloud versus 70% of the overall sample. Cyber Champions are better at baking security into their cloud initiatives—they don't see security involvement as a significant barrier to cloud discussions (Figure 14).

Cyber Champions know what to do; they work in close alignment with the business to migrate to the cloud more securely.

**Figure 14. Cyber Champions move to the cloud with security in mind**




Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

# Are security and non-security executives on the same page?

**Our latest survey shows that there are still differences in how security and non-security executives see things. In all, their responses highlight gaps between security and non-security executives in how they perceive security effectiveness, budget and attack risks (Figure 15).**

When we asked about the barriers preventing their organizations from realizing cybersecurity objectives, there was an average 14 percentage points difference between non-security and security responses on seven significant factors. In particular, they disagreed about security involvement in cloud discussions—43% of non-security executives versus 31% of security executives said that security was not part of the discussion and are now trying to catch up.

These differences of opinion may reflect higher confidence on the part of the security executives for their cyber resilience. Or it may indicate that security executives need to work harder at integrating into the business so that priorities are agreed and clear. Either way, it's important for security and business executives to better align so that business outcomes can be targeted, measured and met.

**Figure 15. Differences of opinion between security executives and non-security executives**

| | Security executives | Non-security executives |
|---|---|---|
| **Security effectiveness:** My organization is well-protected from cyber threats. | **52%** | **38%** |
| **Spending:** Estimated percent of IT budget spent on security in my organization. | **15%** | **26%** |
| **Attacks in my organization:** | | |
| • Number of attempted breaches | **270** | **180** |
| • Number of attempted ransomware attacks | **180** | **300** |

Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=4,244) and non-security executives (N=500)

# The path to cyber resilience

## Although this has been a year like no other, it has emphasized the critical role of cybersecurity within the business and how important it is for cybersecurity and business strategies to align.

We're seeing familiar challenges that we've noted in the past—cyber attacks are spiralling upward, security investments are still on the rise and security's relationship with cloud continues to prove challenging.

Even the CISOs stature in the organization has grown—more CISOs than ever report directly to CEOs or Boards (72% in 2021 compared with 59% in 2020) and they're being given more direct control over their budgets.

In such a climate, where change is the byword, seeking out the best way to run security operations can make all the difference. It is not a one-way street.

As we have seen in this report, organizations that focus solely on business growth are missing out on the benefits of cyber resilience. And there are gains for those organizations that proactively seek out a strong synergistic alignment between security and the business.

By aligning their cybersecurity efforts with the business strategy, organizations can not only achieve better business outcomes, but also seize an advantage in the race to cyber resilience.

> "Leadership is now highly invested in things like cyber resiliency; there's a willingness to put more money that way. It's a conversation that's happening right now and it's better than it ever was before."
>
> CISO, Insurance industry

# About the research

## Demographics

The State of Cybersecurity Resilience 2021 research surveyed 4,744 executives in March and April of 2021 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$1B or more from 18 countries and 23 industries across North and South America, Europe and Asia Pacific.

**4th**
Annual Research Study

**US$1B+**
Revenues

**4,744**
Total respondents

**4,244** Security respondents

**500** Non-security respondents

**18**
**Countries**

- Austria (50)
- Australia (372)
- Brazil (177)
- Canada (194)
- France (369)
- Germany (364)
- Ireland (100)
- Italy (307)
- Japan (388)
- Netherlands (118)
- Norway (124)
- Portugal (100)
- Saudi Arabia (111)
- Singapore (102)
- Spain (251)
- Switzerland (50)
- United Kingdom (489)
- United States (1,078)

**23**
**Industries**

- Aerospace & Defense (101)
- Automotive (101)
- Banking (345)
- Biotech (11)
- Capital Markets (121)
- Chemicals (200)
- Consumer Goods & Services (440)
- Energy (210)
- Healthcare Payers (102)
- Healthcare Providers (102)
- High Tech (343)
- Industrial Equipment (434)
- Insurance (456)
- Life Sciences (139)
- Media (222)
- Metals and Mining (100)
- Pharmaceutical (49)
- US Federal Services (100)
- Retail (438)
- Software & Platforms (220)
- Telecommunications (207)
- Travel & Hospitality (93)
- Utilities (210)

## Our methodology

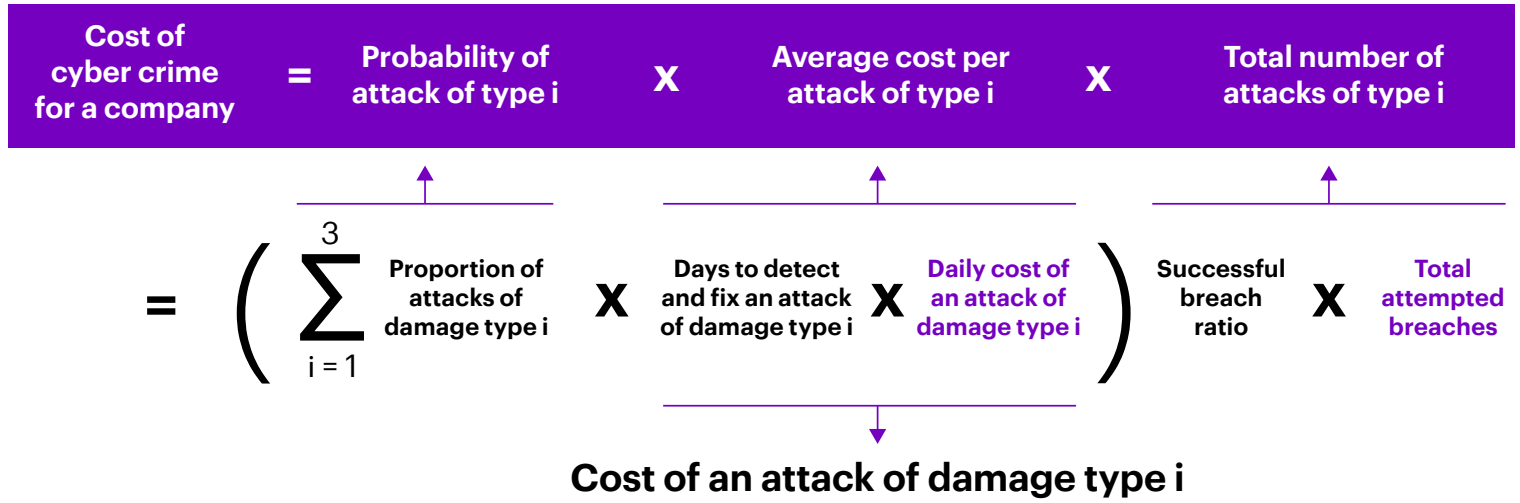
Continuing our approach from previous years, we first defined **leaders in cyber resilience** as those who exhibit high-performance (top 20% of sample) in at least three of the following four performance criteria:

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

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 cyber crime for a company: the average cost per attack, multiplied by the total number of attacks.

The average cost per attack was the sum of the product of the daily cost of an attack by damage type, the days to detect and fix an attack of this damage type and the proportion of attacks for this damage type. The total number of attacks was the product of the security breach ratio and the total number of attempted breaches (Figure 16).

**Figure 16. Modeling formula to assess the cost of cyber crime**




Note: For the modeling exercises, we ran our analysis on a sample of 3,455 organizations that responded to all key components of the cost of cyber crime model. We assume variables in purple to remain constant in the series of "what if" experiments we conduct. Damage type includes attacks that are: (1) Significant, (2) Moderate, (3) Minor and (4) No impact.

## About the research

We ran our modeling analysis on a sample subset of 3,455 organizations that responded to all key components of the cost of cyber crime model.

Next, we examined **how strength of alignment between cybersecurity strategy and business strategy impacted cyber resilience.** Strength of alignment was defined by the following components:

1. The extent to which business objectives (e.g. cost reduction, business growth, customer satisfaction) are a priority for the organization's overall business strategy and the extent to which cybersecurity is consulted when planning for these business areas.

2. The extent to which respondents agreed or disagreed with statements on alignment (e.g. organization-wide involvement in understanding and mitigating cyber risk, and leadership involvement in setting cyber strategy and budgets.)

Both components are rescaled to between 0 and 100 and averaged to arrive at a final alignment score. Taking these definitions of cyber resilience and alignment, we grouped our sample into four levels of cyber resilience:

**Business Blockers**

15% of the survey sample

522 respondents

**Cyber Champions**

5% of the survey sample

172 respondents

**The Vulnerable**

55% of the survey sample

1,876 respondents

**Cyber Risk Takers**

25% of the survey sample

885 respondents

We then continued our "what if" experiments based on the equation presented on page 30 to study the return on investments from alignment.

# References


1. Accenture Research analysis of 1,548 Securities Exchange Commission 10-K quarterly reports across 500 companies during 2017 to 2020

2. Third Annual State of Cyber Resilience, Accenture 2020

3. The Cloud Continuum, Accenture 2021

4. Make the Leap, Take the Lead, Accenture 2021

5. Ransomware response and recovery, Accenture 2021

6. Secure Cloud, Accenture 2021

## About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 624,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.
**Visit us at www.accenture.com**

## About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us **@AccentureSecure** on Twitter or visit us at **www.accenture.com/security**.

## 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**.



12460920

210573