Elevating the Cybersecurity Discussion:

Why CEOs need to get more involved in securing the business

accenture

Seemingly overnight, the world has changed. The expanding, escalating and unpredictable cyber threat landscape has illustrated the urgent need to change our approach to cybersecurity.

While Russia's invasion of Ukraine remains within its borders, cyberwarfare is borderless. As expected, we've seen an increase in cyber threat activity, chatter and misinformation.

Governments around the world have sounded the alarm and asked critical infrastructure providers to operate at a heightened state of readiness. But how long can that be sustained? The old rules no longer apply. Intelligence sharing early and often must remain a key strategy in this conflict, including in the development of government recommendations for critical infrastructure.

The cybersecurity dimension of the conflict compounds the changing risk landscape brought about by wider geopolitical change, rapid digital transformation brought on by the pandemic and innovations that were already on the horizon: the metaverse, cloud, edge devices, IoT and quantum. And it brings to light the fact that—against increasingly well-funded, sophisticated and coordinated cyber criminals—efforts around cybersecurity, so far, have fallen short.

But business leaders have the power to turn the tide.

The world has changed and so must security

As the physical and digital worlds grow ever more connected, collaborative and complex, cybersecurity has become a business imperative. Organizations have responded by dramatically increasing their cybersecurity investments—yet breaches and threats continue to climb. Threat conditions will only worsen as digitalization, connectivity, data privacy laws and geopolitical tensions expand.

A profound change in how cybersecurity is viewed, planned and executed is needed. CEOs should not leave this change solely to IT or the security team. Rather, *they* must lead the change—a change that demands they create, instil and maintain trust with their customers, employees and vendors. That's what leading companies are doing.

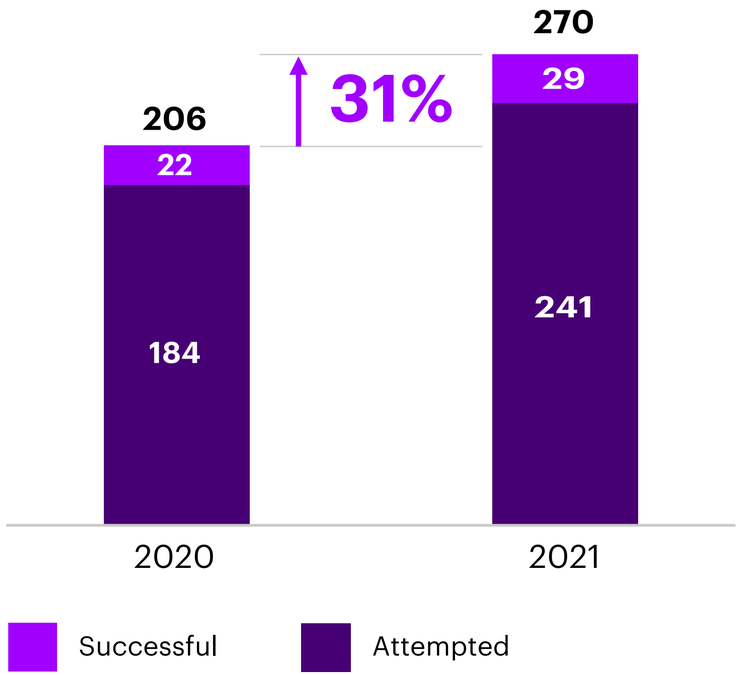
The pandemic fueled a quantum leap in digital adoption at every level. The migration of communications and data to the virtual world accelerated exponentially. It is a new world—not only one with more complexity and more threats, but also with more opportunity for those who get it right.

To succeed, CEOs should align their business and security teams to one cohesive strategy and plan of action to create safe, trusted environments for customers, employees and vendors. We believe CEOs have had the ability to change this dynamic all along, yet our latest State of Cybersecurity Resilience research among 4,744 global respondents (4,244 CISOs and senior security executives and 500 CEOs and CFOs) indicates only 5% of companies are getting business and security alignment right.[1] Put simply, the vast majority of businesses are not thinking about security in the right way.

Despite more investment, incidents, costs, and impact are rising

Our research found that companies faced an average of 270 attacks in 2021—a 31% increase over 2020[2] (Figure 1). As the rate of cybercrime grows, costs are rising. As a result, by 2025, industries worldwide could pay as much as US$10.5 trillion annually.[3]

Figure 1. Cyber attacks are up



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)

But such estimates do not consider the long tail costs of a breach that can extend for months to years. These may include substantial expenses that companies are not aware of or do not consider in their planning, such as lost data, customers and revenue from system downtime; drop in stock price; or damage to a brand's reputation.

Growing consumer concerns about data use are adding even further complexity. With the rise in data breaches and other incidents, many consumers are taking a closer look at who they do business with. According to one study, 88% of customers wouldn't use the services or purchase products from an organization they distrust, while more than a third (39%) had lost trust in a company due to a data breach or misuse of data they heard about.[4] The propagation of "fake" news and misinformation has further eroded consumers' trust. Research found that if a brand produced fake content about their services or products, more than half (59%) of consumers would stop buying that brand immediately.[5]

A natural response to these challenges is to think that investing more will solve the issue. Our research found that nearly half of CEO/CFOs in our study said that poor allocation of funds (47%) and lack of budget (46%) are preventing them from realizing their cybersecurity objectives.[6]

Yet, our research also found that security investment continues to rise. Security now accounts for 15% of all IT spend, five percentage points higher than reported in 2020.[7]

Given the current threat and cost trajectory, it is time for organizations to put more emphasis on allocating security investments for the desired outcome, rather than just investing more.

Security now accounts for 15% of all IT spend, five percentage points higher than reported in 2020.

Compliance does not equal security

We often find security is heavily driven by compliance requirements rather than business needs. Compliance is a checklist, while security is about outcomes and reducing impact. Guided by the mindset that "compliant equals secure," many organizations have yet to address basic cybersecurity practices, such as data security or a threat intelligence program.

As a result, governments and regulators are stepping in with initiatives aimed at improving organizations' cybersecurity, such as the U.S. President's 2021 Executive Order on Cybersecurity; Europe's efforts through the NIS (and soon NIS2) Directive; and Australia's recent critical infrastructure laws.

However, these solutions may not fully consider the context for and impact of implementation. For example, the United States Department of the Treasury's 2021 advisory is one of many initiatives to discourage companies from paying ransoms. On paper the prevention incentives may look good but the decision to pay or not to pay is rarely clear cut. For example, in healthcare the risk of sanctions could mean deciding between actions that save lives and those that risk lives if patient treatment is stalled by an attack. Likewise, for a manufacturer—who may be losing millions for every hour its machines are offline—making the payment in hopes of getting back online may feel like the right business decision.

Realistically, reacting to a mandate is a not a strategy to reduce risk. While organizations focus resources on compliance, hackers evolve their tactics, leaving organizations vulnerable and unprepared for the next big attack. CEOs must lead more permanent change—making preparedness, building trusted partnerships and cyber resilience strategic to the company—rather than relying on compliance to provide cybersecurity protection.

Cybersecurity accountability is still fragmented

While a growing corporate mantra is "security is everyone's responsibility," the criticality of information security has mandated that a single person be responsible for its oversight. This role has often been held by the CIO, but in the last 15 years more organizations have shifted security to the CISO role. According to the latest CISO 500 study, CISO representation at Fortune 500 companies jumped from 70% in 2018 to 100% in 2021.[8]

Despite a greater need and new roles to manage security, organizations we surveyed still grapple over who is responsible for cybersecurity.

Nearly half of CEOs/CFOs surveyed said siloed responsibilities (49%) and unclear accountability (51%) are barriers to realizing their cybersecurity objectives.[9]

One solution to overcoming these barriers is for security leaders to report directly to the CEO, the COO or the board. This reporting structure ensures that CISOs have a seat at the table and that C-suite leaders and the board are directly informed of potential risks to the organization, what mitigation efforts are in place and the company's true security posture. This also helps spread accountability for security across the wider leadership team, rather than siloing responsibility with the CISO.

In turn, CISOs draw on the experience and insights of the wider leadership team, helping them gain a broader perspective that serves the entire business.

> Nearly half of CEOs/CFOs surveyed said siloed responsibilities and unclear accountability are barriers to realizing their cybersecurity objectives.

A cohesive strategy that aligns security and business is needed

Our research explored characteristics of leaders in cyber resilience and 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.

We identified a group of Cyber Champions—organizations that strike a balance between excelling at cyber resilience and aligning with the business strategy, incorporating security from the start to achieve better business outcomes. These Cyber Champions are better at stopping attacks, finding and fixing breaches faster and reducing their impact. However, only 5% of the 4,500 companies surveyed have achieved this level of excellence[10] (Figure 2).

> We identified four levels of cyber resilience, including an elite group of Cyber Champions

Figure 2. Four levels of cyber resilience

Yet, our research found there are still gaps in alignment between CISOs and other senior leaders. When asked about their program's effectiveness, more than half of security executives (52%) report that over 75% of their organization is actively protected by their cybersecurity program, while only 38% of CEO/CFOs report the same level of confidence. And considering barriers that prevent their organizations from realizing cybersecurity objectives, there was an average 14 percentage points difference between non-security and security responses on seven significant factors[11] (Figure 3).

Figure 3. CEO/CFOs more inclined to see barriers to reaching objectives

CEO/CFOs need to lead the change via closer engagement with Security executives and alignment of business strategy

To what extent does each of the following prevent your organization from realizing your cyber security objectives?

Represents total responses for Significantly and Very Significantly

Part of this misalignment could stem from a continued, outdated view that cybersecurity is an IT responsibility, rather than a business challenge. When asked who is responsible for cybersecurity, most (91%) CEOs/CFOs put the responsibility squarely with IT.[12]

This mindset often results in security being siloed and viewed as a maintenance or tactical concern, rather than being seen as a strategic enabler embedded in every facet of an organization: research and development, risk management, workforce, procurement, mergers and acquisitions, platforms and operations.

The accelerated adoption of digital technologies across all areas of the business —cloud computing, 5G, Industrial Internet of Things, metaverse, quantum computing —has prompted new features, functions and workflows. Increasingly, purchasing decisions for these new technologies are driven from the C-suite. Security needs to be embedded into these new initiatives from the start to ensure that increased risks are addressed up front—rather than retrofitting security on the back end. This could save time and money. By aligning and building cybersecurity into every facet of the business, organizations can achieve better business outcomes and better cyber resilience.

91% of CEOs/CFOs put the responsibility for cybersecurity squarely with IT.

The cyber-savvy CEO

Now is the time to be a cyber-savvy CEO who drives trust by making cybersecurity an integral part of the business.

Here are some considerations to shape a path forward:

- How well is your business strategy supported by your security strategy? Is it helping you take calculated risks and protecting your most critical assets or is it a focused on addressing compliance requirements? Establish a business cyber protection strategy that is shaped to protect your most critical assets and corporate value.
- How do your business unit leads and core product and functional areas incorporate security into their decisions and operations? Is cybersecurity well integrated into your organization or is it siloed? Build cybersecurity into every facet of your organization to improve cyber resilience.
- Where is cybersecurity spending allocated within your organization? Focus on where you're investing, rather than just on how much you're spending.
- Do you know where your organization is most vulnerable? Conduct attack simulations to test your cyber resilience. Establish an incident response capability.
- Do you understand the risks of your business partners and third-party providers? Understand and manage third-party risks to help reduce your exposure to attacks.
- Are you tapping into your network to help prepare and educate yourself about cyber crises? Use your contacts who have experienced a serious incident to help educate and prepare for potential attacks.
- What is your relationship with law enforcement? Develop a collaborative relationship now for sharing threat intelligence, rather than waiting for a crisis to happen.

Solving the collective cybersecurity challenge requires a broader, more inclusive approach. An effective business cybersecurity strategy must be shaped jointly amongst the CEO, CISO, board and business leaders. The effort relies on CEOs to ask the right questions, challenge their organizations to identify and treat cyber risk effectively, be more attuned to how security investments are faring and lead the culture change to embrace security across the business.

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 CEO/CFO 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)

References

1. “State of Cybersecurity Resilience 2021,” Accenture, November 2021. https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
2. Ibid
3. “Cybercrime To Cost The World $10.5 Trillion Annually By 2025,” Cybercrime Magazine, November 13, 2020. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
4. Devanesan, Joe. “Customers are losing patience with data security issues.” Tech Wire, February 15, 2021. https://techwireasia.com/2021/02/customers-are-losing-patience-with-data-security-issues/
5. Baduel, Farzana, “How ‘Fake News’ and Bogus Content Are Changing the Way Consumers Look at Brands,” Prowly, https://prowly.com/magazine/fake-news-bogus-content-changing-way-consumers-look-brands/
6. “State of Cybersecurity Resilience 2021,” Accenture, November 2021. https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
7. Ibid
8. “List Of Fortune 500 Chief Information Security Officers,” Cybercrime Magazine, May 23, 2021. https://cybersecurityventures.com/ciso-500/
9. “State of Cybersecurity Resilience 2021,” Accenture, November 2021. https://www.accenture.com/us-en/insights/security/invest-cyber-resilience
10. Ibid
11. Ibid
12. Ibid

About the authors

Paolo Dal Cin
Global Lead
Accenture Security

Paolo oversees the full spectrum of Security services globally and is a member of the Accenture Global Management Committee. He most recently led the Security practice in Europe. Prior to that, he led and built the Accenture Security practice in Italy, central Europe, Greece, Latin America and the Middle East. Paolo brings more than 20 years of experience working with clients across multiple industries such as telecommunications, media, financial services, utilities and the public sector. He specializes in cybersecurity strategy, business resilience, cyber defense, cloud protection, incident response and managed security services.

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.

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, **LinkedIn** or visit us at **accenture.com/security**.

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, Technology and Operations services and Accenture Song—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 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 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.

Visit us at **www.accenture.com/research**.

220002