

How financial services boards are addressing top cyber risks



**EY**

Building a better  
working world

# Content

- 3 Cybersecurity tops the board and C-suite agenda
- 7 Empowering CISOs and cybersecurity teams
- 9 Leading practices and actionable insights for oversight and governance
- 11 Looking ahead: the long game of cybersecurity

## Cybersecurity is a top strategic and tactical priority for boards and senior management across all industries.

It's an especially urgent matter within financial services because – to paraphrase the old joke about why bad guys rob banks – that's where the money is. However what does the most damage, losing money or trust? Trust can be damaged by a cyberattack and with attacks increasingly focused on brand reputation and information assets the potential impact to trust is of significant concern to financial institutions.

Financial services board directors clearly recognize that they are under attack and understand the high stakes. They are challenging themselves to think differently about cybersecurity and find new ways to promote it across the business and for their full network of stakeholders, including customers, regulators and third-party suppliers and partners.

The recent EY Cyber forum for US financial services board members, hosted by the EY Financial Services Center for Board Matters, explored these and other urgent issues, with an emphasis on the role of the board in providing strong oversight. Key themes included:

- ▶ **Financial services is a leader in cybersecurity**, but remains a top target for “bad actors” of all types. With proliferating and increasingly sophisticated threats, boards must be on the lookout for complacency and overconfidence. Ransomware attacks have increased dramatically largely because they are so effective and lucrative.
- ▶ **Intensifying regulatory oversight**, as demonstrated by the recent executive order, centered on data privacy, consumer protections, planned response to incidents like ransomware and more extensive reporting on breaches, particularly third-party and supply chain attacks.
- ▶ **Chief information security officers (CISOs) and other cybersecurity leaders** are under intense pressure to identify and manage threats but often struggle to engage with business leaders or development teams as strategic advisors. More boards are looking at the ideal CISO reporting relationships and seeking ways to ensure that CISOs can promote innovation to become business enablers.
- ▶ **“Trust-by-design” principles and “zero-trust” access management** are among the leading practices being adopted across the industry. Trust-by-design makes security an enabler of, rather than a barrier to, innovation while zero-trust has emerged in response to the increasing number of third-party attacks.
- ▶ **The ability to quantify risk and track progress are critical** for companies that want to stay ahead of the latest threats – and for boards that want to enhance oversight, ask tougher questions and make more confident decisions about cybersecurity. Better data – rather than simply more data – is also essential.

This report highlights key points from the discussion, including real-time results from surveys conducted during the event.

# Cybersecurity tops the board and C-suite agenda

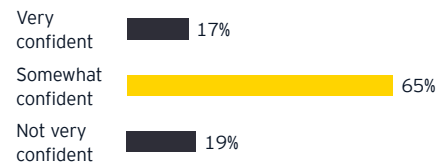
## More sophisticated threats raise the stakes

In the EY 2019 CEO Imperative Survey, national and corporate cybersecurity was the top global challenge to business growth and the global economy.<sup>5</sup> The COVID-19 pandemic only intensified the threats, thanks to new vulnerabilities created by widespread remote working.

In one of our in-session surveys, we asked participants if they would be surprised or prepared if a breach occurred tomorrow. A full 85% of participating directors said they would not be surprised, but prepared. A similar proportion, 81%, are either very confident (16%) or somewhat confident (65%) that their board has the necessary understanding to fully evaluate the cyber risks facing their organization and the measures it is taking to defend itself. Across all industries, that figure is 48%, according to the EY 2020 Global Information Security Survey.<sup>6</sup>

These results reflect the relative maturity of cybersecurity and resilience strategies across the financial services industry. Given the variety and pervasiveness of risks (including increasing attack sophistication, third-party exposures and the vulnerabilities associated with more advanced technology), financial services boards must remain vigilant.

### Director's confidence that their board has the necessary understanding to fully evaluate cyber risk facing the organization and the measures it is taking to defend itself:



### State of cybersecurity:

**59%**

of companies have experienced a significant or material breach in the last 12 months<sup>1</sup>

**3.8 million**

is the average estimated cost per data breach for an organization in 2020<sup>2</sup>

**\$10.5 trillion**

in damage related to cybercrime is projected to hit annually by 2025<sup>3</sup>

**6 months**

is the average length of time for companies to detect data breaches, even major ones<sup>4</sup>

<sup>1</sup> "The risky six: Key questions to expose gaps in board understanding of organizational cyber resiliency," the Institute of Internal Auditors (IIA) and Ernst & Young LLP, The IIA website, February 2021, © 2021 The Institute of Internal Auditors.

<sup>2</sup> "Cost of a Data Breach Report 2020," IBM website, [www.ibm.com/security/digital-assets/cost-data-breach-report](http://www.ibm.com/security/digital-assets/cost-data-breach-report), accessed 22 July 2021.

<sup>3</sup> Steve Morgan, "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025," Cybercrime Magazine, 13 November 2020, © 2021 Cybersecurity Ventures.

<sup>4</sup> Devon Milkovich, "15 Alarming Cyber Security Facts and Stats," Cybint, 23 December 2020, © 2021 Cybint.

<sup>5</sup> "EY CEO Imperative Study 2019: For CEOs, are the days of sidelining global challenges numbered?" EY website, [www.ey.com/en\\_gl/growth/ceo-imperative-global-challenges](http://www.ey.com/en_gl/growth/ceo-imperative-global-challenges), accessed 22 July 2021.

<sup>6</sup> "How does security evolve from bolted on to built-in? Bridging the relationship gap to build a business aligned security program, EY Global Information Security Survey 2020" EY website, [www.ey.com/en\\_gl/consulting/how-does-security-evolve-from-bolted-on-to-built-in](http://www.ey.com/en_gl/consulting/how-does-security-evolve-from-bolted-on-to-built-in), accessed 22 July 2021.

## An expanding “attack surface” – how the pandemic increased cyber risk

Remote working has expanded the attack surface. In the rapid shift to all-digital working, 60% of companies either abbreviated or skipped security and compliance checks as they stood up the necessary systems to support remote working.<sup>7</sup> As a result, the number of devices that can be attacked by hackers increased significantly.

Behavioral threats also rose. Home-based workers (both company employees and third parties) began acting as proxy threats; with the notion that people are more likely to click on malware attachments or phishing attempts when they are bored or stressed. As hybrid working models become more common, these concerns will remain on CISOs’ radars.

---

<sup>7</sup> “EY CEO Imperative Study 2019: For CEOs, are the days of sidelining global challenges numbered?” EY website, [www.ey.com/en\\_gl/growth/ceo-imperative-global-challenges](http://www.ey.com/en_gl/growth/ceo-imperative-global-challenges), accessed 22 July 2021.

“

By any measure, 2020 was the worst year ever when it comes to ransomware and related extortion events.

**John Carlin**  
Former Acting Deputy Attorney General,  
U.S. Department of Justice



## The rise of ransomware and third-party attacks

Directors clearly see the increasing sophistication of attacks as the biggest challenge to cybersecurity risk management. Nearly two-thirds of respondents to our cyber forum in-session survey cited sophisticated attacks as the top challenge, with third parties coming in a distant second at 18% (see page 10 for full results).

That's no surprise given that bad actors are refining their tactics and adopting alternative and more coordinated vectors of attack. For example, any company identified as an acquisition target can count on increased probing from attackers, who will seek to embed Trojan horse software to enter the acquiring company's networks. As seen by the dramatic spike in ransomware attacks, the main goal is no longer simply to steal and monetize data.

Bad actors also seek back-door access to high-value assets through the source code repositories of third-party technology providers. That was the technique used for the SolarWinds attack, which affected hundreds of thousands of organizations, including key government agencies and was particularly innovative given it was a one-to-many attack vs. the traditional one-to-one attacks.<sup>8</sup>


---

<sup>8</sup> Katie Canales and Isabella Jibilian, "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal," *Business Insider*, 15 April 2021, ©2021 Insider Inc.

It's not just attackers who are getting more sophisticated. As more companies adopt advanced technology, they need more advanced capabilities to manage the unique risks associated with internet of things (IoT) sensors, drones and cloud-hosted tech. As a result, cybersecurity teams at some companies are now divided, with one group covering legacy tech and another focused on advanced tech. Given how scarce and expensive cybersecurity talent is, boards must ensure that these teaming efforts are closely aligned and well synchronized.

### **Closing the "back door" of third-party exposures**

While the focus on increasingly sophisticated attacks is justified, boards should be careful not to underestimate the risks of third-party connections. For example, as more large banks rely on third parties for non-core services, they must recognize how this transfer of risk has led to increased frequency and severity of attacks, as starkly demonstrated by the SolarWinds attack. The variety and velocity of threats will only continue to expand and accelerate.



Sophisticated attacks demand sophisticated strategies and iterative response plans

## More regulation is coming – is your organization ready?

Boards need to be aware of, and prepare for, likely regulatory changes. The Biden administration, the Federal Reserve, the New York Department of Financial Services and other authorities have all passed guidelines or conducted enforcements to drive increased accountability and governance of cyber risk. The focus is on incident response and recovery plans and more extensive reporting of breaches, including “view-only” breaches. Beyond more extensive data privacy requirements, regulators are interested in where and how CISOs fit into the three lines of defense and board responsibilities when cyber events occur.

The SolarWinds attack will also likely prompt regulatory follow-through because it confirmed that current defenses are inadequate. In response, the American Rescue Plan has set aside approximately \$10 billion for security improvements. The William M. Thornberry National Defense Authorization Act for Fiscal Year 2021 includes more than 70 measures designed to enhance security, including the restoration of the position of a national cyber director at the White House. This represents the primary steps towards greater coordination of defensive cyber campaigns across federal agencies and the private sector.

## Why cyber insurance attracts bad actors

## Cyber priorities across financial services

The top-priority risks and issues vary by sector. In banking and capital markets, responses to renewed regulatory interest are at the top of agendas for boards, especially as the number of matters requiring attention (MRAs) grows. Resilience, identity access management (IAM), privileged access management and insurance coverage are other priorities in banking.

Wealth and asset managers are focused on vulnerability management and identifying cyber risk within business operations. For CISOs, the challenge is to correlate the risk framework and controls data to quantify vulnerabilities at the appropriate risk level.

For insurers, ransomware is the top priority because they are both vulnerable to such attacks and facing more frequent and larger claims to other companies that are victimized. In fact, ransomware attacks have become so pervasive and expensive that they are now commonly referred to as “extortionware.” Insurers have become a “honeypot” for hackers, because their data confirms which companies have cyber insurance and thus are attractive targets given their likelihood to pay.

Institutions may see their cyber insurance rates increase quite significantly in the future as well as tighter language limiting coverage and the growing prevalence of ransomware exclusions. Thus, boards must seek to understand the exposures via policy language and protections for policy data and be wary of significant changes to coverage.

### Key questions for directors to ask around ransomware and cyber insurance:

- ▶ In the event of a ransomware attack, what is your governance process for deciding whether to pay or not?
- ▶ Has the company conducted ransomware-attack simulations to identify vulnerabilities and assess your preparedness to respond?
- ▶ Is cyber coverage affirmative (i.e., not “silent” or covered under a non-cyber policy)?
- ▶ Is ransomware coverage included upon renewal?



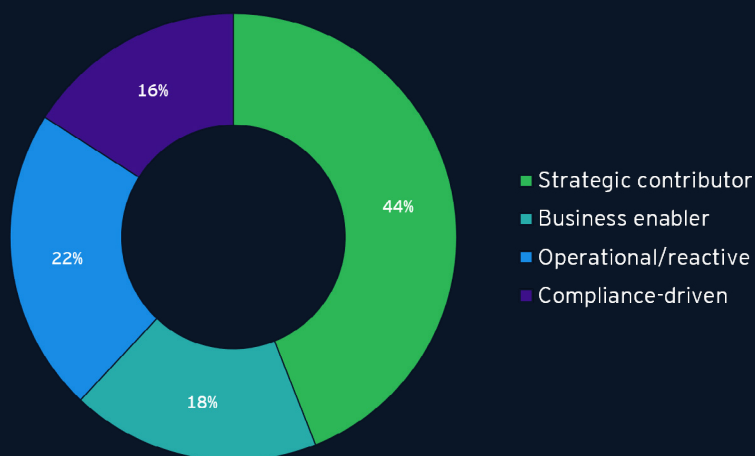
# Empowering CISOs and cybersecurity teams

As boards seek to expand their knowledge and further harden company defenses, they are paying closer attention to the role of the cybersecurity function and the critical role played by CISOs. Our cyber forum in-session survey question about CISOs demonstrated again that financial services are more mature than other sectors. Certainly, top-performing CISOs are business enablers, but in other sectors, it is more common for CISOs to play primarily operational or compliance-centric roles. The fundamental question is whether CISOs should function as security guards or strategic advisors who can contribute to innovation and growth.

For their part, CISOs and other cyber leaders are asking how they can modernize cybersecurity practices and techniques to meet risk appetites, even as threat levels inevitably rise and attackers become more determined and resourceful. Everyone knows that CISOs have a big job to do: identifying threats, plugging vulnerabilities, assessing the financial impacts of breaches and providing vital information and critical insights to boards.

However, the formidable challenges faced by many CISOs are not well recognized across organizations or boardrooms. Certainly budget cuts (which were common in the last year) and talent constraints make it harder for CISOs to do their jobs well, even as they are expected to produce higher returns on investments. They are often left out of key tech decisions and board-level discussions and can feel second-guessed by outside advisors, an experience they share with many chief risk officers (CROs). Given the pressures, it's no wonder the average tenure for CISOs is estimated at 18 to 26 months.<sup>9</sup>

## The CISO in your organization is primarily:



Source: EY Cyber forum for financial services board directors, 29 April 2021.

<sup>9</sup> Steve Morgan, "24 Percent Of Fortune 500 CISOs On The Job For Just One Year," Cybercrime Magazine, 13 July 2020, © 2021 Cybersecurity Ventures.



## Balancing business knowledge and tech expertise

For CISOs to be viewed as business enablers, they must collaborate early and often with development and innovation teams to embed strong security principles with new applications and enhanced experiences, particularly when application programming interfaces (APIs) are used to exchange data with external collaborators. They must also report with appropriate frequency and independence to the right leaders or board committees. Further, top CISOs do more than just share raw metrics with the board; they provide context and even build narratives that can help boards make strategic decisions.

The most effective CISOs handle the business-oriented and tech-driven parts of their jobs equally well, a particularly important balance in financial services. Plus, they know how to manage through budget shortfalls and are able to project a strong presence in front of the board and engage effectively with third-party cyber advisors.

## What boards can do to enable CISOs

In overseeing internal cyber resources, boards may need to advocate for CISOs to embrace more strategic, business-enabling roles and question whether the cybersecurity budget is appropriate and allocated to the right capabilities and activities. Further, they can explore where third-party advisors can best augment internal resources, including via managed services for baseline testing and network monitoring services.

Lastly, given the rush to remote working, boards should encourage CISOs to evaluate the current technology environment to find systems and tools that are redundant or underutilized. Rationalizing systems pays off by reducing both costs and eliminating potential vulnerabilities.





# Leading practices and actionable insights for oversight and governance

Given the breadth and complexities of cyber-related issues, directors are understandably interested in leading practices and proven approaches. Many questions during our cyber forum addressed what boards and senior management can do differently and which risk management and response techniques other firms have used effectively.

It's clear that boards will leverage both internal and external resources and a range of actions to strengthen their cybersecurity oversight, as highlighted by one of our in-session surveys.

## Which of the following would most enhance your board's oversight of cybersecurity risk?



Improved reporting from management



Increased frequency of cyber on the board agenda



Leveraging independent advisors to the board



Reconfiguring/strengthening board committee oversight



Participating in director-education programs



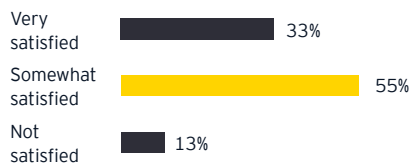
Adding new committee members with tech or cyber experience

Source: survey of participants in the EY Cyber forum for financial services board directors, day month year.

## More data and knowledge on – and available to – the board

Companies and boards recognize the need for board members to be more informed about cyber issues and risks. We've seen this focus in cyber-related disclosures of Fortune 100 companies where the percentage of companies discussing cybersecurity in the context of director qualifications has increased significantly in recent years from 39% in 2018 to 58% in 2020. Our expectations are this has increased further in the 2021 proxy season.<sup>10</sup> While boards recognize the need to be more informed, our cyber forum in-session survey showed only 33% of board members are very satisfied with the cyber reporting they receive, with 55% only somewhat satisfied and 13% not satisfied. Additionally, board members consider improved reporting their top priority in enhancing oversight of cybersecurity, followed by participating in director education programs and leveraging independent advisors. Adding new directors with technology/cyber expertise fell last on their list of enhancement options.

### How satisfied are you with the cyber-related reporting you're getting?



Source: survey of participants in the EY Cyber forum for US financial services board members, 29 April 2021.

<sup>10</sup> Stephan Klemesh, "What companies are disclosing about cybersecurity risk and oversight," EY website, 7 August 2020, © 2021 EY GM Limited.

When it comes to board reporting, defining the right objective metrics and delivering them on a sufficiently frequent basis is a challenge. Cyber risk is constantly evolving with changes to the business model, technology and increased sophistication of attacks. It's not just about protection but also what the bad actors are going after and their new behaviors. It is important to use a variety of techniques to quantify cyber risk and calculate the risk exposure and how that exposure is reduced if you make certain investments. Benchmarking, being able to show progress over time, and risk assessments are critical. Board reporting is often a look back at what the institution is working on today and investing in tomorrow – and not enough on the risks from technology disruptions in the marketplace, third party changes or new behaviors like those of social activists. There is a real need for coherency around the strategy of addressing these evolving risks and hearing from CISOs and external advisors more often (i.e., quarterly), whether in committees or to the full board, can help build the knowledge base, strengthen decision-making and give the board the unfettered access to ask these challenging questions.





## Looking ahead: the long game of cybersecurity

Financial directors understand just how big an issue cybersecurity represents – both in presenting significant risks, but also in providing an opportunity to differentiate based on trust. They are well attuned to the likelihood of new regulations and the need for actionable insights and proven practices they can apply immediately. They also understand that they are playing a long game. Whether or not the rest of 2021 feels like a return to normalcy, directors can be sure that cybersecurity will be high on their agendas for the years to come.

## About the EY Financial Services Center for Board Matters

Financial Services Center for Board Matters helps financial services boards of directors to identify, understand and navigate complex global and domestic sectors, regulatory risks and opportunities facing their firms. We help directors provide effective oversight of their firms by asking better questions of management and enhancing board committee, and individual director performance and effectiveness. We help champion the benefits of strong board governance and facilitate engagement of directors with peers and other key stakeholders – such as shareholders and regulators – to stay abreast of trends and leading practices. We drive board refreshment by identifying, sourcing, and introducing qualified, diverse director talent and promoting and enabling diversity and inclusion. Contact us at [fs.board.matters@ey.com](mailto:fs.board.matters@ey.com) for more information.

## EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](http://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](http://ey.com).

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

### What makes EY distinctive in financial services

Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus – to build a better financial services industry, one that is stronger, fairer and more sustainable.

© 2021 Ernst & Young LLP

All Rights Reserved.

US SCORE no. 13580-211US

2106-3790442

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

[ey.com](http://ey.com)

## Ernst & Young LLP contacts

### Kris Lovejoy

EY Global Consulting Cybersecurity  
Leader

[kristin.lovejoy@eyg.ey.com](mailto:kristin.lovejoy@eyg.ey.com)

### Dave Burg

EY Americas Cybersecurity Leader

[dave.burg@ey.com](mailto:dave.burg@ey.com)

### Steve Ingram

EY Americas Financial Services  
Cyber Leader

[steve.ingram@ey.com](mailto:steve.ingram@ey.com)

### Paul Haus

EY Financial Services Center for Board  
Matters Leader

[paul.haus@ey.com](mailto:paul.haus@ey.com)

### Mark Watson

EY Financial Services Deputy Leader

[mark.watson@ey.com](mailto:mark.watson@ey.com)

### Bill Hobbs

[bill.hobbs@ey.com](mailto:bill.hobbs@ey.com)

### Chrissy Warren

[chrissy.warren@ey.com](mailto:chrissy.warren@ey.com)

## Further reading

Six questions to expose gaps in your organizational cyber resiliency

[Download the complete report](#)

Data breaches and cybersecurity: managing third-party risk

[Download the complete report](#)

Three ways to protect organizations against ransomware

[Download the complete report](#)

Beyond COVID-19: Five ways to protect your organization and help it prosper

[Download the complete report](#)

Cybersecurity: How do you rise above the waves of a perfect storm?

[Download the complete report](#)

## Looking for more?

Access additional information and thought leadership from the EY Center for Board Matters at [ey.com/us/boardmatters](http://ey.com/us/boardmatters)