An integrated vision to manage cyber risk

Why cybersecurity is everyone's responsibility in today's financial services organization

EY
Building a better working world

Contents

Introduction

Today's cyber attacks are becoming more numerous, more frequent and existentially more threatening than ever before. The new generation of attackers are no longer always motivated simply by stealing funds and holding companies' information hostage. Instead, their aim can be to infiltrate and manipulate not just an individual company but the entire ecosystem to which it belongs.

Cyber risks are heightened as financial institutions transform their operations via new digital channels, automation and other advanced technologies. This is in addition to open banking beginning to reshape the sector's approach to data sharing.

Financial services companies continue to devote significant investments in securing gaps in their internal, online and digital frameworks, as those who want to exploit the weaknesses are getting smarter, bolder and more destructive. In response, regulators are heavily focused on managing systemic cyber risk and potential contagion across organizations and third parties.

The new cyber threats pose serious questions about organizations' preparedness to rebound from a breach — less than 14% of respondents to EY's latest *Global Information Security Survey (GISS)*[1] think their information security function fully meets their organizational needs. In order for confidence to grow, cybersecurity must become every employee's responsibility as it extends across an organization's customer, supplier and vendor ecosystem.

Contemporary cybersecurity extends beyond protecting sensitive information and systems from malicious external attack, into guarding identities, data privacy and vulnerability management on a vast scale.

For individual businesses, a new strategy for addressing cybersecurity is clearly needed. What we at EY call for is an integrated cybersecurity risk management approach that encompasses the resources and activities of the entire organization.

Jeremy Pizzala
EY Global FS Cybersecurity Lead

[1] *Path to cyber resilience: Sense, resist, react - EY's 19th Global Information Security Survey 2016-17,* www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016.

The need for an integrated cybersecurity vision

At their core, all financial services are based on trust. To win and maintain the trust of customers, financial institutions have to demonstrate consistent dedication to preserving confidentiality, confirming the availability of systems and services, and maintaining the integrity of data. As such, cyber attacks pose an unprecedented and existential threat to the sector.

Putting cybersecurity at the heart of business strategy will help the financial services sector maintain and even enhance the trust of consumers, regulators and the media. For a start, the C-suite can no longer assume that cybersecurity is solely the responsibility of the information security (IS) or information technology (IT) departments. Instead, financial services companies must make cybersecurity a core part of business strategy and culture. In doing so, they can enable the whole organization to understand the risks they face, embrace the innovation needed to counter those risks, and have the resilience to regroup and restore operations smoothly and efficiently in the wake of a cyber breach.

Companies need an integrated cybersecurity vision – one that brings together the various functions and dependencies with other parts of the organization, external key stakeholders and third-party suppliers.

This is no easy task but is achievable if companies prioritize the following five areas:

1. **Talent centricity**
   Build a culture that makes cybersecurity part of everyone's job and create a chief information security officer (CISO) role that is fit for the purpose of your organization.
2. **Strategy and innovation**
   Put cybersecurity at the heart of business strategy and ensure that new digital innovation includes cybersecurity at the outset.
3. **Risk focus**
   Understand broad trends and new regulations that will impact how cyber risk governance needs to evolve. Implement a three-lines-of-defense (3LoD) approach with clearly defined roles and responsibilities to manage cyber risk effectively.
4. **Intelligence and agility**
   Develop internal knowledge capabilities to use contemporary insights and information to assess the greatest cybersecurity threats. Deliver timely threat identification with a sharp focus on protecting the critical assets of the organization.
5. **Resilience and scalability**
   Be prepared to recover rapidly from a cyber breach while holding your ecosystem to the same cybersecurity standards that you follow as an organization.

These five priorities will help financial services companies develop a cyber-secure and aware business culture that will protect the company, offer competitive advantage in the marketplace and help to solidify trust in the sector.

Figure 1: An integrated cybersecurity vision

The pace of change in today's increasingly digitized world has led to the convergence of different risk disciplines that complement each other to address our clients' needs and those of their customers, regulators and business partners.

Figure 1 source: "Who are the typical cybersecurity stakeholders" EY model, 2017.

Priority one

Talent-centric – making employees cybersecurity smart

EY's *GISS* found that 81.8% of executives see employees as posing the biggest internal cybersecurity vulnerability – they are typically the people who click on a link and cause the problem to occur – but the reality is that it's becoming ever harder to differentiate legitimate from illegitimate information sources.

At present, there is a real skill set shortage in cybersecurity. Some estimates suggest there will be more than one million unfilled cybersecurity jobs worldwide by 2019.[2] The problem runs far deeper than cybersecurity experts, though. At all levels, there is a lack of training around how cyber risk should be handled in day-to-day business life.

Companies need to increase cybersecurity awareness training, but they also need to instill an understanding of how cyber risks impact different roles and individual projects, as well as the overall business.

In other words, if financial services companies are to fully grasp the existential risks posed by cyber risk, they must instill responsibility and agency for cybersecurity at the level of the individual. All employees, from new recruits to the C-suite, will need to realize just how a cyber attack can erode trust in the organization, and how damaging and far-reaching the consequences may be.

81.8% of executives see employees as posing the biggest internal cybersecurity vulnerability.

[2] "Cybersecurity skills shortage leaves companies vulnerable," *InformationWeek website,* www.informationweek.com/strategic-cio/security-and-risk-strategy/cyber-security-skills-shortage-leaves-companies-vulnerable.

The changing role of the CISO

To reach that level of competence throughout the company, executive boards are going to need smarter, more comprehensive reporting on cybersecurity risks, and board-relevant reports that speak the language they understand.

Reimagining the role played by the CISO is an important step. Just as organizations need to embrace cybersecurity as part of business strategy, they also need to expand the remit and influence of the CISO. The CISO should be driving the overall cybersecurity strategy, helping the board understand and calibrate their appetite for cyber risk. They ought to help the board understand the most critical assets to secure and advise where money needs to be spent. Then they need to take charge of making sure that investment is directed to the right parts of the business, calibrated to the level of cyber risk.

Some more cyber-experienced companies are already doing this. They're moving the CISO out from under their traditional reporting line, often to the chief information officer (CIO), to the chief risk officer (CRO). This sends a clear signal throughout the organization that cybersecurity is not a technology issue alone.

A second change taking place is that CISO roles are starting to be split into two — a tacit acknowledgment of the size of the ongoing work required by cybersecurity. One of the two emerging roles mirrors the traditional CISO — to look after the build and run of cybersecurity projects. The second role is new and is focused on strategy, policy and governance, as well as liaising with external regulators.

Rethinking the CISO role doesn't just make good strategic sense, it is smart management for an executive position that becomes a lightning rod when something goes wrong. CISOs know they are going to shoulder the blame when cybersecurity breaches occur, but if companies can provide them with broad-based support, funding and board engagement, not only will the organization be more secure, but it will be more likely to retain the experience and domain-specific expertise the CISO builds up in their job.

Talent-centric calls to action:

- Review your current cyber risk organization and operating model, and answer the questions: what is the CISO's role and reporting lines?
- Use social engineering exercises, coupled with training (focused on all employees, as well as targeted training for high-risk employees, such as executives and IT administrators) to raise awareness of individuals' roles in the organization's cybersecurity strategy
- Ensure that a clear identity and access management program is in place to limit access to those who need it, coupled with real-time monitoring tools that allow abnormal behavior to be quickly identified

Priority two

Strategic and innovative — integrating cybersecurity within the organization

Cybersecurity should be treated as another operational risk to be embedded in the organization's enterprise risk management framework. Boards are already comfortable discussing market risk, credit risk and operational risk. The time has come to include cybersecurity as another nonfinancial risk that should be evaluated and challenged.

The increase in frequency and scope of cyber attacks, combined with new and pending regulation, has already prompted some of the sector's biggest names to review their cyber defenses. Fifty-three percent of *GISS* respondents say their cybersecurity budget increased over the previous year. This, however, is just the start of what is required by the sector as a whole.

Companies need to integrate cybersecurity throughout corporate structure, strategy and culture, so that all employees (even contractors) participate actively in defending the business from cyber attacks. This starts with the board embracing a cyber strategy that takes the breadth of the business into consideration. Too often, boards take a narrow view of cybersecurity and direct resources toward perimeter security and security monitoring software, while failing to fully consider the business implications for other areas, including legal, compliance, customer service, and even marketing and corporate communications.

Protecting against a cyber breach might once only have kept the IT department awake at night, but today it has a direct and immediate effect on corporate reputation, new business acquisition and client retention.

Having someone on the board who is both knowledgeable about cybersecurity, and who has a direct link to the CRO and the operational risk committees, should be the minimum for best practice in this new cyber age. That way, the board will be equipped to make informed decisions about CISO funding needs and where that money is being spent.

At present, the CISO sits on the board at just 22% of financial institutions, according to our *GISS* respondents.

Figure 2: Who are the typical cybersecurity stakeholders?

The audience for cybersecurity is larger and wider than the CISO, embedded in different parts of our clients' organizations.

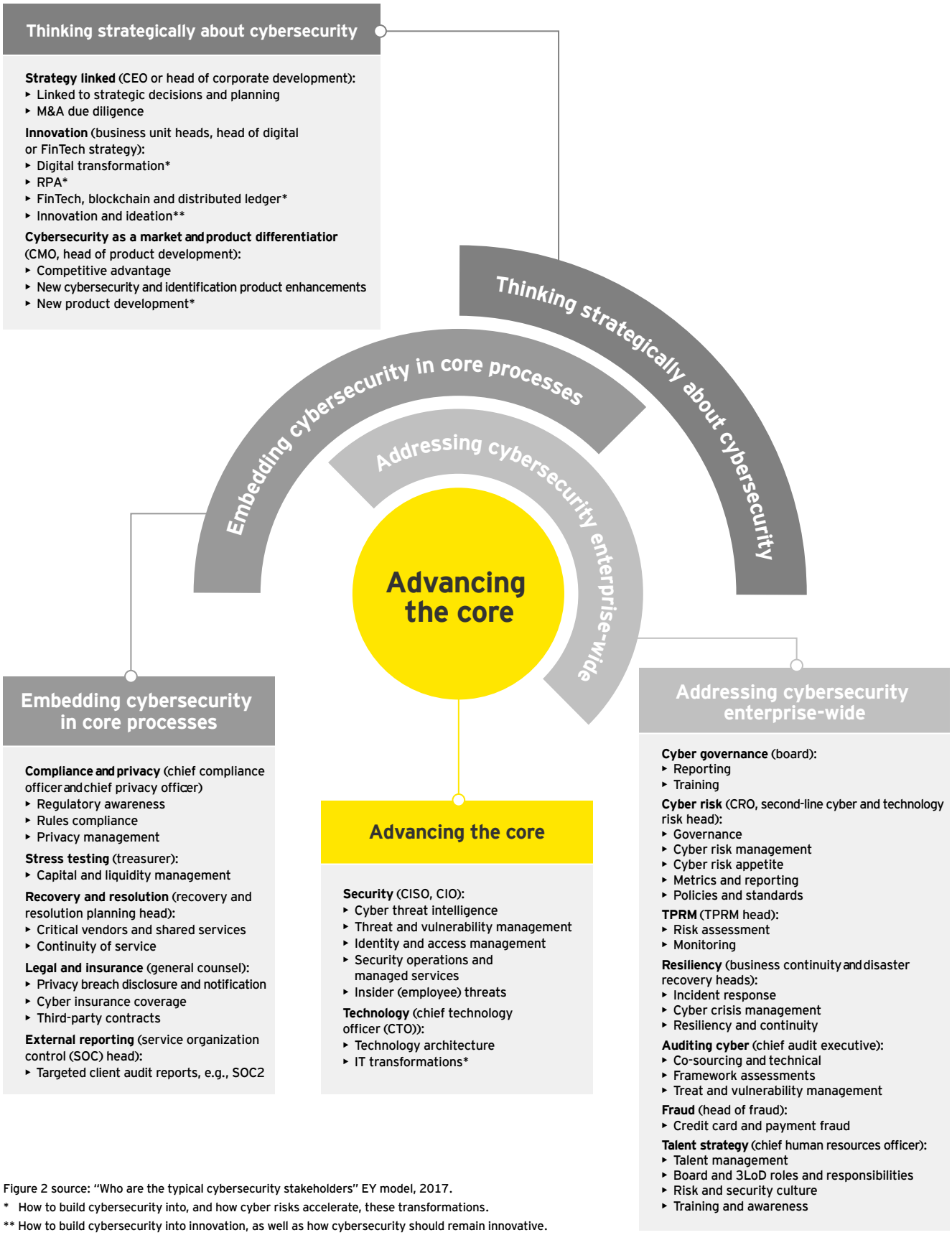


Figure 2 source: "Who are the typical cybersecurity stakeholders" EY model, 2017.

* How to build cybersecurity into, and how cyber risks accelerate, these transformations.

** How to build cybersecurity into innovation, as well as how cybersecurity should remain innovative.

Innovation that improves security

As financial services organizations increase the pace at which they adopt (and integrate with) new FinTech solutions, they need to make sure that their technological innovation also extends to their cybersecurity infrastructure.

Embracing **FinTech** can mean creating new, disruptive functions within existing organizations. FinTech "solutions" that promise to streamline and automate many parts of the sector, whether front-end consumer interaction or back-office operations, pose added cyber risks. However, they can also help improve security, as long as companies embed cybersecurity strategy into their FinTech plans at the outset.

Big Data will increasingly play a major role, particularly in the form of cyber analytics. As the name suggests, cyber analytics overlays statistical modeling that looks for abnormal behavior in sets of Big Data whether it's from the end-user side, or within the network or other parts of the IT infrastructure.

Cyber analytics on this scale can provide a smarter and more knowledgeable approach to tracking how cyber attacks affect systems. Clicking on a link in a spear phishing email, for example, might download malware onto a PC and then infect an organization's network. That malware will trigger certain behaviors in the network that are abnormal. Cyber analytics can help experts spot those abnormalities and react to them much quicker than traditional signature or rules-based defenses.

Cyber analytics on this scale can provide a smarter and more knowledgeable approach to tracking how cyber attacks affect systems.

Blockchain is often cited as the next big technological game changer for business and for financial services, in particular. Its inbuilt set of digital checks and balances, delivered through a decentralized list of transactions, offers a secure and transparent way of protecting digital payments and data privacy. Blockchain checks and balances can potentially be applied to everything, from identity access management to audit functions to TPRM services.

Artificial intelligence (AI) could also help counter cybercrime. The US Department of Defense's research arm (DARPA), has experimented with "robot hacking" to see how connected computers can defend themselves against cyber attacks.[3]

One area where AI looks set to have a real impact is in the triage and response or "react area" of security operating centers. Currently, that work is handled by people but, as attackers leverage AI and so attacks increase and mutate rapidly, companies will need their own AI to counter that threat. Humans won't be able to keep up with the volume of data that's going to be a hallmark of these attacks.

This will necessitate a transfer of trust and decision-making to AI — a big change from today, where humans determine whether to close down a network segment or change the firewall settings to prevent what looks like a particular attack.

Strategic and innovative calls to action:

- Implement tollgates that require cyber risk to be considered and signed off at the outset and at key points throughout all new business ventures — everything from FinTech and new product development to M&A activity
- Consider fusing cyber analytics with existing security operating center models to identify highly sophisticated but hard to detect breaches
- Review evolving areas of robotics and AI regularly, and look for early opportunities to experiment in controlled environments

[3] "Robot hackers could be the future of cybersecurity," *Scientific American website,* August 2016, www.scientificamerican.com/article/robot-hackers-could-be-the-future-of-cybersecurity.

Priority three
Risk focused — prioritizing what's critical

The fast-evolving nature of the cyber risk environment makes it increasingly important that financial services firms adopt a risk-based approach to cybersecurity. Firms simply can't protect everything to the same degree. Priorities matter.

The first step is getting cyber risk governance right. Boards of directors understand that cybersecurity is a major risk, perhaps even the number one risk. They know the risk is fast changing and that it's difficult to keep up with. Yet they struggle to determine how their governance should evolve. In practice, a broader set of trends will influence the future design of cyber risk governance. These include new privacy and data laws, the implementation of cybersecurity 3LoD, the need to build cybersecurity into innovation, and complying with new regulations and enhanced supervisory expectations. An appreciation of these broader trends is important for better design of governance.[4]

The management approach to cyber risk is also important. Depending solely or mainly on the first-line cybersecurity team is no longer acceptable. That group needs to be well resourced, focused and integrated. But first-line business leaders need to own cyber risks, and maintain and test necessary controls. After all, they should own and manage all risks that relate to their business.

[4] *Governing cyber risks in financial institutions,* EY, July 2017, www.ey.com/gl/en/industries/financial-services/ey-governing-cyber-risks-financial-services.

Figure 3: The role of the cybersecurity 3LoD

	Who are they?	What is their cybersecurity role?	What is their challenge?
First line	Business units and information security teams with direct accountability for owning, understanding and managing cyber risks	▸ Measure, monitor, manage and mitigate cyber risks and vulnerabilities within the board-approved cyber risk toleranace if front-line business units are working with the information security and cybersecurity teams ▸ Define the cyber risks and exposures each line of business faces ▸ Develop standards and procedures that implement the second-line cyber risk framework in the context of specific business risks	▸ Getting cybersecurity thinking embedded in day-to-day operations ▸ Getting the first line (not the cybersecurity group) to identify cyber risks properly, and develop and maintain strong controls
Second line	Risk managers responsible for aggregate enterprise-wide cyber risks, who are granted independent authority to challenge the first line's approach to cyber risks effectively	▸ Develop a cyber risk framework and challenge the first line's implementation of it ▸ Develop the firm's cyber risk appetite and monitor conformance to it ▸ Report on aggregate enterprise-wide cyber risks	▸ Developing an insightful set of enterprise-wide cyber metrics ▸ Aligning the cyber risk management framework with the overall risk framework ▸ Finding talent that knows risk and cybersecurity
Third line	Internal audit team providing assurance of the firm's overall cyber risk governance	▸ Audit core elements of cyber, either as separate audits (e.g., on access controls) or with relevant topic-specific audits (e.g., vendor risk management) ▸ Evaluate overall design and operating effectiveness of cyber risk management across first and second lines	▸ Providing insights that materially improve the quality of cyber controls ▸ Determining the best approach to independently assessing the cybersecurity risk framework

The second-line risk function has to build out its capabilities. Cyber risks should be hardwired into the firm's enterprise-wide risk appetite framework, so that the board formally approves its appetite for cyber risk and monitors that the firm stays within that tolerance. The cyber risk management framework should be fully incorporated in the broader risk management approach, and aligned well with IT, security risk and operational risk frameworks.

The third line (internal audit) will need a stronger focus on cybersecurity, new personnel (or co-sourced capabilities) and a more independent view on how well the board, and first and second lines, oversee, evaluate and manage cyber risk.

A major challenge for all three lines is managing cyber risk associated with third parties. Regulators are increasingly pushing for more ongoing, detailed oversight of third parties, particularly as it relates to cybersecurity, resiliency and data protection (see "A growing regulatory challenge" on page 15).

In essence, a fully functioning 3LoD approach to cyber risk management is now required.[5] The industry is moving quickly to adopt such a firmwide strategy. In so doing, financial services firms are having to develop their cyber talent strategy, as noted earlier.

Keeping an eye on what's critical

In the end, financial services firms have to prioritize their efforts.

First, they have to identify what business processes and assets are most critical to them, and implement a differentiated approach to protect those assets. This requires firms to map business processes to applications and infrastructure, and include data flows and upstream and downstream dependencies. That way, firms know the universe of what constitutes critical.

Second, firms have to determine how they will segment or quarantine critical assets. Too many times, cyber attackers access critical processes by way of less-protected assets.

Finally, firms have to determine which third parties are critical to those processes. Critical vendors must be evaluated and monitored in a more rigorous way. Where possible, firms should have alternative vendors that can be called upon if the existing vendors suffer material cyber attacks, data breaches or technology failures. Cyber resiliency is becoming a major theme in the industry, beyond third parties.[6]

[5] *Cyber risk management across the three lines of defense,* EY, April 2017, www.ey.com/Publication/vwLUAssets/ey-cyber-risk-management/$File/ey-cyber-risk-management.pdf.

[6] *Cyber resiliency: evidencing a well-thought-out strategy,* EY, August 2017, www.ey.com/Publication/vwLUAssets/EY-cyber-resiliency-evidencing-a-well-thought-out-strategy/$FILE/EY-cyber-resiliency-evidencing-a-well-thought-out-strategy.pdf.

A growing regulatory challenge

In response to the growing cyber threats to the financial services sector, regulators all over the world are pushing to hold more companies accountable for cybersecurity, through tougher regulation and enhanced supervisory expectations.

Broadly speaking, existing cyber regulation covers two main areas: protecting consumer privacy and protecting the financial services system as a whole.

The EU's General Data Protection Regulation (GDPR) is very much focused on consumer privacy, as its title suggests. It requires companies to report on a cyber breach anywhere within their ecosystem, including contractors, third-party vendors and affiliates.

The US is ramping up cyber regulation on a number of fronts. The Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve Board (FRB) have proposed enhanced cyber risk management standards for financial institutions. The comment period for the advance notice of proposed rulemaking (ANPR) has been completed and proposed rulemaking is pending notice.

The ANPR is very much aimed at systemic risk within companies and the sector as a whole. Indeed, its overarching goal is to protect the entire financial system. It is considered the most significant and demanding set of standards relevant to cybersecurity applied to major financial services firms with operations in the US. One of its central benchmarks is for companies to develop and maintain a written, board-approved, enterprise-wide cyber risk management strategy that is integrated into strategic plans. Taken as a whole, the ANPR signals that cybersecurity sits at the heart of business strategy and the broader financial services ecosystem, including third parties.

Other regulators across the global financial system are also meeting the challenge head on, including the monetary authorities of Singapore and Hong Kong. Additional regulations that are rapidly approaching relate to network and information security, and payments systems.

The scale and scope of new cybersecurity regulations coming into force poses an obvious compliance challenge for financial services companies, not least because a very large part of the financial services market consists of organizations with global market presence, or with clients distributed in different markets. These global players are going to have to adhere to all these different regulations around the world.

Risk focused calls to action:

- Evaluate cyber risk governance to determine what refinements are required to provide robust board oversight of cyber risks
- Establish a strategy for implementing a 3LoD approach to cyber risk management, with a major focus on clearly articulating roles and responsibilities across and within the three lines, and on critical business processes, assets and vendors
- Develop a second-line cyber risk management approach, built around a well-articulated, board-approved statement on cyber risk appetite, supported by accurate, timely cyber risk metrics
- Establish a cyber regulatory compliance capability that merges all the competing and overlapping regulatory requirements; this will ensure the organization has a 360-degree view of the activities that will address one or more regulations

Priority four

Intelligent and agile – protecting what's critical

Deciding what is critical can be a challenging process for any big organization, not least because attacks are becoming increasingly sophisticated and the lines of attack shift every day. Different parts of the business can make compelling cases for why their assets are crucial and must be protected. The reality, though, is that no organization can fully protect itself from a cyber attack. Which means that the real question is: what is the risk appetite for protecting the critical assets? This will depend on both the nature of the assets themselves (which determines their inherent vulnerability) and the organization's priorities – for example, it may be better to accept certain risks in order to dedicate resource to reputation management.

Then, what are the critical assets that really matter to your business? For many companies, it is their customer data – 65% of respondents to our *GISS* cited customer personal and identifiable information as the most valuable asset to protect, while 36% cited customer passwords. For other companies, it might be financial information, corporate strategic plans, personal data related to the board or information about M&A activity.

Figure 4: Customer data is considered by far the most valuable asset to protect

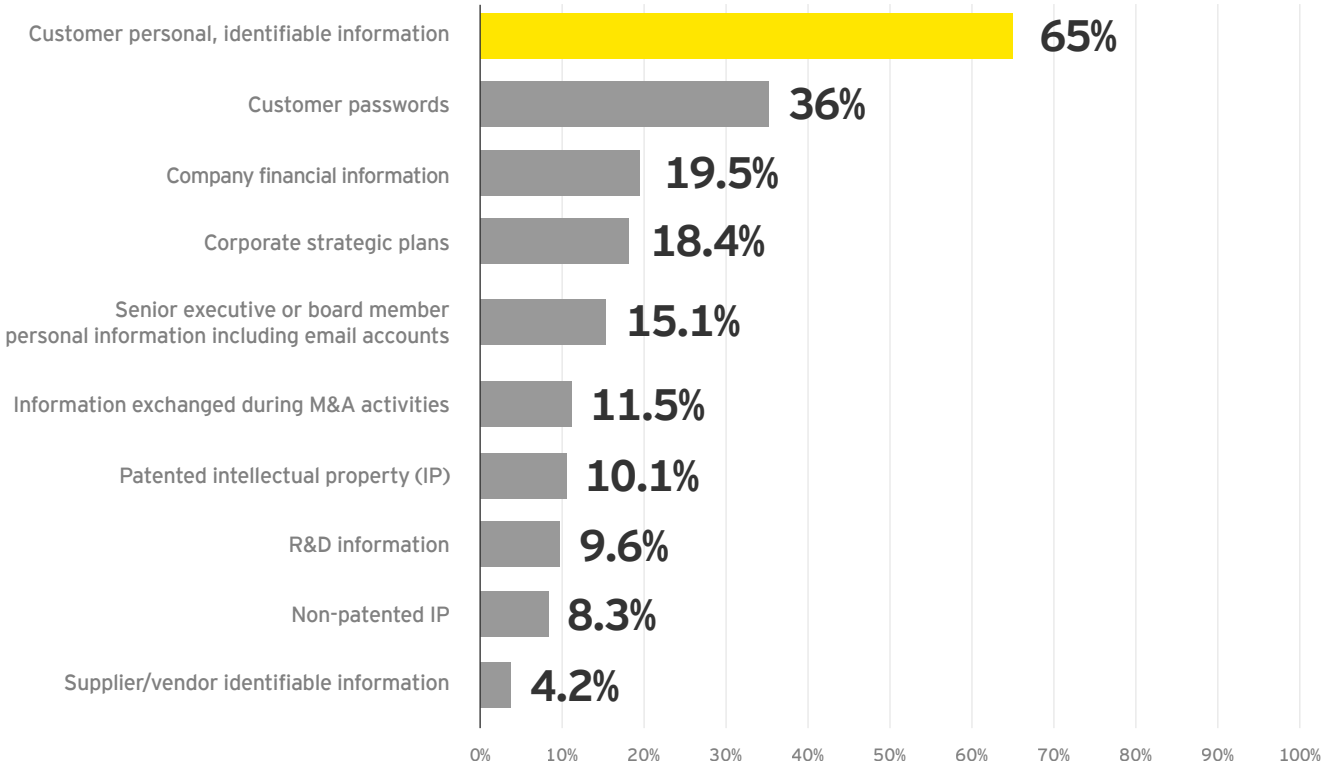
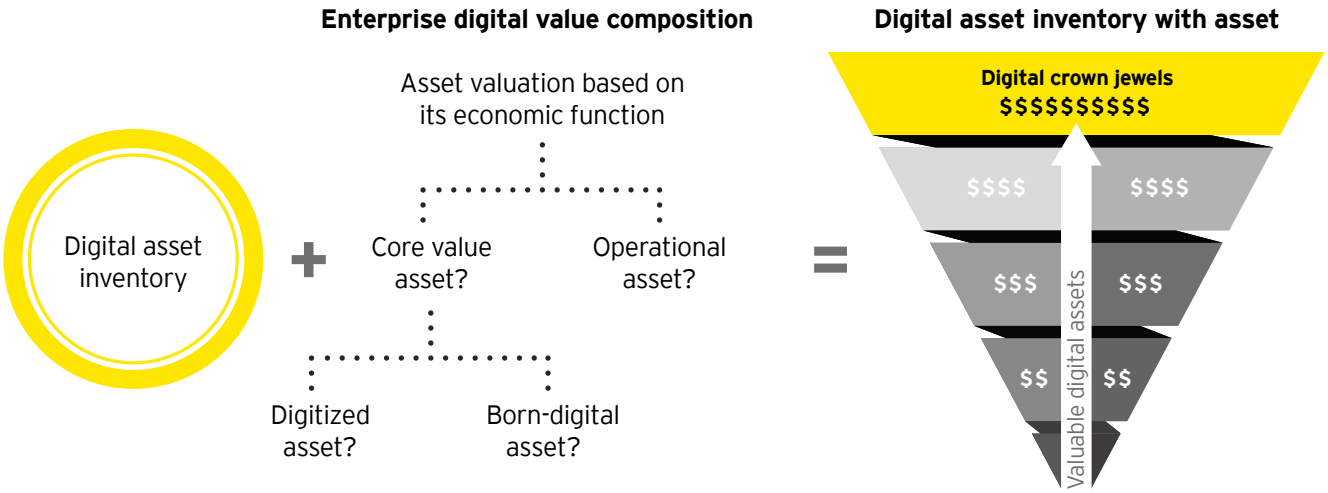


Figure 4 source: "Customer data is by far considered the most valuable asset to protect," *EY Global Information Security Survey 2016,* Sample: 300 financial services (FS) executives www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016.

Ultimately, as organizations look to protect what is critical, they must weigh up the economic cost of a cyber attack. The economic impact of cyber attacks and incidents are almost always significantly higher than the face value of the direct loss.

That's because the overall losses include indirect costs related to investigation and correction of the problem, reputational damages and loss of customers, legal liabilities, potential regulatory fines, and impact on share price. Companies can assess the value of their organization's cyber resilience through tailored economic modeling tools.

Figure 5: How to manage cyber risk from your balance sheet?



Applying a cyber-economic model can help to identify the most crucial assets that need protecting and quantify the economic loss following cybersecurity attacks. For example, what would be the quantified loss to an individual bank if it lost one million customer records, and that loss became public? By employing this model, you can plot how the value at risk will start to decline as you increase your defensive controls to prevent the attacks that are relevant to those cyber-economic loss scenarios.

Intelligent and agile calls to action:

- Take an inventory of your key assets and processes to identify which ones are considered to be critical
- Identify who would threaten them, why and what attack methods would they deploy; use this threat intelligence on an ongoing basis to refine and keep your threat assessments current
- Assess how vulnerable your critical assets are based on your threat analysis, and focus effort and investment on managing these vulnerabilities
- Undertake cyber-economic modeling, incorporating your threat and vulnerability assessments, to identify the potential monetary losses if your critical assets are successfully attacked (this will inform investment budgets and provide the board with a more quantified business case)

Figure 5 source: *Economic modeling for cyber resilience: how to manage cyber risk from your balance sheet.* EY, 2017.

Priority five

Resilient and scalable — bouncing back and protecting the ecosystem

If we accept that some form of cyber attack is inevitable, then it becomes even more important for the organization to have systems and strategies in place to reinstate business as usual in the fastest possible way, learn from what happened, and adapt and reshape the organization to improve cyber resilience going forward.

This calls for a centralized, enterprise-wide cyber breach response program (CBRP) that can bring together the wide variety of stakeholders that must collaborate to resolve a breach. The CBRP needs to be led by someone who is experienced with technology, and able to manage the day-to-day operational and tactical response. That leader should also have in-depth legal and compliance experience, as any cyber breach can trigger complex legal and regulatory issues with financial statement impact.

The 2008 financial crash highlighted the extent to which the financial services sector is interconnected. Since then, the web of connectivity has increased as companies have looked to outsource ever greater parts of their business. Today, a global bank can have up to 6,000 vendors. That poses real challenges when it comes to making sure each vendor has the right cybersecurity controls in place.

68% of executives would not increase their information security spending even if a supplier was attacked — even though a supplier is a direct route for an attacker into the organization.

Companies now need to place as much importance on shoring up their entire ecosystem of vendors and partners as they do preparing their entire workforce with the skills and tools to protect against cyber attacks.

Having confidence in the company's ecosystem will require a supplier strategy that, at first, may seem overly cautious but is, in fact, crucial given that the greatest security threat often comes from third-party connections. Large and mid-tier financial services firms have recognized this and have spent time risk prioritizing their vendors over recent years through a combination of questionnaires and remote and on-site assessments, alongside reviews.

Companies will need to continue to take a risk-adjusted approach to partners and suppliers — rating them on a number of risk criteria that are aligned with the overall cybersecurity strategy. Threat intelligence programs can help companies get a better understanding of supplier vulnerabilities, and existing vendor risk assessments need to be upgraded and bolstered to plug all the cybersecurity gaps that currently exist.

Taking a robust line with outsource partners is important because so much of an organization's activities typically rest on third parties. Is the vendor really processing your data or has it been outsourced to another company? Can you be sure that it is acting in a secure way and has a program to ensure its employees are protecting your data appropriately?

A risk assessment process may well result in a reduction in the number of vendors the company relies on. If so, companies can incentivize compliance on the part of their suppliers and make them easier to monitor in the future.

Resilient and scalable calls to action:

- Confirm that you have a documented CBRP, which includes all stakeholders (from the board and C-suite, through to legal, HR, risk, PR, communications, IT, business unit leads, etc.)
- Verify that all stakeholders have been trained on the plan and most importantly, that they have taken part in a cyber incident simulation exercise, to challenge and test their ability to respond[7]
- Re-examine the crisis communications plan and ensure it not only covers key external stakeholders, such as law enforcement, regulators, customers and media, but also includes the different scenarios when these stakeholders need to be communicated with, focusing on striking the right balance between disclosing too early and too late
- Build a centralized third-party management program around a register of all third parties, including information as to whether the third party manages your data or has access to your systems; appropriate oversight, including on-site cybersecurity audits, can then be focused on those vendors that pose the most risk

[7] *Cybersecurity incident simulation exercises: Is simply waiting for a security breach the right strategy?* EY, August 2017, www.ey.com/Publication/vwLUAssets/ey-cyber-incident-simulation-exercises/$File/ey-cyber-incident-simulation.pdf.

10 things to do right now

Putting into a place a holistic, business-driven approach to combating cyber attacks might feel overwhelming when your organization is already facing disruption on many different fronts.

Nevertheless, cybersecurity has to be a core business priority and it has to be everybody's concern in the modern financial services organization.

Here are 10 things you can do right now to make that happen:

1. Integrate cybersecurity into the talent strategy and create a CISO role that is fit for the purpose of your organization
2. Clearly define cybersecurity responsibilities in your organization
3. Put cybersecurity at the forefront of a cross-functional business strategy. It mustn't be viewed as IT's problem
4. Ensure that cybersecurity is at the heart of digital innovation and helps, rather than hinders it
5. Understand how regulation impacts your global business, and work with regulators, as they too want a strong financial services sector
6. Risk rate all your key assets and determine a protection approach for each one with a focus on the most critical ones
7. Develop a dynamic and nimble cybersecurity risk management model to enable your organization to scale if there is an escalation of external risk or a decision to change the firm's risk appetite

8. Integrate compliance into your cybersecurity strategy, so that any money invested in compliance will return value to the business by providing proper defense for the organization

9. Strengthen resilience by having a clear crisis action and communication plan for when things do go wrong, so that crisis and continuity management can be thought through and practiced at all levels of the organization

10. Collaborate with your peers to seek more intra-sector solutions; today's cyber risks threaten the entire financial system, and the failure of one key player could damage the reputation of an entire industry

Conclusion

The future for the financial services sector will be defined by the digital agenda, with an increased reliance on technology and connectivity. This will deliver many benefits for financial services companies and their customers, but it will also present many cyber risks and, by doing so, threaten the core foundation of financial services — trust.

As customers demand an expanding range of digitally accessible products and services, they expect their confidential information to be well protected. Therefore, to win and maintain customer trust, financial services companies will need to preserve their customers' data privacy, be available any time and any place, and maintain the integrity of data.

As we have detailed in this report, this involves understanding how cyber risks are evolving, keeping ahead of new regulation, embedding the right cybersecurity strategy and culture within the company, working closely with partners and vendors to secure the entire ecosystem and, crucially, identifying the most critical assets that must not be compromised.

Companies that achieve these goals and prove to be reliable and trustworthy guardians of data will not only be those that customers trust. They will also have succeeded in making cybersecurity a market differentiator that will offer stability in a disruptive age and help win more business. Those that cut corners and fail to combat cyber risks will lose both trust and customers.

How we can help

At EY Financial Services, our fully integrated and globally connected teams create a single, all-encompassing vision for managing cybersecurity risk. Seeing things from all angles means we put cybersecurity at the heart of our clients' business strategy, to support innovation and help them gain a competitive edge in today's digital world.

Contacts

To find out how we can help you address the five priorities covered in this report, please contact your regional EY FS cybersecurity leader:

Jeremy Pizzala
Partner, Global and Asia-Pacific FS Cybersecurity Lead

Ernst & Young Advisory Services Ltd

Email: jeremy.pizzala@hk.ey.com
Tel: +852 2846 9085

Cindy Doe
Principal, FS Americas Integrated Cyber Risk Lead

Ernst & Young LLP

Email: cynthia.doe@ey.com
Tel: +1 617 374 558

Steve Holt
Partner, EMEIA FS Cybersecurity Lead

Ernst & Young LLP

Email: sholt2@uk.ey.com
Tel: +44 20 7951 7874

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

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. For more information about our organization, please visit ey.com.

EY is a leader in serving the financial services industry

We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions. The better the question. The better the answer. The better the world works.

EYG no. 05716-174Gbl

EMEIA Marketing Agency

1000912

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/fs