Remember when stolen credit card numbers represented the height of sophistication in cybercrime? Those days are long gone. Now, complex, hard-to-detect attacks could bring down not just a single institution but also large parts of the internet and the financial markets.

Consequently, cybersecurity is no longer just about deflecting attackers. Today, it’s about figuring out how to manage and stay ahead of intruders that are already inside the organization.

Today’s attackers typically aren’t seeking quick results; rather, they attempt to insert themselves silently into a financial institution’s networks — probing for vulnerabilities, waiting for an opportune time to strike their targets or using their host’s trusted connections to infiltrate other unsuspecting institutions. These attacks often span several months or even years.

Organizations must respond to criminals who are constantly developing new, nefarious methods and techniques to achieve their objectives. As for cybercriminals’ myriad motives, some want to damage the reputations or brands of their targets; others seek customers’ or clients’ sensitive information, which can be used to compromise and steal various types of assets; and other motives are hard to discern.

Recent concerns about systemic cyber threats have elevated cyber risk to a higher place on the political and regulatory agenda. Following recent cyber attacks, the industry began to seriously consider the real risk that cyber attackers could disrupt...
larger financial systems rather than just harming individual firms. Such an attack could significantly disrupt financial transactions, halt entire markets, and undermine stability and trust in the financial services sector.

This has led to a call for a better approach for addressing cyber risks, an approach that goes beyond being the sole concern of the information security group. To that end, the financial services industry has embarked on a journey to implement a “three lines of defense” (3LoD) model for cyber risk, encompassing the following:

First line: Business units and information security teams with direct accountability for owning, understanding and managing cyber risks

Second line: Risk managers responsible for aggregate enterprise-wide cyber risks, who are granted independent authority to effectively challenge the first line’s approach to cyber risks

Third line: Internal audit team providing assurance of overall cyber risk governance for the enterprise

These three lines of defense are guided by an active, engaged and qualified board of directors that approves and oversees the firm’s approach to cybersecurity, while achieving alignment by providing a credible and effective counterbalance to management (see Figure 1).

Figure 1: Evolution of cyber risk management

These three lines of defense are guided by an active, engaged and qualified board of directors that approves and oversees the firm’s approach to cybersecurity.

* Advanced persistent threats
Blueprint for enterprise-wide cyber risk governance

Establishing a 3LoD approach to cyber risks is not a trivial task. Financial services firms are still grappling with how to best implement the model across their businesses for existing non-financial risks. Adding cyber risk management to the 3LoD model will pose an even greater challenge for organizations.

The overall concept is well-known; it's the practical implementation that's the issue. Some common questions include the following:

- Frontline accountability for all risks makes sense, but what needs to be done for first-line business and technology leaders to effectively meet their risk obligations?
- Second-line oversight of aggregate risks is clearly important, but how does the second line undertake this role without leaving the impression that the first line may abrogate its duty, knowing the second line is there?
- Third-line assurance acts as an important backstop, but how does internal audit engage sufficiently to drive improvements in cyber risk governance without undermining its independence?

A critical success factor will be understanding each line’s role and having strong board oversight during the implementation of the 3LoD model for cyber risks.
First line: enhance cybersecurity capabilities, bring in the business

Front-line business units, working with the information security and cybersecurity teams, have to measure, monitor, manage and mitigate cyber risks within the board-approved cyber risk tolerance.

A strong first line of cybersecurity requires a significant effort within the lines of business. Whether in the retail bank, investment bank, corporate bank, private bank or any other area, business heads will have to perform a thorough examination to determine whether the business is doing enough to manage cyber risk. Information security groups can no longer apply one-size-fits-all solutions to the entire enterprise. Instead, each line of business must carefully define the cyber risks and exposures it faces. Cyber risks need be woven into the fabric of the first line’s risk and control self-assessment and into fraud, crisis management and resiliency processes.

This will require businesses to achieve a better understanding about the interrelationship between their activities and cyber risks. The lines of business will need to actively monitor existing and future exposures, vulnerabilities, threats and risks associated with their activities. After all, the business best knows its own data flows and business processes. Working with technologies, businesses need to determine the impact cyber risk will have on its clients, operational processes and strategies.

These new responsibilities will require significant investment in people and tools, including upgraded monitoring and analytic capabilities to provide improved assessments of current levels of cyber risk. Information security already has many capabilities in these areas, but they will need to be reinforced and shared across all three lines.

These new responsibilities will require significant investment in people and tools, including upgraded monitoring and analytic capabilities to provide improved assessments of current levels of cyber risk.

Getting to the right level of security

Underpinning an effective and robust firmwide cyber risk management approach is a set of core fundamental capabilities. EY’s 2016-17 Global Information Security Survey (GISS) highlighted that few financial service firms feel they have achieved the highest level of maturity on these fundamentals.

For example:

- Only 7% of banks and 6% of insurers believe they have advanced vulnerability intelligence, including the ability to conduct, throughout the year, risk-based assessments that result in agreed-upon remediation plans between the business and the risk function.
- Only 3% of banks and 2% of insurers have formal processes for threat collection, dissemination, integration, response, escalation and prediction of attacks.
- Only 9% of banks and 3% of insurers have a robust incident response program that includes third parties and law enforcement, integrates with a broader threat and vulnerability management function, and responds to potential incidents with regularly tested playbooks.
Second line: involve cyber risk managers in operations

Cyber risk shouldn’t be walled off as a separate risk function. Instead, it should be embedded into the broader second-line risk management framework. Enterprise risk managers need to compare cyber risks to other risks using the same financial and probability benchmarks, so that investment on cyber risk prevention and remediation can be considered simultaneously with other pressing enterprise risks.

Second-line risk management plays a critical role in managing cyber risks. As the keeper of a firm’s board-approved risk tolerance, it determines how to appropriately measure cyber risks, embedding quantitative and qualitative (e.g., reputational) thresholds for cyber risks into the statement of risk tolerance for the firm. Moreover, these clearly established appetite and associated thresholds need to cascade down into the operations for each line of business.

Other core activities of risk managers need to be extended to treat cyber risk in much the same way as market risk or operational risk. To do so, cyber risks need to be embedded firmly into the organization’s firmwide risk taxonomy and risk-and-control processes, including a distinct cyber risk management framework that covers internal and external risks and dependencies. Based on that framework, second-line risk managers should develop a comprehensive picture of cyber exposures, vulnerabilities, and risks and then generate solid metrics to inform decision-making and to establish the risk/return trade-offs involved with investments in cybersecurity. Furthermore, risk managers need to monitor the lines of business for sufficient adherence to the firm’s cyber risk appetite.

Inevitably, cyber risk loss data will become a more important factor in investment decisions, as well as capital and liquidity stress tests. Traditionally, loss data simply reflects the cost of remediating breaches, not the business costs of lost business or the erosion of customer trust and brand equity. By including those factors in a broader view on what constitutes loss with respect to cyber risk, managers will be able to improve their overall decision-making.

The Chief Risk Officer (CRO) has an important role in leading an enhanced second-line cyber risk management team, with actions including the following:

- **Management and oversight:** Create a dialogue with the board and risk and audit committees
- **Organizational structure:** Establish reporting relationships with Chief Information Officers, Chief Information Security Officers (CISOs), Chief Privacy Officers and Chief Compliance Officers
- **Risk framework:** Fit cyber risk into enterprise-wide risk frameworks, including risk governance, risk reporting and metrics, and escalation mechanisms
- **Impact assessment:** Quantify the potential impacts to liquidity, capital or earnings from a cybersecurity event
- **Preparedness:** Challenge the effectiveness of disaster recovery and business continuity efforts with respect to cyber threats, as well as the degree in which recovery and resolution planning properly incorporate cyber risks
- **Insurance:** Assess the residual cyber risk and decide which risks need to be addressed through insurance (externally or self-insured).

CROs should report independently to the CEO and board of directors, as appropriate, when their assessments of cyber risks differ from that of the first-line business units, or when a unit has exceeded the entity’s established cyber risk tolerances. Such reporting is in addition to reporting from the first-line information security professionals.

Given the relative novelty of applying the 3LoD model to cyber risk, most of the first- and second-line focus is appropriately on more effective management of these risks rather than the narrower issue of compliance. However, given the increasing volume of regulatory guidance and mandatory requirements stemming from industry, professional and regulatory standards, cyber will increasingly constitute a material compliance risk. Accordingly, financial institutions should integrate cyber risk compliance into second-line risk management.
Third line: expand internal audits mandate to cover business disrupters – cybersecurity

Traditionally, the main role of the third line of defense is to independently assess the firm’s risk and control environment and enhance the effectiveness of the firm’s risk governance approach. The question regulators are now asking is: How effective and how independent is a firm’s internal audit team when it comes to reviewing a firm’s approach to cybersecurity?

As a foundation, the internal audit team will need to include within its overall audit plan an evaluation of the design and operating effectiveness of cyber risk management across the first and second lines of defense. Traditionally, industry standards (such as National Institute of Standards and Technology’s Cybersecurity Framework) have been used as the benchmark for evaluating a firm’s effectiveness. Going forward, internal audit teams may need to create their own framework or apply multiple industry frameworks. By doing so, auditors will maintain greater independence in assessing cyber risk management effectiveness, eliminating the potential blind spots that can result from using a common standard throughout all three lines of defense.

Under the 3LoD model, internal auditors will do the following:

- **Perform assessments:** Report on how well the first and second lines of defense adhere to the firm’s cyber risk management framework, compare actual cyber risk exposures with approved risk appetite and tolerances, and assess the firm’s capabilities to adapt to evolving threats and vulnerabilities.
- **Validate applications and connections:** Independently validate the firm’s application inventory throughout its catalog of internal applications, technology infrastructure, business processes and vendors; monitor connections and dependencies both internally within the firm and externally to other financial institutions and information-sharing organizations.
- **Evaluate third-party risks:** With a heightened focus on critical vendors and “nodes” within the financial system that have the potential to create system-wide contagion, internal audit may need to enhance its evaluation of critical vendors, such as through stronger ongoing monitoring techniques or more on-site reviews. For their part, third parties may have to step up the degree to which they issue attestation reports (e.g., Service Organization Control 2 reports) to provide sufficient information to their clients on their cyber risk management approach.
- **Conduct independent penetration tests and vulnerability assessments:** At a minimum, the internal audit team may need to enhance the manner in which it independently validates the scope, quality and remedial activities associated with the first line’s penetration testing and vulnerability assessments. But, in time, that may not go far enough. The internal audit team may have to conduct its own testing and assessments. The assessments – its own or those conducted by the first line – have to be able to adapt to a changing threat environment. This may require periodic rotation of third parties used for such assessments.
- **Enhance regular audit procedures with cyber risk considerations:** Factors relevant to addressing cyber risk should be incorporated into standard audits throughout the year. For example, as part of routine audits, internal auditors should also review business continuity and disaster recovery plans; capital and liquidity stress testing scenarios (including various scenarios related to cyber breaches); recovery and resolution plans (especially for critical vendors and internal shared services); information technology and security risk management; and impact assessments related to the adoption of new disruptive technologies or digital platforms.
- **Stay abreast of threat intelligence:** To align audit activities with enterprise priorities based on active risks and threats, internal auditors should collaborate with the first line to receive appropriate threat intelligence and analytics.
Banks are already moving toward a 3LoD model

Although regulatory emphasis on the 3LoD cyber risk model is relatively recent, there are clear signs that the banking industry is moving on its own to consider risks across the three lines. In A Set of Blueprints for Success, the seventh annual global bank risk management survey by EY and the Institute of International Finance, cybersecurity was ranked second in the list of top five concerns for chief risk officers, with over half (51%) of CROs making it a priority, up from 22% in 2015 and 10% in 2014. Numerous other functions or governance groups have increased their focus on cybersecurity in the past year, including the board of directors (80%), business-line management (71%), internal audit (66%) and compliance (42%).

In building out the 3LoD cyber risk model, banks have been designating more roles to address cybersecurity in second-line risk and compliance groups. They have increased dedicated headcount (75%), appointed designated specific cybersecurity roles (55%) and created a CISO-type position (32%). These professionals complement, rather than supplant, existing roles in the first line.

In addition, as shown in Figure 2, across the three lines, banks have been enhancing the degree to which they embed cyber risks into their risk operating models, including the risk management framework, the audit plan and in compliance.

Figure 2: Strengthening cyber risk management

- Incorporated cybersecurity into enterprise risk management framework: 67%
- Developed additional metrics to support second-line monitoring of cybersecurity: 60%
- Developed a cybersecurity approach that spans three lines of defense: 55%
- Incorporated cyber risks into risk-appetite framework: 48%
- Increased number of internal audit hours dedicated to cybersecurity: 48%
- Developed “what-if” analyses to assess an event and actions taken: 47%
- Incorporated cybersecurity into compliance management framework: 20%

Increased board oversight
Cyber risk governance

The board of directors is ultimately responsible for verifying that management implements an effective 3LoD approach for cyber risks. The board and its committees — notably, audit, risk, and for some technology — need to validate the delineation of risk management and cybersecurity oversight responsibilities across risk management, internal control and internal audit. The board should provide strong oversight and effective challenge to management.

The board maintains oversight of the enterprise-wide cyber risk management strategy, including an appropriately set appetite for cyber risk. It also has to validate that cyber risk management strategies and risk appetites have been integrated into strategic plans and risk management structures in other areas of the enterprise.

Embedding cybersecurity across the organization

To the extent that firms more accurately measure and manage cyber risks, they will need to integrate more sophisticated cybersecurity analysis into a range of activities, including the following:

- **Strategy and mergers and acquisitions**: Cyber risks should be considered in the overall strategic plans and strategic risk management processes, and more effectively in the due diligence and analysis regarding corporate development and mergers, acquisitions and dispositions, and within alliance-partner relationships.

- **Innovation**: While new innovations drive business growth and profitability, they can produce new cyber risks. Cyber risk will need to be considered more effectively in the new product approval process, in financial technology initiatives and acquisitions, and in the adoption of new technologies and digital platforms.

- **Talent management**: Inevitably, as firms build out the 3LoD cyber risk model, it will test their talent acquisition and retention strategy. Firms will need to validate that they have the right skills and competencies across the three lines. According to EY’s 2016–17 Global Information Security Survey (GISS), 51% of banks and 59% of insurers cite skills shortages as being a major constraint on their cybersecurity programs. The competition for talent will intensify as more financial institutions implement new, demanding regulatory requirements.

- **Employee training**: Effective training is essential. After all, the best line of defense is a firm’s employees. Yet EY’s 2016–17 GISS highlights that 67% of banks and 82% of insurers state that the most significant source of an attack is from careless employees. Accordingly, training should be tailored to the role and applied broadly. All personnel — including third-party contractors and temporary staff — should attend regular cybersecurity awareness training sessions that are consistently updated to reflect risks identified in the firm’s annual risk assessment. Beyond that, all cybersecurity personnel should attend regular cybersecurity update and training sessions, with key personnel taking additional steps to stay abreast of changing cybersecurity threats and countermeasures. Metrics should be developed and used to track employee understanding.

The cyber risk management strategy needs to address the following items:

- Managing inherent/aggregate residual cyber risk (i.e., before and after mitigating controls)
- Maintaining resilience on an ongoing basis
- Identifying and assessing activities, exposures and resources that involve cyber risk
- Establishing policies for identifying cybersecurity incidents, addressing shortfalls, and responding to cybersecurity incidents and threats
- Testing and measuring cybersecurity protection, detection and response

Increasingly, regulators will expect boards to validate that cyber risk management strategies consider the firm’s overall position, importance and interconnectedness within the broader financial market. An internal perspective will no longer be enough.
We're all in this together

Regulators are pushing the 3LoD model to compel banks to improve their risk management in response to failures before and after the financial crisis. Firms have successfully implemented the model in the area of financial risks, such as credit and liquidity. Where the industry is most challenged is in the area of non-financial risks, including cyber risk.

Regulators have clearly concluded that a 3LoD cybersecurity model is critical. Cyber risk can no longer be considered an information risk for the information security professionals to manage by themselves. They still have a critical role to play in managing cyber risk, working directly alongside first-line business management. At the same time, the second and third lines have independent roles to perform, overseen by an engaged and effective board of directors.

Getting this right will take time. But with system-wide cyber risks in mind, the industry needs to move quickly to get the fundamentals in place so that, together, individual firms and the industry as a whole become better protected, more resilient, and capable of responding quickly and effectively to the inevitable and increasingly potent attacks the industry will experience over the coming years.

Boards should confirm that management has clear metrics for success. These includes absolute metrics such as year-over-year comparisons; goal-based metrics that assess how well the organization performed against stated objectives (e.g., if the goal is “no unscheduled downtime greater than one hour,” how often did that happen?); capability-based metrics that describe new capabilities that a firm would not have been able to do in a prior period; and peer analysis using industry-level data and surveys.

As boards evolve their cybersecurity oversight roles and responsibilities, it’s important that they evaluate whether they have adequate cybersecurity experience among their members. At a minimum, they need access to staff with such experience, or they may rely on support from third parties. Additionally, one or more board members may need enough technical knowledge to enable the board to properly hold management to account for developing and implementing a cyber risk strategy and managing the firm within board-approved cyber risk levels.

Endnotes


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 global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY’s Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY’s financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2017 EYGM Limited.
All Rights Reserved.

EYG no. 01005-171Gbl
1701-2185273 BDFS
ED None

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

ey.com