Building a better working world

Cyber resiliency: evidencing a well-thought-out strategy

Understanding cyber resiliency risks and managing them effectively across the firm is a challenge, even for the most mature firms.

Today, firms are facing much tougher questions than ever before from external parties as to their cyber resiliency strategy. Increasingly, regulators and major clients are demanding evidence that firms' cyber resiliency strategies are effective.

Questions have moved beyond those concerning one's business continuity plan (BCP) and disaster recovery (DR) approach. Today's questions include: How do firms reduce the likelihood of a disruption to their services? What will firms do if their systems are down for five days? How will firms continue to operate and process transactions – manually, if necessary – when systems are down for an extended period? How will firms recover effectively in a timely and well-controlled manner?

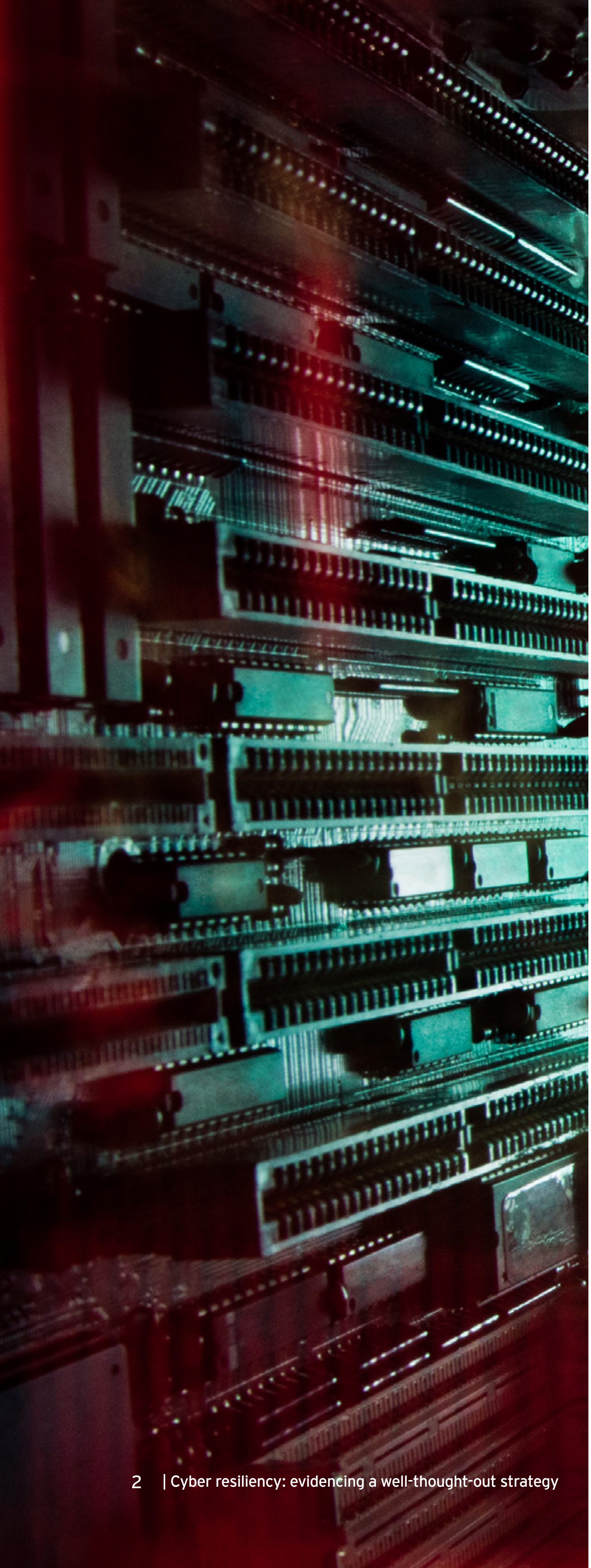
Yet, the term "cyber resilience" has confused many. Some view it merely as the term de jour. For those thinking this way, it's simply the new term for BCP or DR. Those firms are pulling out and tactically updating their plans to evidence to regulators and clients that they are well-placed to respond and recover from a cyber event.

Others, rightly, recognize cyber resiliency is much broader and relates to the seamless initiation of approaches to maintain the ongoing delivery of operations during a disruption. This includes how firms:

- Govern and challenge cyber resiliency
- Risk-assess cyber resiliency
- Identify, architect and protect systems, especially those most critical for the firm and the broader financial services ecosystem
- Manage critical third parties and other key dependencies
- Detect, respond, recover and communicate
- Test systems and recovery plans

Understanding cyber resiliency risks and managing them effectively across the firm is a challenge, even for the most mature firms.

For more, visit ey.com/fscyber



Govern and challenge cyber resiliency

A significant burden for addressing cyber resiliency falls to those at the front line — the first line. This includes business-process owners, technologists, vendor owners and cybersecurity teams. After all, those who own the risks should manage those risks.

However, regulators and clients increasingly expect independent challenge of the first line by the second and third lines, and that includes intelligently and independently challenging the cyber strategies being adopted by the first line.[1] This is not about checkers checking the checkers. It's about building a robust three lines of defense for cyber resiliency.

Regulators and clients are focused on:

- **Overall accountability:** ultimately, resiliency is a team sport. What are firms doing to ensure it is not just the operational or cybersecurity professionals who own resiliency, but also other internal stakeholders, including the business-line management, vendor management, second and third lines, legal and the board, among others? How are firms implementing a cyber resiliency strategy that is effectively concerted, coordinated and multidisciplinary, including with third parties?
- **Second-line risk management:** second-line oversight of the firm's first line is a core part of a risk management program. What role does the second line play in developing the cyber resiliency risk framework? Typically, framework development is a second-line function, with the first line developing policies on how to execute the framework in their specific context. How well does the second line validate the first line's approach to implementing the framework? Primary testing should be done by the first line, but some second-line testing is often warranted to validate that the first line's controls and testing approach is effective. How well does the second line build cyber resiliency into the firm's risk-appetite framework? In this context, the second line needs to have an effective set of metrics to evaluate cyber resiliency risk. Many of those metrics may come from the first line, but the second line needs its own metrics, especially to evaluate enterprise cyber risk at the aggregate level.

[1] Cyber risk management across the lines of defense, EYGM Limited, 2017.

- **Internal audit:** the third line (internal audit) has a key assurance role to play. What approach does the third line take to validate the effectiveness of the cyber framework(s) adopted by the first and second lines for evaluating and managing cyber resiliency risk? What independent testing does internal audit need to conduct of elements of the firm's cyber-risk strategy and its recovery capabilities? In some instances, this can include independently commissioning external parties to conduct attack-and-penetration testing on behalf of internal audit. What areas have been identified by internal audit as unsatisfactory or in need of improvement, and how robust are management's plans to address those deficiencies?
- **Board oversight:** external parties want to see that the board of directors — and its committees (especially risk and audit) — have the necessary understanding of the firm's cyber risk profile and are actively overseeing and challenging management's cyber resiliency strategy. How effectively does the board oversee cyber resiliency risk?

Risk-assess cyber resiliency

First, firms need to assess their cyber risk profile and identify major risks, threats and vulnerabilities. This requires:

- **An effective risk assessment process:** risk identification is a first- and second-line role. How well does the first line consider cyber and resiliency risks, from their perspective? This means taking an end-to-end view so that the entirety of the process and supporting systems, vendors and dependencies can be identified. How well does the second line independently assess these risks to effectively challenge and complement the first-line view? The first and second lines' risk view needs updating routinely, given the fast-evolving nature of cyber risks.
- **Effective controls:** building controls in light of the risk assessments is critical. How well does the first line implement and maintain effective end-to-end controls? Those controls have to reduce residual risks to levels within the firm's overall risk appetite for resiliency. This includes understanding how dependency on third parties impacts the control environment.
- **An enterprise-wide, prioritized view on critical processes and flows:** given finite resources — management time, budget and people — firms inevitably have to prioritize certain resiliency activities. How well do firms prioritize critical processes and systems? Inevitably, firms need to prioritize which processes and systems require a differentiated strategy. There will likely be differing views within each firm about what constitutes critical. What first-line businesses view as critical may be different from risk management's enterprise-level view. Likewise, what regulators emphasize may differ from the client's perspective. For example, regulators recognize the important of protecting retail systems and personally identifiable information (PII). If those systems go down or if firms lose PII, firms can suffer financial and reputational damage. Clients and customers would emphasize these risks as the ones they want to see firms managing well. However, ultimately, in the hierarchical view of criticality, systems that undermine financial stability — settlement and clearing, trading, processing — will be viewed as most critical by regulators, and they will expect a differential approach to protecting and managing those systems, from a resiliency context. Firms have to manage these competing stakeholder demands for resiliency.

The cyber resiliency risk assessment — coupled with the prioritization view of criticality — is a fundamental building block for any cyber resiliency program.

Identify, architect and protect systems, especially the most critical

Firms also need to identify their most critical systems and assets (including high-value assets). Those that are "sector-critical systems" (to use a term from draft enhanced cybersecurity risk management standards issued by US banking regulators[2]) are generally easier to identify. Those are the key intraday settlement and clearing systems that help the financial system operate smoothly. Beyond those systems and assets, however, differing views will exist as to what is critical. Clients will view other systems as critical, from their perspective.

Once critical systems have been identified, firms have to:

- **Identify systems' ecosystem:** systems are supported in an array of ways. How do firms identify assets – data, software and hardware – processes, staff and subject matter experts that support those systems? How well do firms map processes and data related to critical systems?
- **Evaluate – and where necessary improve – system architecture and design:** critical systems have to be sufficiently flexible, agile and resilient. How do firms design security into system architecture and not just focus on it as an afterthought? For example, increasingly regulators will no longer accept excuses about delayed patching that relates to bad system architecture. The root cause is not the patching, it's the systems. To fix them, firms should:
  - **Find ways to isolate or enclave those systems:** too often, when major breaches have occurred, attackers came in through less-protected systems, and from there they maneuvered to critical systems. So how do firms reduce connectivity between critical systems and those less-protected systems?
  - **Greatly limit access:** firms continue to mismanage access rights. How well do firms limit access to critical systems? Employees who can access critical systems should be evaluated more thoroughly than others – from onboarding to ongoing assessments (e.g., of their financial position). When those individuals get promoted, they should be rechecked. If they move laterally or downward, their access may need to be removed.
  - **Limit attack surface:** reducing the opportunities for attackers is part of cyber by design. How effectively are firms hardening their critical systems by, for example, limiting the threat or attack vectors – i.e., points of attack/entry?
- **Evaluate if systems and tools used to monitor infrastructure present major vulnerabilities:** firms have, appropriately, implemented a growing set of tools to evaluate their networks and systems to detect threats and have implemented encryption tools to protect sensitive information and PII. However, it is important that firms validate that those tools do not, in themselves, create additional security threats, and if they do that those risks are mitigated. After all, if these tools are breached, often attackers get access to a broad swath of important systems. How well do firms evaluate and manage these risks?
- **Evaluate system obsolescence:** how do firms approach system obsolescence? Every firm has adopted its own strategy for managing system obsolescence, such as the pace at which it moves to new versions of software or hardware, the approach to patching, and the degree to which the firm will depend (or not) on systems that are no longer vendor-supported. While the overall strategy may make sense for the firm, it is important that firms show they have carefully considered if a differentiated strategy is needed for critical systems. As recent global ransomware attacks have shown, system outages can be traced to dependencies on old versions and bad patching practices. This is unacceptable for critical systems.

[2] Enhanced cyber risk management standards for financial institutions, or Advanced Notice of Proposed Rulemaking (ANPR), EYGM Limited, January 2017.

Manage critical third parties and other key dependencies

Firms need to evaluate dependencies on third parties, especially those that support or connect with critical processes and systems. This may include re-evaluating how they identify critical vendors and dependencies. An enterprise view of criticality is important, not just one driven by lines of business or subject matter experts. It needs to be tied directly to the view of which vendors and dependencies support or are directly associated with critical processes and systems, and be informed by – while being broader than – the firm's analysis of which vendors are critical in the context of recovery and resolution plans.

Critical vendors should be evaluated and monitored more than others. Firms have to:

- **Evaluate – or re-evaluate – those vendors' resiliency and cybersecurity practices:** this may have been done prior to onboarding vendors, but likely it may have been too cursory and need revisiting, or it might be out of date. Firms will need to determine how quickly vendors can get their systems back up after disruption. How will vendors support the firm during an outage, especially one that's prolonged? How will the vendors prioritize the firm's needs over other clients during the disruption? How have vendors evaluated their own critical third parties from a continuity and recovery perspective?
- **Contractual obligations:** firms need to build in contractual terms that clarify not only the level of performance but the key risk and performance indicators that the vendor has to provide on a pre-defined frequency. How do firms ensure proper contractual obligations are in place for new vendors? How do they change contracts with existing vendors, especially critical ones?
- **Ongoing monitoring:** Firms will need to re-evaluate their approach to monitoring critical vendors on an ongoing basis. To the extent real-time monitoring is not possible, near-real-time monitoring (that is, within the day) is required. How well do firms conduct ongoing monitoring? Increasingly, major vendors provide tools to their clients that enhance their clients' ability to monitor the vendor's performance on a more real-time basis. How effective are firms at identifying that such tools are available and where they are in incorporating them into their vendor risk management approach?

It's not just critical vendors. Firms can be impacted by disruptions in critical players in the financial ecosystem – ones that directly may not be critical to the specific firm – because disruptions can have an indirect ripple effect. After all, post-crisis there often is a consolidation in clearing and processing activities – e.g., through the creation or expansion of central counterpart clearing – that heightens the risk of system-wide contagion when disruptions occur.

With regard to critical players or dependencies, firms have to enhance their abilities to:

- **Sense:** how well can they pick up signals ahead of a potential problem? Perhaps trading volume of a key counterparty falls unexpectedly in an unusual fashion. System latency is higher than normal.
- Preempt: how well can firms react if they sense problems are coming? How preemptive can a firm be in making changes in its exposure to those firms ahead of a disruption being confirmed?
- **Manage through:** if the external party stays down for a day, how will firms react? For three days? What are the plans for managing as an external party comes back online after a disruption?

Detect, respond, recover and communicate

Even with all the best planning in the world, firms still need to conduct their ongoing detect, respond and recover activities, and they need to communicate effectively during potential and actual disruptions. Cyber attacks will occur, and firms need to spot them early, detect and repel, and when those attacks are successful, firms need to know how to react.

In the context of resiliency, key areas of focus from regulators and clients include:

- **Detect:** detecting problems is essential. It is the lifeblood of resiliency. How well do firms collect intelligence across the firm and from external sources? This extends to data from day-to-day operations and vendors' operations, as well as data that is more traditionally labeled as cyber intelligence. How effectively is that intelligence analyzed? How quickly do firms share intelligence across the firm and adapt their security posture to respond quickly to emerging threats? How effectively do firms activate processes focused on reducing the impact of disruptions when they start to detect problems?
- **Respond:** being able to respond and operate is a core part of being resilient. How effective are firms' incident response programs? How effectively do firms manage the transition from incident response and crisis management, and how do they determine when and how to invoke crisis management? How do firms manage through when systems are down, and what alternatives have been considered to manage through during the disruption? How do firms test alternative processes? Such alternatives can include:
  - Alternative internal systems or processes – this can include alternative sites that can be used to process work
  - Manual workaround
  - Transferring processing to an alternative entity
  - "Buddy banks" – peer banks that may be able to process on the firm's behalf, when needed in the extreme
- **Recover:** recovering after a disruption remains important. How well are firms enhancing their data center strategies to support local and remote high availability and data center recovery for the critical systems and data? How do firms segment their data to prioritize critical systems and processes? How do firms validate data used during disruption – especially in manual processing – and confirm that backed-up data is complete and accurate?

  Firms have to recognize cyber incidents present distinct recovery challenges when systems are down. For non-cyber technology or operational disruptions, firms have to be able to assess that backed-up data that is brought back online – and any data created or used during the disruption (for example, in manual processing) – is valid. It's not easy, but the task at hand is relatively straightforward – it's a reconciliation. In the cyber context, however, it is more challenging to validate the quality and integrity of data. Attackers may have corrupted or changed data, or installed damaging code or data. Instances of ransomware or malware, or nuisance hacking, are prime examples. Determining the golden source of data against which a careful review of data can be conducted is difficult.
- **Communicate:** speedy and effective escalation is important in times of disruption. How well do firms escalate communications when problems occur, including to the first and second lines, to senior management, and when necessary to the board of directors? How do firms determine when to communicate to regulators or clients, especially in the context of more demanding regulatory notification processes (e.g., in the cybersecurity regulation issued by the New York State Department of Financial Services)?[3]

[3] Cybersecurity requirements for financial services companies: Overview of the finalized Cybersecurity Requirements from the New York State Department of Financial Services (DFS), EYGM Limited, February 2017.

Test systems and recovery plans

Firms need to test their cyber resiliency strategies. The first line has to test the effectiveness of its own controls, in the context of its risk assessment, and the second and third lines (internal audit) should review some of these processes to validate their robustness.

Testing includes:

- **Tabletop exercises:** how well do firms use scenarios to test their plans? Routine role-playing scenarios across the firm are an important way to test plans, educate participants and identify areas for improvement. The selection of scenarios is a key success factor. The chosen scenarios need to be realistic, include people from across the lines of defense, and include specific cyber scenarios (e.g., when data may or may not have been corrupted by attackers). One scenario that is often forgotten is one in which the cause/problem is unknown. This scenario is important because firms need to be agile enough to react to situations in the moment, to be able adapt quickly to what needs to be done based on developing information, determine who from within the firm needs to be involved given that data, and so on.

- **Penetration and vulnerability testing:** how well do firms test vulnerabilities, based on emerging threats? The first, second, and increasingly third lines should conduct routine tests to assess the degree to which systems can be penetrated. This typically requires external third parties.

- **Industry-level war-gaming:** how well do firms anticipate how other firms will react to disruptions? In addition to tabletops within the firm, firms should participate in industry-level scenario exercises, when possible. These exercises help firms better appreciate industry-type scenarios — e.g., a major player in the market is disrupted for an extended period — and also bring to light areas where a firm's expectations of how the market or peers will react, under a given scenario, are incorrect, so adjustments to its own responses may be required.

- **Corrective action:** how well do firms use outcomes from these tests to improve? In the end, testing is only helpful if identified deficiencies are addressed. Inevitably, areas of enhancement are identified, even in the most successful tabletops or war-gaming. A continuous learning philosophy needs to drive cyber resiliency.

Resiliency extends beyond cyber attacks

Getting cyber resiliency requires an integrated approach. Across technology and the front-line businesses. Across cybersecurity and information security. Across the three lines of defense. Across the entire organization, up to the board of directors.

However, being resilient is a much broader challenge than just cyber. It extends from business-as-usual operational and technological resilience to resiliency in the recovery-and-resolution context. From information security to physical security. From incident plans for cyber to plans for other severe situations. From cyber resiliency risk to fraud, operational, IT and other such risks. From testing cyber controls to testing a broader set of controls. From cyber threat data to surveillance data related to fraud, compliance, conduct and more.

In practice, resiliency is a broad-based concern that firms can only address effectively and efficiently by integrating a set of disparate activities across the enterprise. That's true for operational resiliency, as much as it is for cyber resiliency.

For more cyber insights, visit
ey.com/fscyber

EY contacts

Tom Campanile
+1 212 773 8461
thomas.campanile@ey.com

Cindy Doe
+1 617 375 4558
cynthia.doe@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

Steve Holt
+44 20 7951 7874
sholt2@uk.ey.com

Jaime Kahan
+1 212 773 7755
jaime.kahan@ey.com

Chris Kipphut
+1 704 338 0491
chris.kipphut1@ey.com

Samir Nangea
+1 212 773 6742
samir.nangea@ey.com

Jeremy Pizzala
+1 852 2 846 9085
jeremy.pizzala@hk.ey.com

Dan Stavola
+1 212 773 5767
dan.stavola@ey.com

Roy Thetford
+1 212 773 3951
roy.thetford@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com

For more cyber insights, visit ey.com/fscyber

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 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.

EYG no. 04557-171Gbl
1708-2374696 BDFSO
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