OLIVER WYMAN

POINT OF VIEW

DEPLOYING A CYBER RISK STRATEGY

FIVE KEY MOVES BEYOND REGULATORY COMPLIANCE

AUTHORS

Paul Mee, Partner

James Morgan, Partner

Financial institutions are acutely aware that Cyber Risk is one of the most significant perils they face and one of the most challenging to manage. The perceived intensity of the threats, and Board level concern about the effectiveness of defensive measures, ramp up continually as bad actors increase the sophistication, number, and frequency of their attacks.

Cyber Risk management is high on or at the top of the agenda for financial institutions across the sector globally. Highly visible attacks of increasing insidiousness and sophistication are headline news on an almost daily basis. The line between criminal and political bad actors is increasingly blurred with each faction learning from the other. In addition, with cyber attack tools and techniques becoming more available via the dark web and other sources, the population of attackers continues to increase, with recent estimates putting the number of cyber attackers globally in the hundreds of thousands.[1]

Cyber offenses against banks, clearers, insurers, and other major financial services sector participants will not abate any time soon. Looking at the velocity and frequency of attacks, the motivation for cyber attack upon financial services institutions can be several hundred times higher than for non-financial services organizations.

Observing these developments, regulators are prescribing increasingly stringent requirements for Cyber Risk management. New and emerging regulation will force changes on many fronts and will compel firms to demonstrate that they are taking cyber seriously in all that they do. However, compliance with these regulations will only be one step towards assuring effective governance and control of institutions' Cyber Risk.

In this paper, we explore the underlying challenges with regard to Cyber Risk management and analyze the nature of increasingly stringent regulatory demands. Putting these pieces together, we frame five strategic moves which we believe will enable businesses to satisfy business needs, their fiduciary responsibilities with regard to Cyber Risk, and regulatory requirements:

1. Seek to quantify Cyber Risk in terms of capital and earnings at risk
2. Anchor all Cyber Risk governance through risk appetite
3. Ensure effectiveness of independent Cyber Risk oversight using specialized skills
4. Comprehensively map and test controls, especially for third-party interactions
5. Develop and exercise major incident management playbooks

While this paper is US-centric, especially with regard to regulation, these points are consistent with global trends for Cyber Risk management. Further, we believe that our observations on industry challenges and the steps we recommend to address them are applicable across geographies, especially when considering prioritization of Cyber Risk investments.

1 Joint Chiefs of Staff

FIVE STRATEGIC MOVES

The current environment poses major challenges for Boards and management. Leadership has to fully understand the Cyber Risk profile the organization faces to simultaneously protect the institution against ever-changing threats and be on the front foot with regard to increasing regulatory pressures, while prioritizing the deployment of scarce resources. This is especially important given that regulation is still maturing and it is not yet clear how high the compliance bars will be set and what resources will need to be committed to achieve passing grades.

With this in mind, we propose five strategic moves which we believe, based on our experience, will help institutions position themselves well to address existing Cyber Risk management challenges.

1. SEEK TO QUANTIFY CYBER RISK IN TERMS OF CAPITAL AND EARNINGS AT RISK

Boards of Directors and all levels of management intuitively relate to risks that are quantified in economic terms. Explaining any type of risk, opportunity, or tradeoff relative to the bottom line brings sharper focus to the debate.

For all financial and many non-financial risks, institutions have developed methods for quantifying expected and unexpected losses in dollar terms that can readily be compared to earnings and capital. Further, regulators have expected this as a component of regulatory and economic capital, CCAR, and/or resolution and recovery planning. Predicting losses due to Cyber is particularly difficult because it consists of a combination of direct, indirect, and reputational elements which are not easy to quantify. In addition, there is limited historical cyber loss exposure data available to support robust Cyber Risk quantification.

Nevertheless, institutions still need to develop a view of their financial exposures of Cyber Risk with different levels of confidence and understand how this varies by business line, process, or platform. In some cases, these views may be more expert based, using scenario analysis approaches as opposed to raw statistical modeling outputs. The objectives are still the same - to challenge perspectives as to how much risk exposure exists, how it could manifest within the organization, and how specific response strategies are reducing the institution's inherent Cyber Risk.

2. ANCHOR ALL CYBER RISK GOVERNANCE THROUGH RISK APPETITE

Regulators are specifically insisting on the establishment of a Cyber Risk strategy, which is typically shaped by a Cyber Risk appetite. This should represent an effective governance anchor to help address the Board's concerns about whether appropriate risks are being considered and managed effectively.

Setting a risk appetite enables the Board and senior management to more deeply understand exposure to specific Cyber Risks, establish clarity on the Cyber imperatives for the organization, work out tradeoffs, and determine priorities.

Considering Cyber Risk in this way also enables it to be brought into a common framework with all other risks and provides a starting point to discuss whether the exposure is affordable (given capital and earnings) and strategically acceptable.

Cyber Risk appetite should be cascaded down through the organization and provide a coherent management and monitoring framework consisting of metrics, assessments, and practical tests or exercises at multiple levels of granularity. Such cascading establishes a relatable chain of information at each management level across business lines and functions. Each management layer can hold the next layer more specifically accountable. Parallel business units and operations can have common standards for comparing results and sharing best practices. Finally, Second and Third Line can have focal points to review and assure compliance.

A risk appetite chain further provides a means for the attestation of the effectiveness of controls and adherence to governance directives and standards. Where it can be demonstrated that risk appetite is being upheld to procedural levels, management will be more confident in providing the attestations that regulators require.

3. ENSURE EFFECTIVENESS OF INDEPENDENT CYBER RISK OVERSIGHT USING SPECIALIZED SKILLS

From our perspective, firms face challenges when attempting to practically fit Cyber Risk management into a "Three Lines of Defense" model and align Cyber Risk holistically within an enterprise risk management framework.

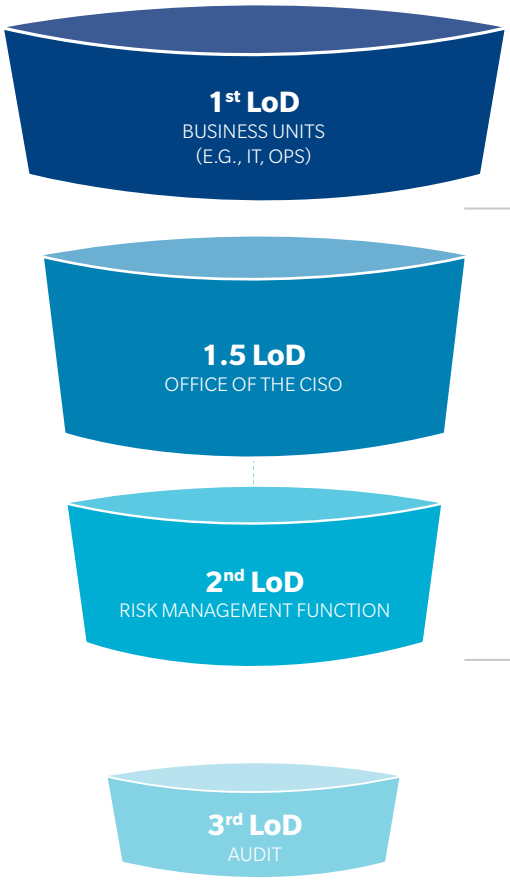
CROs and risk management functions have traditionally developed specialized skills for many risk types, but often have not evolved as much depth on IT and Cyber Risks. Organizations have overcome this challenge by weaving risk management into the IT organization as a First Line function.

In order to more clearly segregate the roles between IT, business, and Information Security (IS), the Chief Information Security Officer (CISO) and the IS team will typically need to be positioned as a 1.5 Line of Defense position. This allows an Information Security group to provide more formal oversight and guidance on the cyber requirements and to monitor day-to-day compliance across business and technology teams.

Further independent risk oversight and audit is clearly needed as part of the Third Line of Defense. Defining what oversight and audit means becomes more traceable and tractable when specific governance mandates and metrics from the Board down are established.

Institutions will also need to deal with the practical challenge of building and maintaining Cyber talent that can understand the business imperatives, compliance requirements, and associated Cyber Risk exposures. At the leadership level, some organizations have introduced the concept of a Risk Technology Officer who interfaces with the CISO and is responsible for integration of Cyber Risk with Operational Risk.

Exhibit 1: Three Lines of Defense concept as applied to Cyber



- Assess Cyber Risks associated with activities of the business unit on an ongoing basis
- Ensure that Cyber Risk information is shared in a timely manner with senior management, including the CEO

- Ensure operations are consistent with Cyber Risk management framework
- Identify, measure and monitor Cyber Risks and notify the CEO, board and CRO accordingly
- Maintain sufficient independence, stature, authority, resources and access to Board
- Be well integrated with enterprise-level strategic risk management function
- Maintain linkages to key elements of internal and external dependency management such as policies, standards, roles and responsibilities

- Evaluate effectiveness of risk management, internal controls, and governance
- Assess whether the Cyber Risk management framework is appropriate in the face of emerging risks and complies with laws and regulations
- Incorporate assessment of Cyber Risk management into overall audit plan of enterprise
- Evaluate compliance via penetration testing and vulnerability assessments

4. COMPREHENSIVELY MAP AND TEST CONTROLS, ESPECIALLY FOR THIRD PARTY INTERACTIONS

Institutions need to undertake more rigorous and more frequent assessments of Cyber Risks across operations, technology, and people. These assessments need to test the efficacy of surveillance, the effectiveness of protection and defensive controls, the responsiveness of the organization, and the ability to recover in a manner consistent with expectations of the Board.

Exhibit 2: Key Cyber control tests, aligned to the NIST Cybersecurity Framework

Given the new and emerging regulatory requirements, firms will need to pay closer attention to the ongoing assessment and management of third parties. Third parties need to be tiered based on their access and interaction with the institution's high value assets.

Exhibit 3: Key third party Cyber Risk management controls

1	**DUE DILIGENCE REQUIREMENTS (INITIAL AND ONGOING)**	• Company background accreditation • Financial reviews • Insurance liability coverage validation • Business license certification • Information security assessment + onsite visit
2	**SECURITY ASSESSMENTS (ONSITE/REMOTE)**	• Ongoing outside-in external security scans • Security recertifications (e.g. annually) • Changes in regulations and/or compliance requirements
3	**SECURITY SCORECARDS**	• Technology operational metrics (availability, reliability) • Reported cyber security events (time to detect, respond, communicate, resolve, associated impact) • Vendor/partner security training compliance
4	**ESCALATION AND REPORTING**	• Third party review meetings • Escalation and tracking of issues/concerns identified • Board and Risk governance reporting

Through this assessment of process, institutions need to obtain a more practical understanding of their ability to get early warning signals against cyber threats. In a number of cases, a firm may choose to outsource more IT or data services to third party providers (e.g., Cloud) where they consider that this option represents a more attractive and acceptable solution relative to the cost or talent demands associated with maintaining Information Security in-house for certain capabilities. At the same time, the risk of third party compromise needs to be fully understood with respect to the overall risk appetite.

5. DEVELOP AND EXERCISE INCIDENT MANAGEMENT PLAYBOOKS

A critical test of an institution's Cyber Risk readiness is its ability to quickly and effectively respond when a cyber attack occurs. As part of raising the bar on cyber resilience, institutions need to ensure that they have clearly documented and proven cyber incident response plans that include a comprehensive array of attack scenarios, clear identification of accountabilities across the organization, response strategies, and associated internal and external communication scenarios.

Institutions need to thoroughly test their incident response plan on an ongoing basis via table top exercises and practical drills. As part of a table top exercise, key stakeholders walk through specific attack scenarios to test their knowledge of response strategies. This exercise provides an avenue for exposing key stakeholders to more tangible aspects of Cyber Risk and their respective roles in the event of a cyber attack. It also can reveal gaps in specific response processes, roles, and communications that the institution will need to address.

Last but not least, incident management plans need to be reviewed and refined based on changes in the overall threat landscape and an assessment of the institution's cyber threat profile; on a yearly or more frequent basis depending on the nature and volatility of the risk for a given business line or platform.

CYBER RISK MANAGEMENT CHALLENGES

Given the alarming nature of the external cyber attack environment, institutions face a number of major challenges inside their organizations, especially within the associated processes and IT systems.

ESTABLISHING COMMON UNDERSTANDING OF CYBER RISK PROFILE UP TO BOARD LEVEL

An increasing number of Boards are creating pressure on their respective management teams to provide a much clearer view of their Cyber Risk profile. More and more, organizations are arming their Boards with the right level of intelligence on the overall threat landscape, their readiness to respond to a cyberattack, and where critical cyber investments are being directed.

From our perspective, organizations are spending a tremendous amount of effort and investment in cyber defense activities, but most are unable to synthesize a vast amount of technical data and metrics into a clear set of Key Risk Indicators (KRIs) and actionable management intelligence for senior decision makers. A significant number of Boards are also still not fully proficient in understanding technical metrics which increases the burden on management to distill clear messages on the state of their cyber program and the associated risks which need to managed and mitigated.

The lack of clear KRIs and actionable intelligence, coupled with challenges in the Boards' technology proficiency, results in the Boards' inability to determine if their direction-setting in governance is effective to shaping the organization's Cyber Risk posture.

QUANTIFYING CYBER RISK EXPOSURE AND VALUE OF DEFENSIVE INVESTMENTS

Risk quantification is a critical step in the risk assessment process. It provides institutions with the ability to express their Cyber Risk exposure in economic terms, thereby removing subjectivity when gauging the potential business impact to the organization. It also enables senior management to direct and prioritize investments that will drive the most effective capital and earnings at risk to exposures. In some cases (e.g., credit risk), it is even possible to relate total organizational risk directly to parameters associated with specific loan amounts.

Unfortunately, the industry has not yet developed robust, mature quantification approaches for Cyber Risk. Most institutions rely on qualitative guidance from "heat maps" that describe their vulnerability as "low", "medium", or "high" based on estimates that lump together frequent small losses and rare large losses. But this approach doesn't help institutions understand if they are dealing with a $10 million problem or a $100 million problem, let alone whether they should invest in malware defenses, email protection, alternative third party solutions, or training. To add to this challenge, quantification solutions and methods are limited, even in terms of establishing relative risk measures and trends. Consequently, the inability to align on an objective view of Cyber Risk exposure for institutions makes it extremely difficult to understand the cost-benefit tradeoffs of potentially enormous cyber investments and to answer the key Board and executive management question – "How much is enough?"

ADDRESSING CULTURAL ASPECTS OF CYBER RISK

Institutions are increasingly realizing that their biggest cyber threats often originate from within their own organization. Cyber adversaries have taken advantage of unsuspecting employees through spear phishing or social engineering attacks. There is also a growing threat of rogue insiders who seek to disrupt business operations or steal the organization's "crown jewels" which can include employee records, customer information, contracts, intellectual property, and other highly sensitive information. This risk is especially elevated in situations when organizations enter new markets, complete notable M&A transactions, or enter periods of turbulence that result in workforce displacement.

Institutions have historically tried to mitigate these challenges by focusing on the technology aspect of cyber defense, through rigorous identity management, access controls, and employee monitoring. However, technical cyber resilience is not sufficient in these situations. To mitigate employee-driven cyber incidents, institutions will need to obtain a clear picture of their organization's internal risk culture, Cyber Risk awareness, and gaps in incentives and interventions. Armed with this knowledge, new and innovative HR and technology policies can be implemented appropriately.

BALANCING CYBER RISK CONTROL WITH PACE OF DIGITAL INNOVATION

Digital innovation continues to be a top priority across many financial institutions. Institutions are focused on addressing rising customer demands for fast, personalized, and compelling digital experiences. As a result, many firms have introduced new digital channels and digital products and interactions. At the heart of this transformation is a fundamental shift in the way applications are built and connected across internal and external systems. This transformation has resulted in significant improvements in the customer experience, increasing cross-selling and loyalty which ultimately results in higher sales and profits.

At the same time, a hyper-connected environment increases the overall cyber attack surface for financial institutions, and creates new vulnerabilities that organizations can be unaware of, and in many cases, de-prioritize in favor of innovation. Institutions clearly need to balance their desire to accelerate speed to market against competitors while ensuring that core systems and capabilities are safe, secure, and reliable.

Firms need to give careful thought to the nature of Cyber Risk across their landscape of technologies. The most critical systems will need the highest level of rigor, controls and tests with regard to cyber security. Given a finite number of resources and expertise, the multiple platforms and applications will need to be tiered in a manner that recognizes their criticality and nature of Cyber Risk.

In specific cases where larger institutions engage smaller FinTech organizations to develop new digital experiences, there is a need to align on an appropriate level of security in a manner that is not overwhelming to the smaller organization, but appropriately weighs the risk of these relationships. This requires both parties to agree on security design principles and technologies that enable innovation, while protecting their primary systems, data, and the financial wellbeing of their customers.

THE GROWING WAVES OF CYBER REGULATION

In the recent past, there have been three major cyber-related regulatory developments in the US:

A. The Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards ("ECRM ANPR") jointly issued by the Board, OCC, and FDIC
B. The Cybersecurity Requirements for Financial Services Companies issued by the New York Department of Financial Services (NY DFS)
C. The revised version of the FFIEC Information Security Handbook

As has been reported broadly and discussed in many industry forums, these regulatory documents present some of the most prescriptive Cyber Risk management requirements to date and include substantial new requirements for an enterprise-wide view of cyber security. We will not present a detailed summary of these regulations, but rather will synthesize the major points where we believe the regulations impose new and challenging pressures.

TOP-TO-BOTTOM CASCADING OF CONTROL

Consistent with other prominent regulatory programs, cyber regulations establish an expectation of direct oversight by the Board of Directors based on policies, standards, and procedures articulated by management. Once a comprehensive Cyber Risk management strategy is defined and implemented, organizations need to continuously monitor its effectiveness and measure its alignment with business priorities.

Regulators want to enforce this philosophy by requiring firms to identify and assess all the activities and exposures that present Cyber Risk, and subsequently aggregate them to evaluate the enterprise-wide residual Cyber Risk. Continuous monitoring of such aggregated information will require significant effort from organizations as they will need to design relevant metrics at different levels and make significant changes to their business processes across functions to include Cyber Risk in consistent ways.

Requirements for certification or attestation of compliance to internal policies, procedures, and regulatory standards will require further process definition and accountabilities clarification.

MULTIPLE LINES OF MANAGEMENT DEFENSE

Financial institutions have already been extending the 'Three Lines of Defense' model to Cyber Risk management, drawing on experience from other areas of risk management. Regulators appear to be making such a model a formal requirement without specifying all expectations.

ECRM specifically suggests increased responsibilities for business lines, Audit, an independent Risk function, and the Board. Starting from the base of the 'Three Lines of Defense' model, business units and technology still form the First Line of Defense. However, business units now face the added responsibility of identifying activities that contribute to Cyber Risk and measuring Cyber Risk on a continuous basis. In addition, business units will be required to frequently conduct assessments to evaluate the Cyber Risk across their activities and report them to the independent risk management function and senior management.

Regulators are favoring the CISO role reporting to the Risk function – implying a change in the interaction model where the historical reporting line of a CISO was to the Chief Information Officer (CIO). The new paradigm expects a CISO to drive the execution of Cyber Risk management strategy from top-down with an enterprise wide remit. At the same time, the CISO also needs to focus on identifying, measuring, and managing the Cyber Risk at a business activity level with front line business unit management and the technology organization.

In addition to strengthening the role of business units and elevating the Cyber Risk function and CISO to the enterprise level, regulators are also prescribing that Audit play an elevated role. The Audit function has been traditionally responsible for conducting an independent assessment regarding Cyber Risk controls compliance. Going forward, Audit teams will be required to assess whether the established Cyber Risk management strategy is appropriate for the nature of the business, strategic objectives, and the board-approved residual Cyber Risk goals.

While the roles of business units and IT as the First Line of Defense and Audit as the Third Line of Defense are consistent across the industry, the design of the Second Line of Defense (made up of the CISO and the enterprise risk function) still varies. The role of the CISO and the definition of second line risk oversight will likely become an important area for achieving further organizational clarity, and an important one to get right to ensure effectiveness of activities without duplication of effort, diffusion of expertise, or a blurring of accountabilities. An organization's ability to effectively define and deploy their Lines of Defense will be critical in accelerating their readiness to monitor their primary assets and respond in the event of a cyber attack.

INSTITUTIONAL AND SYSTEMIC RESILIENCE

The new regulation is clearly oriented towards establishing greater institutional resiliency in being able to detect and manage inevitable cyberattacks through a more explicit risk-based approach.

Further, there is a push towards promoting resiliency of the financial services system through regulation – a rationale for the imposition of controls to prevent interconnected institutions from negatively impacting each other and the financial system more broadly. We can expect this to lead to common checklists, standard reporting, regulatory submissions, etc. all aimed at establishing a level of certainty or confidence across the financial services sector. Such reviews would certainly be more intrusive and subjective – similar to qualitative aspects of CCAR reviews where fundamental risk management capabilities have been questioned.

The more traditional approach to cyber security has focused on strengthening the perimeter by investing in a broad spectrum of sophisticated technical capabilities and process controls across the organization. However, as recent regulation has identified, this approach has become less effective because organizations do always not have a clear understanding of their cyber adversaries and their related motives. In addition, cyber adversaries constantly evolve their attack methods and vectors. What will need to be refined and enhanced is the alignment of cyber surveillance with the Cyber Risk profile and risk appetite of the institution. In addition, the scope of surveillance will need to broaden and deepen as firms seek to confirm internally that Cyber Risk mindfulness is present and sufficiently effective throughout the organization.

EXPANDED VIEW OF THE ATTACK SURFACE TO INCLUDE THIRD PARTIES

One of the prominent features of the proposed regulations is the expansion of the notion of situational awareness. As a corollary of the risk-based approach to cybersecurity, the scope of situational awareness has expanded beyond organizational boundaries. Keeping the interconnectedness of the financial sector in mind, regulators want financial institutions to think carefully about the impact they can have on the rest of the financial sector while managing the Cyber Risk they face from external dependencies and third-party relationships.

Regulators are also expecting institutions to expand the view of cyber threats to fully consider third parties (including vendors, partners and peers in the network) – both in terms of vulnerabilities that could undermine critical services they provide to regulated financial institutions and the potential for them to be the weak point of defense through which cyber attackers infiltrate the critical systems of a financial institution.

Practically, it is also important to understand the nature of third-party access. Increasingly, adversaries are exploiting the electronic access consumers, corporates, and others have via their multi-channel, multi-device connections to financial institutions. In these arrangements, an institution needs to look at methods to help protect the customer as both a means to protect themselves and demonstrate client support and due care.

Considering the cyber exposure of the many third parties is critical, but this also exponentially increases the complexity of the problem for financial institutions. Many organizations struggle to scale up their Information Security and IT Risk assessment and monitoring processes to keep up with the proliferation of third party vendors and partners within their ecosystem (and further, to deal with providers to these third parties, typically defined as fourth parties). The scoping of regulation to the largest institutions creates room for potentially unregulated contractors, vendors, and clients who have some degree of interface with enterprise systems to create transmission vectors.

Organizations will to need to carefully evaluate the cyber resiliency of their overall ecosystem in the broadest sense and lay the necessary groundwork with key vendors, allies, and partners to address "weak links" in their overall business supply chain.

INTEGRATED, PROGRAMMATIC APPROACH TO CYBER RISK

Cyber regulation is focused on defining a distinct "cyber defense program", that can be identified and documented for supervisors, and establishing a "Cyber Risk management strategy" that will provide guidance to all business activities. Given regulatory insistence on multiple lines of governance and control, an institution's cyber program needs to be broader than the IT or Risk organization, with clear linkages to the institution's strategy and controls. Policies and procedures are one form through which cyber considerations are meant to be promoted through institutions, with accompanying training and positioning of specialized personnel in various parts of the organization also suggested.

Choreographing the interactions of standards and procedures, their enforcement, and the various accountabilities throughout the organization in a consistent manner will be particularly difficult.

We can expect that the Board, senior executives, all the way down to front line supervisors, will seek evidence that policies, procedures, training, and expertise are effectively resulting in a much broader understanding of cyber aspects of the business – which is a significant change for a risk type that is not intuitive for many, nor is an existing element of their day-to-day operations.

CONCLUSION

Cyber adversaries are increasingly sophisticated, innovative, organized, and relentless in developing new and nefarious ways to attack institutions. Cyber Risk represents a relatively new class of risk which brings with it the need to grasp the often complex technological aspects, social engineering factors, and changing nature of Operational Risk as a consequence of cyber. Leadership has to understand the threat landscape and be fully prepared to address the associated challenges. It would be impractical to have zero tolerance to Cyber Risk, so institutions will need to determine their risk appetite with regard to cyber, and consequently, make direct governance, investment, and operational design decisions.

The new and emerging regulations are a clear directive to financial institutions to keep Cyber Risk at the center of their enterprise-wide business strategy, raising the overall bar for cyber resilience. The associated directives and requirements across the many regulatory bodies represent a good and often strong basis for cyber management practices but each institution will need to further ensure that they are tackling Cyber Risk in a manner fully aligned with the risk management strategy and principles of their firm.

In this context, we believe the five moves advocated in this paper represent multiple strategically important advances almost all financial services firms will need to make to meet business security, resiliency, and regulatory requirements.

Oliver Wyman is a global leader in management consulting. With offices in 50+ cities across nearly 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 4,500 professionals around the world who help clients optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. For more information, visit www.oliverwyman.com. Follow Oliver Wyman on Twitter @OliverWyman.

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

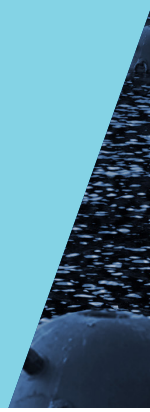
ASIA PACIFIC
+65 6510 9700

ABOUT THE AUTHORS

PAUL MEE
Partner in the Digital and Financial Services Practices
paul.mee@oliverwyman.com

JAMES MORGAN
Partner in the Digital and Financial Services Practices
james.morgan@oliverwyman.com

www.oliverwyman.com



OLIVER WYMAN