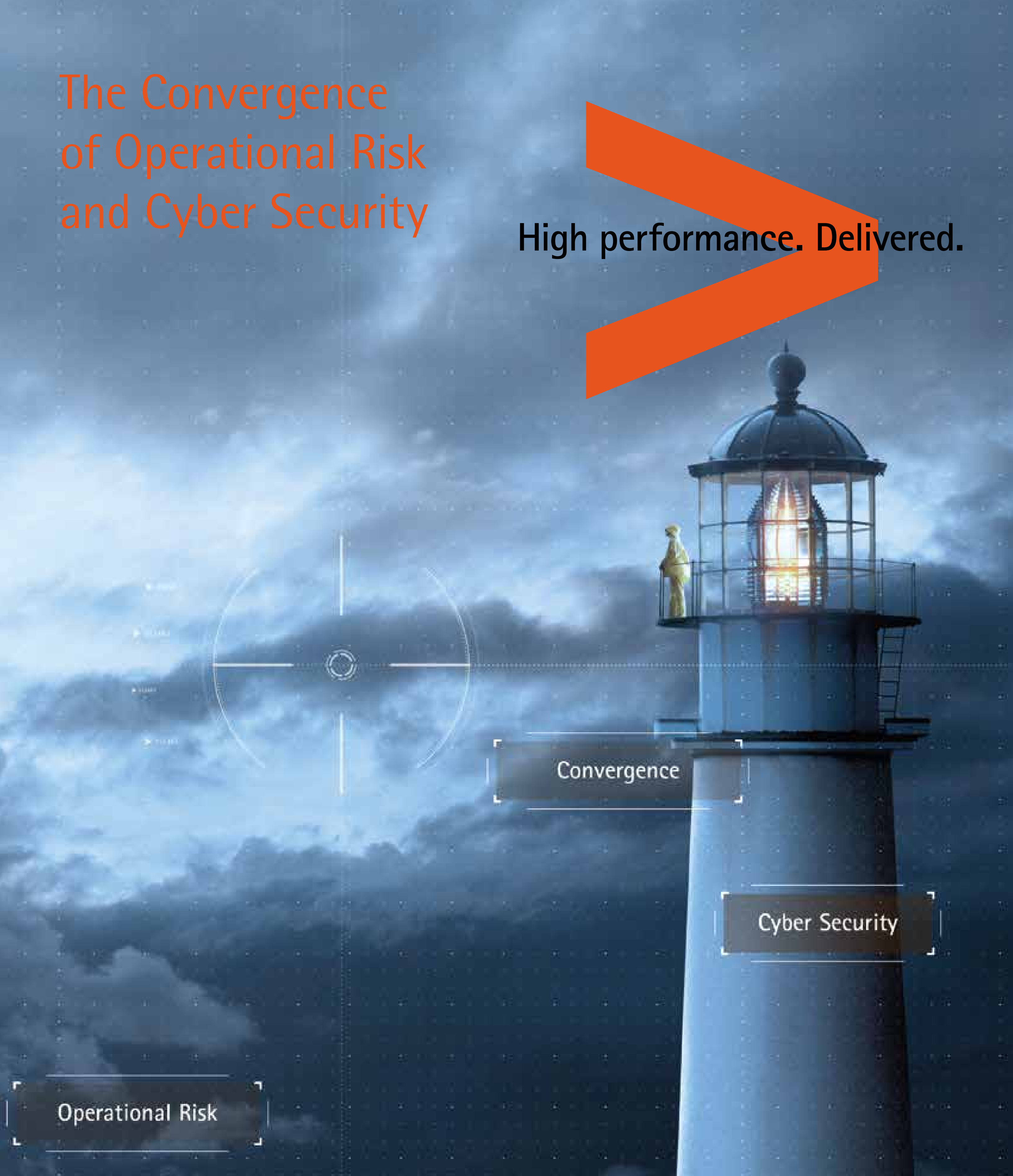
accenture

Chartis

The Convergence of Operational Risk and Cyber Security

High performance. Delivered.



A joint paper by Accenture and Chartis Research advising that operational risk management and cyber security processes should align to better cope with the increasing cyber threat and improve resilience.

Cyber security has jumped to the top of companies' risk agenda after a number of high profile data breaches, ransom demands, distributed denial of service (DDoS) attacks and other hacks. In an increasingly digitized world, where data resides in the cloud, on mobiles and devices connected to the "Internet of Things" threat vectors are multiplying, threatening firms' operations, customer and bank details and future financial stability.

Firms should develop a strategy to cope with this cyber threat emanating from online criminals, hacktivists or nation states looking to destabilize payment and financial systems such as Russia's alleged 2007 cyber-attack against Estonia's financial services ecosystem.[1] The need is most pressing at large scale financial services institutions as many of these sit at the apex of the financial system.

This is a report by Accenture and Chartis analyzing the benefits of better alignment across operational risk management procedures with cyber security in an enterprise risk management (ERM) framework. The objective for leading firms should be to focus on increasing the resilience of the organization, and despite the best efforts it is highly unlikely that any firm can completely avoid security issues in the digitally-connected world we all operate within.

Cooperation is an essential starting point in the organization—a DDoS attack or data breach impacts people, processes and technology across the business. As well as getting IT systems back up and running financial institutions (FIs) should write to customers and regulators, activate back-up facilities, and compensate any losses. Operational and cyber security employees need lines of communications and a coordinated pre-planned response. Firms should take this opportunity to review their existing risk management processes, departments and responsibilities with respect to cyber security, re-aligning them into an overall operational and ERM strategy with boardroom backing.

Scope of the Problem: The Cyber Security Threat

You cannot open a paper, or indeed a link, these days without hearing about a new cyber-attack. The immediate need for firms to protect themselves is made more pressing by the manner in which regulators retrospectively sanction firms for past breaches.

In September 2015, for instance, the Securities and Exchange Commission (SEC) fined R.T. Jones Capital Equities Management, a St. Louis-based investment adviser, $75,000 for failing to establish the required cyber security policies and procedures in advance of a breach that occurred in July 2013. An unknown hacker gained access to data and compromised the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients, after infiltrating its third-party hosted web server. The attack left R.T. Jones' clients, vulnerable to fraud theft and prompted the SEC's action for violating Rule 30(a) of Regulation S-P under the US Securities Act of 1933.[2]

As Marshall S. Sprung, Co-Chief of the SEC Enforcement Division's Asset Management Unit, said in the ruling:[3] "Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cyber security events and have clear procedures in place rather than waiting to react once a breach occurs."

Other examples illustrating the scope of the problem include:

- Interpol and Kaspersky Lab revealed in February 2015[4] that about $1bn had been stolen over a two year period from financial institutions worldwide by a cybercriminal gang comprising members from Russia, Ukraine, other parts of Europe and China. The Moscow-based security firm dubbed the criminal gang "Carbanak" and Interpol was in pursuit. The criminal case proves that FIs are just as susceptible to cyber-attacks as retailers that hold card details or telcos and utilities among others. They are also at the top of the tree for any fraud-related attack.

- The Ponemon Institute LLC has calculated that cyber risk translates to a mean annualized cost, for every company, of $7.7 million.[5]

- In a recent "2015 Cyber Security Global Survey" conducted by Chartis Research,[6] which questioned 103 risk professionals, 69% of them said they expect their cyber security expenditure to increase next year by more than 10%.

- The World Economic Forum (WEF) again identified technological risks, in the form of data fraud, cyber-attacks among the top ten risks in terms of likelihood while critical information infrastructure breakdown is among its top ten risks in terms of impact.[7] The threats are real and growing.

Risk Controls

Defining the Problem

Financial institutions (FIs) want to establish controls to manage cyber risk from the top down. However, while FIs are familiar with the basics of firewalls, malware and phishing, they are struggling to connect the technical aspects of cyber security with the people and process risks that operational risk is designed to monitor and control.

A necessity for establishing control is to first set a good definition of the problem. Many firms produce their own cyber security definition. A common starting point is with the International Standards Organization's ISO 27k series on IT risk, which includes a cyber security component, under ISO/IEC 27032. It reads as follows:

Officially, ISO/IEC 27032 addresses "Cybersecurity" or "Cyberspace security," defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace."[8]

In turn "Cyberspace" is defined as the "complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, and which does not exist in any physical form."[9]

In the US, the National Institute of Standards and Technology (NIST) can also provide useful definitions and guidelines. Both external frameworks should be examined as part of an early stage project to align operational risk management (ORM) and cyber security procedures.

The main definition problem that FIs encounter is around scope. Broad and narrow definitions of cyber security both have strengths and weaknesses. A broad definition provides wide coverage and lends itself to a cross-silo approach. However, it can lead to confusion over responsibilities and cause significant overlap with other areas like IT security. A narrow definition can result in the creation of another tactical risk management silo, which is undesirable. The aim must be to develop an open definition that covers all of the threat vectors, but clearly assigns responsibilities.

Some definitions of cyber security put forward by representatives of international FIs in conversation with Chartis and Accenture appear in Table 1.

Table 1. Varying definitions of cyber security

Examples – Definition of Cyber Security	Coverage	Strengths	Weaknesses
"Protection against services or applications in cyberspace being used for or are the target of a crime, or where cyberspace is the source, tool, target, or place of a crime."	Covering incidents which occur in cyberspace, i.e. online.	Differentiates between local IT issues and online IT.	Doesn't focus on physically-enabled network attacks, such as black boxes.
"Detection, prevention and recovery processes for malicious or deliberate damage, bypass or removal of IT controls."	Covering incidents wherein IT-specific controls are deliberately broken.	Differentiates between IT security and cyber security (by specifying deliberate attacks), and also fraud risks (by specifying IT controls).	Narrow definition; can cause confusion around responsibilities when cross-silo attacks occur such as when a fraud attack is initiated by a phishing malware.
"The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."	Defining cyber security as essentially encompassing the security of all IT processes.	Broad focus, enabling the capture of information from multiple potential silos.	Soft definition; often cannot be distinguished from IT security definitions, such as: "Information security is the set of business processes that protects information assets regardless of how the information is formatted or whether it is being processed, is in transit or is being stored."
"The attempt to subvert information risk controls of the bank for the agenda of the perpetrator."	Defining cyber security as the protection of access to information in an IT system.	Defines information risk controls as a target for perpetrators.	Does not distinguish between technologically-enabled and non-technologically enabled attacks.

Source: Chartis Research, based on discussions with financial institutions, August to December 2015

Beyond this, whether definitions are broad or narrow, or principles- or rule-based, there appears to be a pressing need to help establish frameworks and move the conversation to the board level. More than definitions, the important factors are responsibility and awareness of what each involved party is doing to help protect the institution.

Expanding Operational Risk to Include Cyber Security

Operational risk is defined by the Basel Committee as: "The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events."[10]

Cyber-attacks from external criminals or internally disgruntled employees can fit this definition. They become a problem only if the processes and people elements in an FI's strategy are not sufficiently developed. If the chief risk officer (CRO) is talking to the chief information security officer (CISO) and both are aware of their specific responsibilities, and how they align with the wider ERM strategy, then a data loss event, DDoS attack or hack needn't be catastrophic. Joining the dots and aligning a strategy is key. The challenge is that cyber security is traditionally managed through its own set of internal controls within IT, which are separate from the duties and processes required for operational risk management or compliance. Bringing cyber security into a common framework is necessary in our view.

In addition, the Basel Committee's 2014 report on operational risk includes cyber-attacks as a scenario. This illustrates the nature of the operational risk that can result from cyber security breaches, ranging from continuity to credit and market risk.

"...some banks have developed scenarios related to earthquakes and other catastrophic events such as a cyber-attack to assess not only the operational risk exposures (i.e. business continuity, costs, fraud losses, lawsuits, etc.) but also other risks such as credit risk (i.e. increased defaults, devaluations of collateral), market risk and general economic conditions (i.e. lower revenues)."[11]

The expansion of operational risk to include cyber threats is being driven by a number of trends:

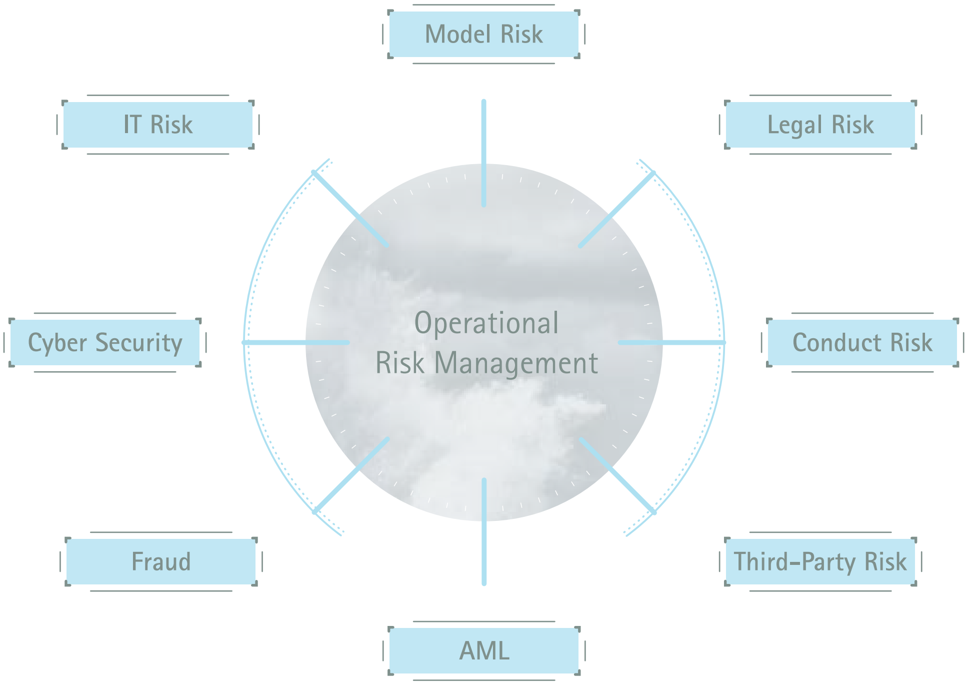
1) The rising number and complexity of cyber-attacks now represents a real threat to an FI's profitable existence. Reputational damage and regulatory fines await FIs that cannot prove a coordinated response, communication and back-up plan is in place.

2) Boards and senior leadership increasingly recognize that the solution lies beyond the technology layer and in the broader people and processes of the institution.

3) Poor cost-to-income ratios are driving banks to consolidate their silo-based risk management.

The "new normal" of expanded operational risk management (ORM) strategies that align with cyber security, fraud and anti-money laundering (AML) disciplines is illustrated in Figure 1. For example, cyber security events such as the "Carbanak" $1bn loss from financial institutions worldwide and this year's Dyre Wolf malware attack against banks[12] show that phishing, malware, fraud, money laundering and business disruption all go together. A cyber risk response and ORM strategy should be similarly coordinated.

Figure 1. Operational risk management can be the integration point for cyber security and other risk management areas



Source: Chartis Research, December 2015

Chartis Research has seen operational frameworks and methodologies expanding into full governance, risk and compliance (GRC) initiatives at FIs. The three lines of defense – inputs such as risk events arising from malware; your monitoring and coping mechanisms; and auditing of the strategy (see Figure 2) – mean that a firm should be able to prove a boardroom-backed governance and risk structure is in place and reinforced by training and testing from the bottom-up.

Regulators and partners in the financial supply chain will be reassured by strong managerial oversight and the presence of a cyber risk-aware culture. In addition, the near-immediate dissemination of negative news through social media and the internet has increased the threat of reputational risk. Loss of reputation could lead to a loss of customer and stakeholder trust, loss of revenue, and a higher level of regulatory scrutiny in future, posing a direct threat to executives and the C-suite, who can potentially lose their jobs.

Establishing a Framework

By taking an integrated view of operational risk and cyber security, FIs will be better able to protect, monitor and mitigate a wider array of threats.

Accenture and Chartis have identified four key building blocks for delivering alignment:

1. Governance and ownership: Tangible improvements can be performed by establishing clear lines of responsibility from board level downwards, including organizational definitions where cyber security and operational risk are aligned as part of a formal GRC strategy.

2. Taxonomies and methods: Bridging the gap between the CISO/ technology or information officer and the CRO by creating a common language.

3. Skills and capabilities: Multi-disciplinary capabilities and competencies across operational risk and cyber security should be encouraged. Practitioners should meet their counterparts in different departments to develop a unified response.

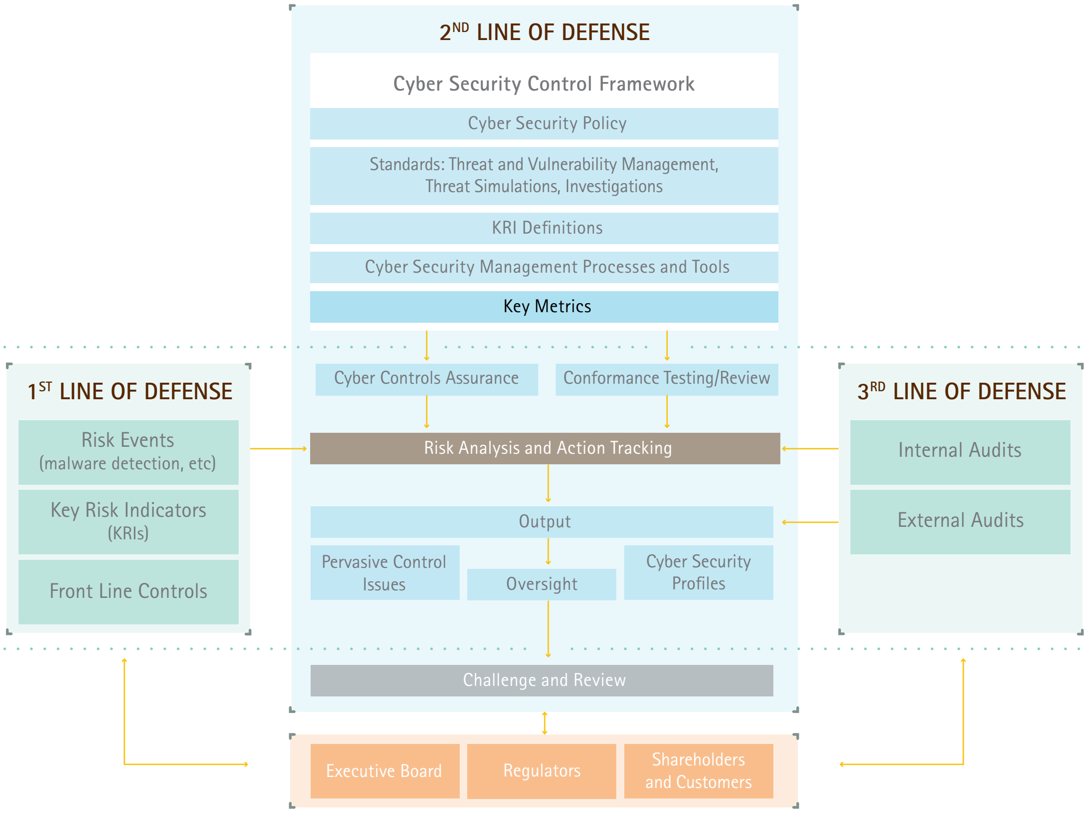
4. Technology and data: Technology is a key facilitator for aligning operational and cyber risk strategy. Advanced data management, analytics, modeling and reporting solutions deliver a better response if attacked.

Governance and Ownership

Top-down governance processes and board-level involvement are important.

First and foremost, FIs should establish cyber security processes as mapped across the three lines of risk defense, covering inputs; monitoring of the strategy; and auditing of the strategy (Figure 2).

Figure 2. Framework for aligning operational risk with cyber security


2ND LINE OF DEFENSE
Cyber Security Control Framework
Cyber Security Policy
Standards: Threat and Vulnerability Management, Threat Simulations, Investigations
KRI Definitions
Cyber Security Management Processes and Tools
Key Metrics
Cyber Controls Assurance
Conformance Testing/Review
Risk Analysis and Action Tracking
Output
Pervasive Control Issues
Oversight
Cyber Security Profiles
Challenge and Review
1ST LINE OF DEFENSE
Risk Events (malware detection, etc)
Key Risk Indicators (KRIs)
Front Line Controls
3RD LINE OF DEFENSE
Internal Audits
External Audits
Executive Board
Regulators
Shareholders and Customers

Cyber Security Controls

- Cyber is a group risk
- Managed through cyber security control
- Cyber security focuses on “attacks”

Evaluation and Response

- The status of risk is assessed by reviewing multiple sources of risk detail (both self-assessment and independent review)
- This data is analyzed to identify risk themes which drive improvement actions within cyber security

Monitor

- Group and board-level oversight of the cyber security profile
- Risk appetite to be set at business unit and group level

Source: Chartis Research, based on analysis of the risk strategies of several global financial institutions, December 2015

Disaster recovery and business continuity planning (BCP) processes should also be clearly defined and link into an institution’s combined operational and cyber risk strategy.

As an example, cyber risk threats and/or vulnerable events, such as wire transfers, should be examined and modeled start-to-finish as part of any FI’s procedure, with a “kill chain” clearly established to mitigate risk. Potential points of compromise, responsibilities, and remediation measures should all be detailed at each stage to establish a comprehensive framework.

Skills and Capabilities

Even if cyber security is firmly established as part of the three lines of defense and aligned with operational risk, there is a pronounced industry-wide gap in the skills and training of the professionals tasked with delivering the integrated strategy.

Front line troops with job titles such as CISO or chief technology or information officer (CTO/CIO) tend to have a strong understanding of IT, but in many cases they have limited formal risk management understanding.

Similarly, risk managers have a strong understanding of the business and risk concepts needed for a good cyber security response in the event of an attack, but a relatively weak understanding of the complex IT issues involved.

Increasing IT and risk knowledge transfer is a critical success factor when aligning cyber security and operational risk. Staff rotation and shadowing may be helpful in promoting mutual comprehension and understanding. Joint competency centers should also be considered, alongside recruitment and incentive strategies to encourage collaboration. Formal knowledge transfer initiatives should have senior management oversight and support.

Speed will be of the essence if an FI comes under attack so lines of communication between risk and IT professionals should be open. Regular test scenarios can help.

On-going training is also advisable so that FIs can keep pace with any technological and regulatory changes. Training remains particularly crucial as the vast majority of cyber security incidents start from avoidable human error, such as an employee clicking on a phishing email. While many firms focus on technology and prevention, training and awareness of potential cyber risks from the bottom up is essential.

This should include mandatory awareness of good security practices, and periodic testing of employee responses to potential attacks. In addition, while it is important that training is part of the front office, it is also vitally important that responsibility for basic cyber security does not die out in middle management. In interviews conducted by Chartis and Accenture with firms who had implemented phishing testing, they said that management (including the C-suite) were more likely to respond to phishing emails than front-office employees.

Some may work under the illusion that their firms' security systems are protecting and insulating them, but with respect to cyber security, all employees are potentially on the front line.

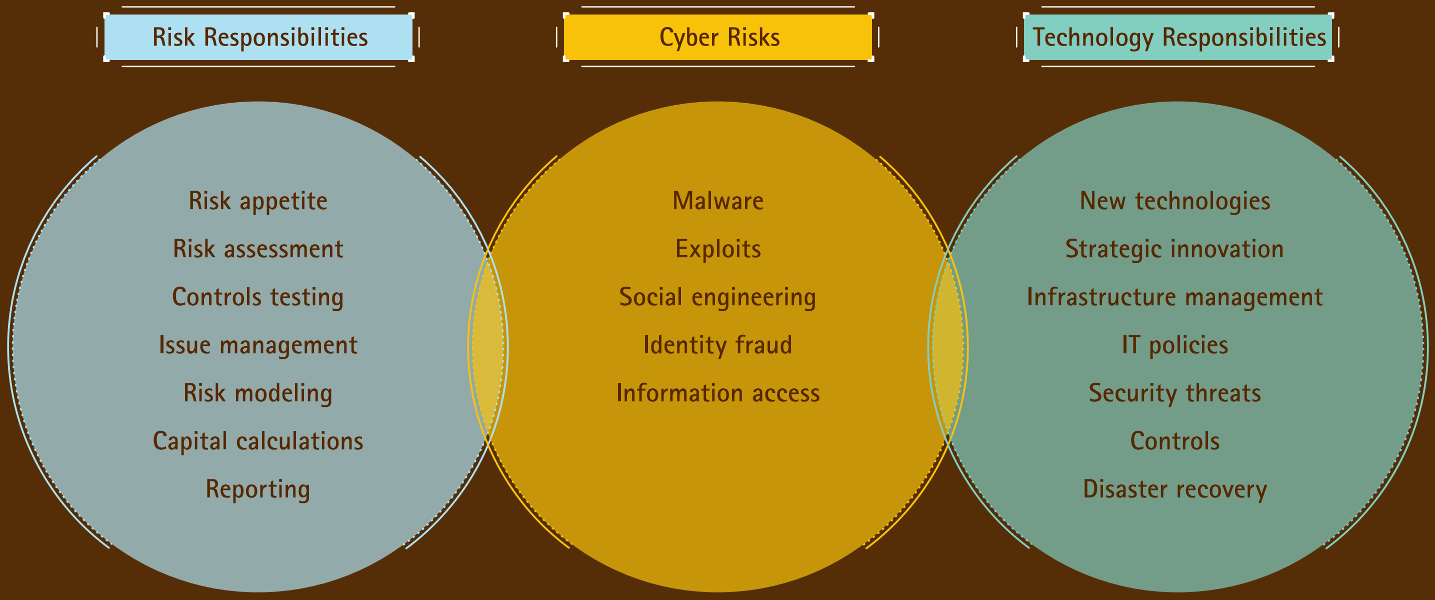
Taxonomies and Methods

If the gap between technological and risk-based knowledge is to be bridged, then the cyber security and operational risk functions need a common language.

This can be established by agreeing to a common definition, using ISO and NIST frameworks if desired, and then formulating a responsibility flowchart.

Cyber security risks can be considered to be part of both the operational risk responsibilities and the typical responsibilities of a CTO/CIO/CISO (Figure 3). Risk and technology responsibilities meet in the middle during cyber security events.

Figure 3. Risk and technology responsibilities


Risk Responsibilities

Risk appetite
Risk assessment
Controls testing
Issue management
Risk modeling
Capital calculations
Reporting

Cyber Risks

Malware
Exploits
Social engineering
Identity fraud
Information access

Technology Responsibilities

New technologies
Strategic innovation
Infrastructure management
IT policies
Security threats
Controls
Disaster recovery

Source: Chartis Research, December 2015

Technology and Data

Technology and data, whether online or stored on internal systems, are a source of risk but can also be a part of the solution.

Good data management, monitoring and analytics can help feed effective processes, communication and early warning mechanisms into the three lines of defense shown in Figure 2. Technology can help deliver an integrated approach to cyber security and operational risk. A common analytical layer is highly desirable.

In addition to the required security tools, Accenture and Chartis consider the following to be important technology elements in any risk-based approach.

Integrated data management

FIs may find it hard to attain a holistic view of their operational risks across the whole enterprise because they have many disparate IT systems in use. An effective operational risk management system should access risk data from various ORM and cyber security applications, as well as operational sources such as AML, 3rd party risk, and fraud management systems, bringing together KRIs based around internal and external losses, malware detection, standards, patching, and model risk management. Unified risk data models and standards are critical.

Metadata

A metadata-driven approach is essential for this integrated cyber ORM approach to work. Metadata is a means of creating a logical and manageable view of all the risk information available to an organization. Use the latest approaches to enterprise data management (EDM) for a more agile and responsive data environment, enabling auditability, traceability of changes, drill-down workflow and enterprise case management.

Real-time reporting

The move towards dynamic and responsive risk management and governance has increased the demand for real-time reporting and the escalation of risk information. The traditional audit-based snapshot approach to ORM should be replaced by dynamic and real-time ORM alerts, including cyber KRIs in a reformed structure that is supported by automated data feeds. Early warning systems can be created in this manner.

Anomaly detection

Current anomaly detection systems are often based on searching for known patterns. However, fraud and cyber security analysts require dynamic abilities to look for unpredictable new patterns of attack and relationships. Advanced anomaly detection software goes beyond business rules to include analytics, using advanced methods such as mathematical correlations, predictive modeling and artificial intelligence to acquire a holistic view of entity activity.

Integrated case management

In most FIs separate business lines use standalone case management databases and workflow solutions for logging and managing alerts. Reporting is also typically done on a siloed basis. Instead FIs are encouraged to pool information. Pooling cross-organizational, cross-border data is perhaps the most important step down the integration path an FI can take. Unusual patterns of behavior and new threats can all be identified more quickly with enterprise-wide search capabilities and remediation action can more easily be activated.

Enterprise Risk Management

Conclusions

Bringing together leadership and capabilities across fraud, IT, cyber security and operational risk in this manner can help FIs to "connect the dots" and improve their enterprise risk management (ERM) strategy. Governance, skills, taxonomies and technology should be aligned with the common definition, language and approach delineated at the start of the alignment push between operational and cyber risk. The ability to view cyber security breaches as a risk, with associated probabilities and impacts, help firms focus on striking the right balance between resilience and protection.

The key recommendations from Accenture and Chartis Research include:

- FIs should establish consistent definitions for cyber security. Firms should avoid the potential creation of another risk management silo by using an open definition that also assigns responsibilities in the event of an attack, helping firms to have a consistent view of cyber security across business and IT processes.
- Cyber security should be managed as a risk discipline across the three lines of defense – ownership, oversight and assurance. This should help firms to align with board-level risk appetite.
- Effective cyber security requires collaboration across silos, knowledge sharing and cooperation between technology and operational risk employees. Each should understand the others' responsibilities. Collaboration between the chief data officer (CDO), CIO, CISO and CRO is very important.
- Coordination between cyber security and operational risk will encourage increased visibility of risks and a communication of cyber security issues at the board level. Boardroom support for the formation of an integrated cyber ORM approach is essential from the top down. Similarly, bottom-up cyber security should be built through a risk-aware culture, including training and periodic testing.
- Alignment between the operational risk and cyber security disciplines should help FIs stay ahead of online criminals, hacktivists and rogue states. A comprehensive pre-planned strategic response will encourage firms to resist the growing cyber threat.

References

[1] "Estonia under cyber attack," Hun-CERT. Access at: http://cert.hu/sites/default/files/Estonia_attack2.pdf

[2] "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach," U.S. Securities and Exchange Commission, press release, September 22, 2015. Access at: http://www.sec.gov/news/pressrelease/2015-202.html

[3] Ibid

[4] "The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide," Kaspersky Lab, Virus News, February 16, 2015. Access at: http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

[5] "Forewarned is Forearmed, 2015 Cost of Cyber Crime Study: Global," October 2015. Access at: http://www8.hp.com/uk/en/software-solutions/ponemon-cyber-security-report/index.html

[6] "Cyber Security Global Survey," Chartis Research, results to be published Q1 2016.

[7] "The Global Risks report 2015," World Economic Forum. Access at: http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf

[8] "ISO/IEC 27032:2012 Information Technology – Security techniques – Guidelines for cybersecurity," ISO website, online browsing platform. Access at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

[9] Ibid

[10] "Consultative Document on Operational Risk," Basel Committee on Banking Supervision, January 2001. Access at: https://www.bis.org/publ/bcbsca07.pdf

[11] "Review of the Principles for the Sound Management of Operational Risk," Basel Committee on Banking Supervision, October 6, 2014. Access at: http://www.bis.org/publ/bcbs292.pdf

[12] "The Dyre Wolf – Bank Transfer Scam Alert," National Fraud Intelligence Bureau and City of London Police, April 2015. Access at: http://www.fsb.org.uk/docs/default-source/fsb-org-uk/152/assets/april-2015/the-dyre-wolf---bank-transfer-scam-alert.pdf

About the Authors

Steve Culp

Steve is a Senior Managing Director, Accenture Finance & Risk Services. Based in Chicago, Steve has more than 20 years of global experience working with clients to define strategy, and execute change programs across a broad spectrum of risk management and finance disciplines. Steve is responsible for leading the global group across all dimensions, from setting the strategic direction through to the enablement of local teams operating across diverse markets. In addition, he oversees Accenture's efforts on large-scale transformation programs across finance and risk for some of our most important financial services clients.

Prior to his current role he was responsible for our Global Risk Management Practice, and prior to that he led Accenture's Finance & Enterprise Performance consulting services for global banking, insurance and capital markets institutions. With his extensive experience in the financial services industries, combined with his knowledge of risk management and the finance function, he guides executives and client teams on the journey to becoming high-performance businesses.

Chris Thompson

Chris is a Senior Managing Director, Accenture Finance & Risk Services, Capital Markets Lead. Based in New York, Chris specializes in complex, large-scale finance and risk programs. He works with some of the world's leading retail, commercial and investment banks. Chris brings 20 years of broad-based experience in financial architecture, risk management, performance management and trading to organizations determined to become high-performance businesses.

Acknowledgement

The authors would like to thank Peyman Mestchian of Chartis Research for his valuable contribution to this document.

Stay Connected

Accenture Finance & Risk Services
www.accenture.com/financeandrisk

Connect With US
www.linkedin.com/groups?gid=3753715

Join Us
www.facebook.com/accenture

Follow Us
www.twitter.com/accenture

Watch Us
www.youtube.com/accenture

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About Chartis Research

Chartis Research is the leading provider of research and analysis on the global market for risk technology. It is part of Incisive Media which has market leading brands such as Risk and Waters Technology. Chartis's goal is to support enterprises as they drive business performance through better risk management, corporate governance and compliance and to help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of risk technology. Areas of expertise include:

- Credit risk
- Operational risk and governance, risk and compliance (GRC)
- Market risk
- Asset and liability management (ALM) and liquidity risk
- Energy and commodity trading risk
- Financial crime including trader surveillance, anti-fraud and anti-money laundering
- Cyber risk management
- Insurance risk
- Regulatory requirements including Basel 2/3, Dodd-Frank, EMIR and Solvency II

Chartis is solely focused on risk and compliance technology giving it significant advantage over generic market analysts. Chartis has brought together a leading team of analysts and advisors from the risk management and financial services industries. This team has hands-on experience implementing and developing risk management systems and programs for Fortune 500 companies and leading consulting houses. Visit www.chartis-research.com for more information. Join our global online community at www.risktech-forum.com.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of Chartis Research Ltd. The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Chartis Research delivers will be based on information gathered in good faith, whose accuracy we cannot guarantee. Chartis Research accepts no liability whatever for actions taken based on any information that may subsequently prove to be incorrect or errors in our analysis. See Chartis "Terms of Use" on www.chartis-research.com. RiskTech100® is a registered trade mark of Chartis Research Limited. Unauthorized use of Chartis's name and trademarks is strictly prohibited and subject to legal penalties.

15-5280

12460326