www.pwc.com/financialservices

Enhancing business resilience: Transforming cyber risk management through the role of the Chief Risk Officer (CRO)

December 2015

pwc

Contents

Introduction

Business and government leaders gathering at World Economic Forum (WEF) meetings over the last three years have consistently identified cyber attacks as one of the greatest threats to global business and the economy. Recognition of the problem has reached the highest levels of national government including the US, where the President has made repeated statements about the need for heightened surveillance of cyberspace and has issued two executive orders over the past year.[1]

By failing to lead, CROs and risk management teams have allowed cyber to become an intractable issue that now has the potential to cause irreparable damage to entire businesses and reputations.

Yet many financial institutions have been approaching cyber threats as an information technology issue, rather than as the business imperative that it is. Ownership and responsibility for cyber risk management have typically fallen on the IT world, generally the Chief Information Officer (CIO). CIOs, in turn, have delegated this responsibility to a Chief Information Security Officer (CISO) who brings a further IT security focus to this issue. Technologists have therefore been leading the charge against cyber risks for some time, and in doing so they have relied heavily on technology risk management and control frameworks such as ISO 27002 or COBIT. Business lines and supporting operations have often taken little if any ownership of the cyber risks to which they are exposed, delegating the responsibility for managing these risks to IT. At the same time, traditional second line of defence risk management teams have often lacked the technical skills and resources to provide effective oversight over cyber risk management activities and, as a result, cyber risk management frequently remains somewhat disconnected from the broader risk management framework of many organisations. In fact, CROs have often struggled to provide similar effective oversight and credible challenge to what they provide for most other risk domains (e.g. credit, market, compliance and operational).

The problem with this approach is that it fails to highlight or address the pervasive business implications of cyber threats. By failing to lead, CROs and risk management teams have allowed cyber to become an intractable issue that now has the potential to cause irreparable damage to entire businesses and reputations. Very few organisations today are able to quantify and demonstrate the extent of their cyber risk exposure, and risk control mitigation taking place remains largely reactive. In many institutions there is also a lack of meaningful communication about risk exposure to the Board, C-Suite and executive team. In risk management terms, this is the equivalent of running the business without any proper instrumentation or measurement.

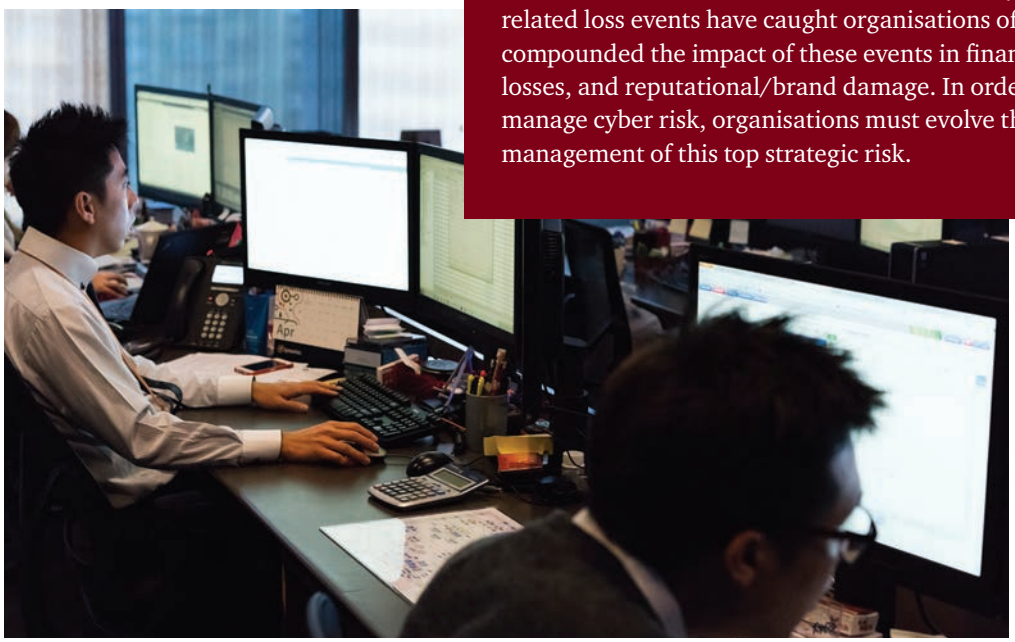
1 For more information on these executive orders and other US actions, see PwC's *A closer look, Cyber: Think risk, not IT* (April 2015).

Our Perspective

It is time for financial institutions to see cyber threats for what they are: strategic enterprise risks that have the potential to severely impact their business. Institutions should focus on becoming more 'cyber resilient'; in other words, able to anticipate, withstand and recover from cyber incidents.[2] For most institutions, this means more than stepping up to the technology challenge – it means 1) reinforcing first line of defence ownership of cyber risk by the business, 2) building an effective second line of defence model for cyber risk management, 3) applying proactive risk management techniques, and 4) relentlessly pursuing a cyber-aware risk culture. CROs will need to be prepared to play an absolutely critical role in driving this transformation in all four areas.

Cyber: Think risk, not IT

Cyber risk management has been treated as a technology problem for many years and predominately owned by the IT function of most organisations. Cyber risk has not been effectively owned by the business and support functions and the CRO has not provided effective oversight and credible challenge similar to most other risk domains (e.g., credit, market, compliance, and operational). This has resulted in a lack of transparency to the Board and senior management of an organisation's current cyber risk profile ratings and key exposures. Many cyber risk management mitigation activities to date have been reactive. As such, cyber attacks and related loss events have caught organisations off guard which has compounded the impact of these events in financial losses, customer losses, and reputational/brand damage. In order to more effectively manage cyber risk, organisations must evolve their governance and management of this top strategic risk.



2 Our definition of cyber resilience is the ability of an organisation to withstand and recover from cyber incidents in line with pre-determined risk tolerance thresholds.

1

Many institutions need to reinforce that the business has first line of defence ownership of cyber risk

CIO and IT functions will, by their nature and their capabilities, always play a critical role in operating cyber risk-related controls and managing cyber risks. Nonetheless, cyber risk management cannot continue to be treated solely as a technology problem that is 'owned' by the IT function. The potential implications of threats and attacks on businesses' ability to reach their objectives are far too devastating in impact. Even if mitigation strategies are currently designed and executed in IT, business leaders cannot delegate their responsibility for owning risks to which their businesses are exposed, and must step into a more active role in the management of cyber risk.

Institutions should appoint an accountable executive for cyber who has appropriate authority over both the business and IT, such as the COO.

Institutions should consider three actions to effectively reinforce first line of defence ownership by the business. First, institutions should appoint an accountable executive for cyber who has appropriate authority over both the business and IT, such as the COO. This will help provide focus and drive consistent prioritisation across the institution.

Second, institutions should strengthen the role and active participation of business leadership in the governance of cyber risk management. Proper cyber risk governance processes should provide visibility to executive management and the Board so that the extent of cyber risk is fully dimensioned and appropriate risk management decision-making is possible. This may require the creation of three key forums, each with distinct and complementary mandates:

- **Cyber Risk Governance Committee:** Responsible for the overall cyber programme, preparedness and response.
- **Cyber Risk Management Committee:** Provides risk decisioning, makes dynamic adjustments to the risk and control posture, and manages cyber risk processes.
- **Cyber Risk Operations Team:** Responsible for collecting and interpreting threat intelligence and making recommendations to the Cyber Risk Management Committee.

Membership of each forum should comprise the business, risk management, and technology. These forums may be incorporated into existing risk committees or established as stand-alone groups – whatever makes the most sense within each organisation. An illustration of a governance model for cyber risk management is provided in Figure A on page 15.

Third, institutions should ensure that cyber risk management figures prominently in the reporting to business line leaders, executive management, and the Board of Directors, just like other important risk exposures. The Committee of Sponsoring Organisations of the Treadway Commission (COSO) and recent regulatory guidance have both emphasised the responsibility of management to provide their Boards with an integrated view of the institution's risk profile. It is hard to conceive how cyber would not be part of that profile for most institutions. The information provided needs to inform management on cyber risk exposures and on their implications from both a business and an IT perspective.

2

Another urgent priority is to build an effective second line of defence for cyber risk management

Building an effective second line of defense for cyber risk management is imperative in those financial institutions where CROs have struggled to provide effective second line of defence oversight and credible challenge, which may result from the lack of skills and resources necessary to understand cyber security practices and techniques.

In today's environment, CROs and their risk management teams need to take a leadership role in building cyber resilience. They need to help articulate the business risks emanating from cyber threats, oversee their mitigation, and provide credible challenge to the cyber risk management practices of the first line of defence – including IT. They also need to assist the first line, by promulgating policies and standards that link the cyber risk management efforts to the institution's overall framework for managing risk. The risk function's oversight and credible challenge should extend to ensuring that the controls implemented in managing cyber risk are indeed in line with the firm's risk tolerance and most likely threat scenarios.

In particular, we believe that the CRO should hold the CIO responsible for providing secure development and maintenance of systems, applications and infrastructure, as well as ongoing monitoring of networks and access. Additionally, CIOs should be tasked with ensuring the reduction of defects and vulnerabilities within their environments, since these are a primary target for cyber threats.

Building out the second line of defence in this manner will 'in many cases' require new skills and resources, yet it is simply bringing the oversight of cyber risk management into line with other important risk domains (e.g. credit, market, compliance and operational).

3

Proactive risk management techniques should be applied to cyber risk in a tailored way

Institutions have too frequently been caught off guard, having to react to cyber events rather than being able to anticipate them effectively. There is no guarantee that applying proactive and forward-looking operational risk management techniques can prevent all such occurrences. However, such techniques could broadly increase the visibility and awareness of cyber risk exposures to the organisation. We see opportunities to do so in three broad areas.

First, explicitly embedding cyber risk management considerations into existing core risk management processes, including:

- Establishment of risk governance and oversight, and cyber risk policies and standards
- Identification of threat sources and determination of risk tolerance
- Consideration of cyber threats when establishing strategic business objectives and approving new products
- Development of risk control mitigation strategies
- Ongoing assessment of risk and monitoring of risk exposure
- Regular and frequent reporting to executive management and the Board
- Design and communication of training and awareness programmes

In particular, CROs should facilitate a discussion with the executive team on the strategic threats that cyber represents to business goals and objectives, and the amount of exposure that the business is willing to accept. Organisations should then document a cyber risk and threat baseline for each area of the business, focusing on identification and prioritisation of business risks and relevant cyber threats. Additionally, organisations should create an inventory of critical business assets that are most at risk. This includes key revenue streams, critical business processes and intellectual property as well as the underlying systems, infrastructure and data that support them.

Leveraging the information obtained from this exercise, the CRO and risk management team should model primary threat scenarios as the basis for further workshops and detailed controls analysis. When organisations understand the level of risk mitigation and control that is needed, the CRO and risk management team should conduct a gap analysis of the existing operating

environment to identify weaknesses, deficiencies and potential areas of exposure. To facilitate this analysis, organisations should leverage industry frameworks (NIST Cybersecurity Framework, SANS Critical Controls, etc.) and regulatory guidance[3] as needed.

Second, enhancing ongoing monitoring and reporting:

An organisation's exposure to cyber threats can change dramatically in a short period of time if they are targeted by an attack. To ensure that dynamic adjustments to the risk and control posture of the organisation can be made, continuous and real-time monitoring of the business risk and cyber threat environment should be performed. A key component of becoming cyber resilient is the ability to consume and act upon cyber threat intelligence, in an operating environment where information about cyber threats is continuously gathered and analysed to determine the amount of risk exposure that exists. This requires a capability to gather and interpret relevant threat data from various internal and external sources.

To ensure that dynamic adjustments to the risk and control posture of the organisation can be made, continuous and real-time monitoring of the business risk and cyber threat environment should be performed.

Unfortunately, the complex structure of many financial services organisations makes it challenging to accomplish this unless it is properly structured and designed. For this reason, the Cyber Risk Operations Team should perform regular analysis of threat data and provide executive business management with their recommendations on relevant actions to be taken, consistent with the threat insights obtained. Risk management teams should develop and maintain cyber risk metrics and provide independent reporting of risk control mitigation and levels of exposure to the executive team. Risk management teams should also be reviewing and challenging cyber risk reporting provided by the first line of defence on a regular basis.

Clearly, without this type of capability it is almost impossible for organisations to know whether they are likely to be targeted and to be proactive in trying to mitigate the cyber threats identified. We therefore recommend that financial services organisations take the following key steps[4]:

- **Establish a cyber threat intelligence capability that is managed and overseen by the Cyber Risk Operations Team:** Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various functional teams together under a common lens to quickly correlate and dynamically adjust the risk posture of the organisation to these threats in real time.
- **Continually gather and analyse cyber threat data, focusing on internal and external insights about threats, vulnerabilities and control posture:** Most threat analysis efforts inhabit a disjointed environment spread across several functions, physical locations and systems. This disjointed nature and lack of common methods to consume intelligence is a significant barrier to establishing a robust cyber risk intelligence capability. To close this deficit, organisations should establish a robust threat analysis capability that is built on shared intelligence, data and research from both internal and external sources.
- **Communicate threat insights and risk exposure to the Cyber Risk Management Committee, which in turn ensures that the necessary risk control decisions are made:** To build a robust cyber intelligence capability, financial institutions should ensure their Cyber Risk Operations Team supports the organisation by correctly analysing cyber risk data, providing leadership with the cyber risk information it needs to make informed decisions, and proactively and quickly responding to attacks.

3 For example, the FFIEC Cybersecurity Assessment Tool can help some organisations assess their level of cybersecurity risk and gauge their ability to respond to cyber incidents.

4 For a further discussion of cyber risk management techniques, see PwC's Viewpoint, Threat smart: Building a cyber resilient financial institution (October 2014).

- **Ensure that decisions regarding adjustments to the risk and control posture are implemented in line with specific threat information and risk control thresholds:** Effective cyber risk monitoring focuses on building a sustainable and resilient approach to putting intelligence inputs from various functional teams together under a common lens to quickly correlate and dynamically adjust the risk posture of the organisation to these threats in real time.

Third, implementing threat playbooks and scenario rehearsals:

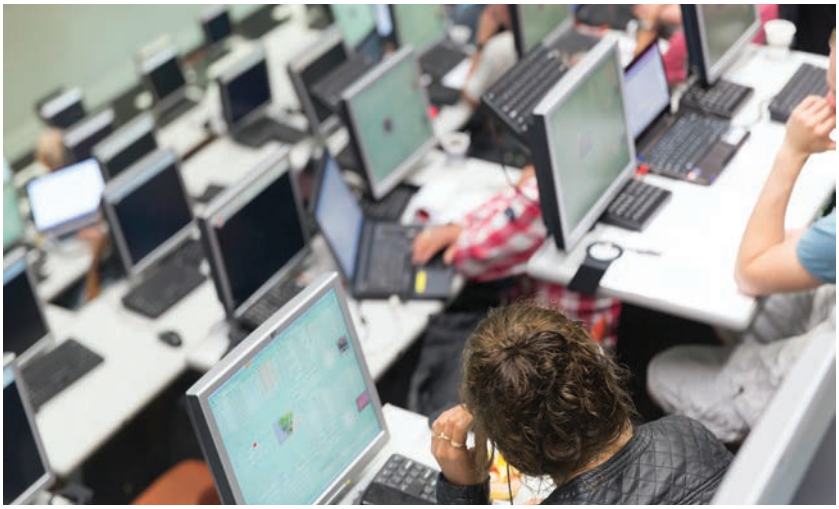
In the context of cyber resiliency, the importance of threat analysis, playbook development and ongoing scenario rehearsal cannot be overemphasised. In our view, they can be the difference between successful mitigation and an unmitigated disaster.

As seen in recent high-profile incidents, the perception that an organisation is ill prepared or poorly informed can severely damage its reputation and shareholder value following a cyber attack. For this reason, threat scenario planning and analysis is a critical step in being prepared, along with documented playbooks where roles are carefully described and rehearsed. The last thing any organisation needs to be seen doing is scrambling in response to a cyber incident in the eyes of the media or security analysts.

We therefore recommend three key steps that risk management teams should follow:

- **Identify cyber threat scenarios:** Consider the full range of scenarios, from the simplest to the most complex. Threat scenario planning should be embedded in enterprise and operational risk management programmes and organisations should ensure that evolving threats are identified on an ongoing basis.
- **Document incident response plans:** The quality of incident management is often the differentiator between a successful outcome and a failure. Clearly define the roles of team members responsible for mitigating and responding to threats. Effective incident management requires participation from numerous business support functions. In addition to IT security, this includes crisis management, business continuity, fraud/ investigations, media relations, corporate affairs etc.
- **Conduct ongoing simulation and rehearsal:** Through practice exercises, rehearse cyber threat scenarios on a periodic basis so that everyone at all levels is familiar with the role they must play during a cyber event.

As seen in recent high-profile incidents, the perception that an organisation is ill prepared or poorly informed can severely damage its reputation and shareholder value following a cyber attack.



4

Finally, many institutions need to relentlessly pursue a cyber-aware risk culture

The blurred lines of accountability between the control functions (which establish governance and process) and the business and key support functions (e.g. IT) need to be clarified. The CRO is responsible to the business leaders for clarifying the types of cyber risk, triggering events and consequential impacts, and for explaining how such risks can be mitigated through proactive planning and embedded into the risk culture framework. Typically, risk culture programmes start with inputs such as the firm's overall risk appetite, and subsequently address dimensions that span leadership, governance and organisation, communications, talent management, systems and data and global operating norms.[5] Although institutions should aspire to have every leader and employee taking ownership of new and emerging risk areas such as cyber, the CRO in collaboration with other executive leaders should focus on some initial activities to start setting the tone for its cyber risk culture.

These activities include:

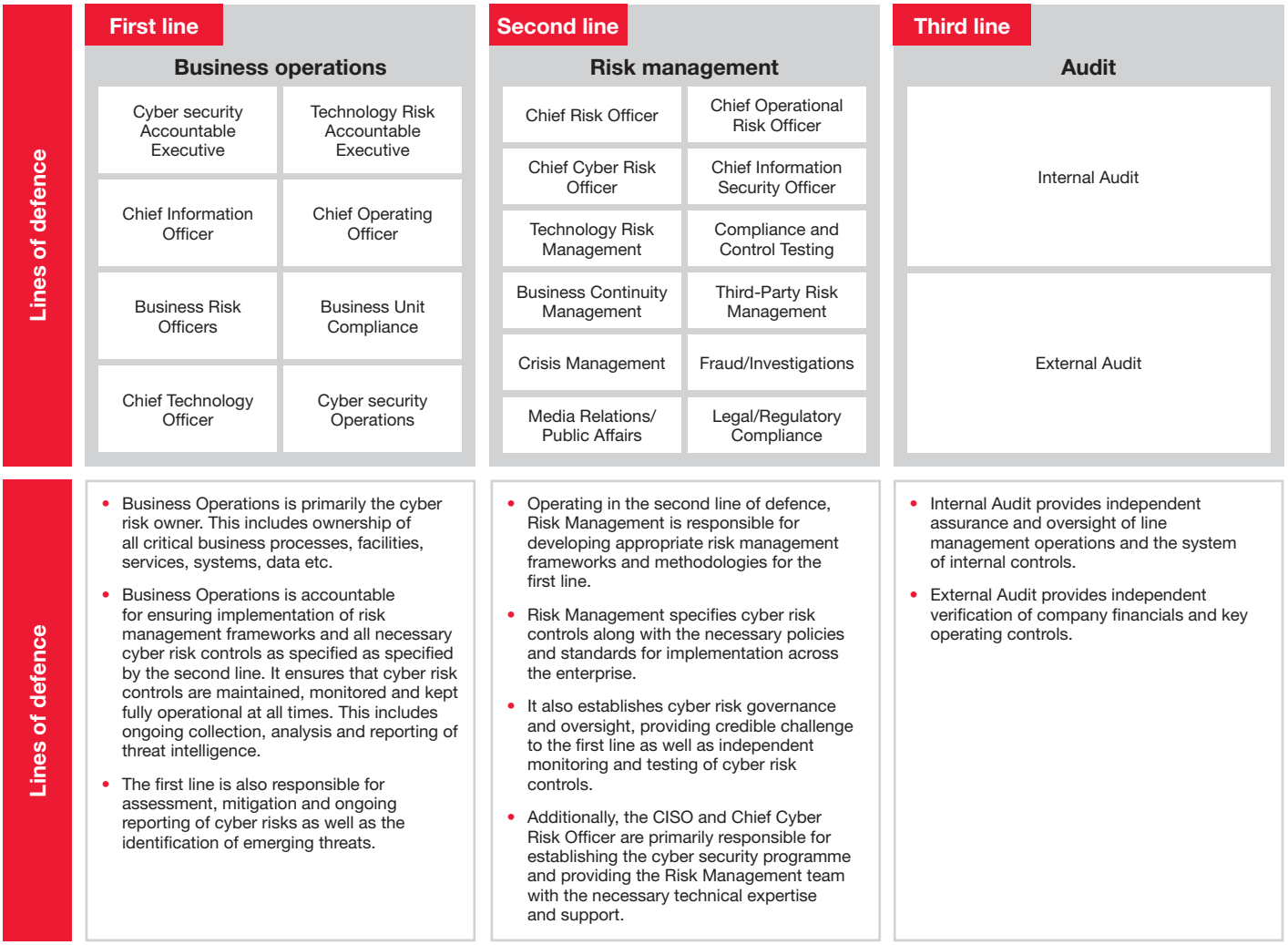
- **Obtain cultural information from leadership and team members pertaining to cyber risk:** To better inform the challenge and effectively evolve the overall cyber risk management programme, it is important to understand the current culture related to this topic. Various methods such as interviews, surveys and focus groups may be used to better inform executive leadership of key challenges, behaviours and areas of focus related to cyber risk management.
- **Communicate the cyber risk management vision to the organisation:** Establish a communication strategy and plan which should be delivered by the key leaders and appropriate business unit leaders to provide transparency regarding the overall vision, demonstrate the organisation's commitment and heighten awareness of cyber risk management.
- **Provide targeted training to the organisation:** It is extremely important with any organisational change to both clarify roles and responsibilities and provide tailored training programmes for each business unit and support function. Key policies and procedures should be codified and referenced during trainings.
- **Consider adjusting incentives to change behaviours:** Based upon the status of an organisation's overall culture, incentives and rewards may need to be adjusted to align with an organisation's strategy and objectives related to cyber risk management. This may include incentives for select leaders coupled with organisation-wide performance objectives and requirements. CROs and other executives should work with the Chief Human Capital Officer to ensure appropriate alignment of incentives.

5 For a further discussion of risk culture, see PwC's Viewpoint, Cure for the common culture: How to build a healthy risk culture (October 2014).

Conclusion

The threat from cyber attacks has become an intractable issue that too often continues to be treated as a technology problem. Addressing the issue more effectively will require financial institutions to effect a number of important changes: reinforcing first line of defence ownership of cyber risk by the business, building an effective second line of defence model for cyber risk management, applying proactive risk management techniques, and relentlessly pursuing a cyber-aware risk culture. CROs will need to be prepared to play a critical role in driving this transformation in all four areas. An important first step that CROs should take is to critically evaluate their risk management team to ensure that they have the skills and resources necessary for effective cyber risk management policy setting and oversight.

Figure A: Cyber Risk Management and Three Lines of Defence



Contacts

Julien Courbe
PwC US
julien.courbe@us.pwc.com
+1 646 471 4771

Dominic Nixon
PwC Singapore
+65 6236 3188
dominic.nixon@sg.pwc.com

Joseph Nocera
PwC US
joseph.nocera@us.pwc.com
+1 312 298 2745

Dietmar Serbee
PwC US
+1 646 471 7270
dietmar.d.serbee@us.pwc.com

George Stylianides
PwC UK
george.e.stylianides@uk.pwc.com
+44 (0) 20 7804 3364

www.pwc.com/financialservices