The evolving role of the CISO

August 2016
By Leathwaite

‘Arguably no role has evolved as rapidly over the past 18 months as the chief information security officer (CISO).’

“What does Information Security mean to you?”

an expert panel discussion
register now for this event
Hosted by Leathwaite
PLUS - LATEST CISO MARKET MOVES
See inside for details
The Financial Services sector remains under the regulatory spotlight, and as cost pressures mount, banks find themselves building an increasing reliance on data.

Sadly, the more data they store away in remote servers located all over the world, the greater the information risk.

Couple this with the global trend of digitisation amongst banks, the growing sophistication of criminal groups, the increasing frequency of cyber-attacks and the continued focus on data protection due to employees enjoying remote access, cyber-risk to these organisations has never been so prevalent.

The heightened awareness and sensitivities borne out of the current financial services landscape means we are seeing banks embrace a more collaborative and collegiate approach to how they structure their information security and cyber risk functions.

Leaders are also rethinking the roles of those individuals leading these practices today, their remit and their reporting lines.

How has the CISO role changed?

As information security is present on every board agenda within the banking industry, arguably no role has evolved as rapidly over the past 18 months as the chief information security officer (CISO).

Between late 2014 and early 2016, a staggering 11 of the 18 large banks regulated by the OCC, the primary regulator of US retail banks, changed their information security leader. All but two of the world’s top investment banks have made similar changes.

Of the 11 large retail banks with a new security leader, six were external hires. In other words, over 50% of banks felt they did not have the skills internally to lead cyber and information security in today’s environment.

Of the remaining banks, virtually all have still undergone significant changes to their information security organisation: restructuring or replacing the team underneath the information security leader, reorganising the security functions that sit in risk or IT organisations or changing the chief information security officer’s reporting line.

The primary driving factor behind the rapid evolution of the CISO function is that the role has changed. The skills required to be a CISO in banking today go beyond having the necessary training and certifications to perform vulnerability assessments, configure firewalls and monitor networks.

Today’s CISO role is an executive position that requires the same strategic vision and executive leadership skills as anyone else in the C-suite, requiring greater emphasis on; influence, risk management, strategic prioritisation, board-level communication, financial management, and business acumen.

Although CEOs have stated they have an unlimited budget for cyber security, the savviest information security leaders understand the
need to demonstrate the business value they bring to the firm’s bottom line.

Financial firms are also wrestling with the organisational operating model for cyber security and IT risk functions.

What is considered “first line of defence” versus “second line”? How can information security maintain independence from IT whilst still giving security leadership the resources they need to protect the firm’s information assets? Does information security need to report into the risk organisation rather than IT?

The result of these questions is that no two information security programs are identical.

However, we have observed that several trends are beginning to emerge.

To whom does the CISO report?

Clear lines of accountability still exist between the first and second lines of defence, with respective responsibilities aligning to technology versus risk. However the most notable shift is how the CISO role is positioned and the level at which it sits.

As with many emerging roles, how best to position them within organisational structures shifts over time. We have observed similar shifts in other areas such as Digital, where because the initial view is that it is a ‘technology issue’ accountability sits with the CIO.

However, as the significance of the function evolves and the business adds more emphasis on the function in its own right, we have seen how these divisions can fragment.

Having emerged from a position entrenchment in the technology reporting structure, often aligned within the infrastructure organisation, the CISO role has risen through the ranks.

Increasingly CISOs are reporting directly to the CIO, or higher.

The debate remains as to whether technology alignment is appropriate and should instead be made a peer to the CIO to ensure checks and balances. To that end, some firms have aligned their CISO into the COO, or even the CRO if they define the role as purely an oversight function.

The result is a lack of consistent reporting structures between businesses.

Of the top 10 global banks by investment banking revenues:

- Four CISOs report to a CIO/CTO
- Four report to a COO/head of operations and technology
- Two report into risk management

Regulators want to see independence from IT, which many interpret to mean that the CISO should report into risk or an alternative function.

Often that is the case, and we have witnessed that this is often the preference of medium-sized financial firms including regional banks, CCPs and retail brokerage businesses. The CISO’s role in these firms is often strictly defined as policy and governance, testing, monitoring and reporting, particularly in companies with an influential risk management team.

There are still instances, however, of information security organisations reporting into risk that still have operational and engineering
The evolving role of the CISO: (continued)

responsibilities otherwise considered ‘first line of defence’. This is also the case at one of the largest global banks.

However, of the remaining top 10 global banks, the CISO title has usually remained within the technology & operations function. As these firms have multiple CIOs across very large individual businesses, they feel that information security can maintain independence from business-aligned CIOs. They also prefer their CISO to have direct oversight by a tech-savvy executive that has end-to-end responsibility of the firm’s technology.

Therefore CISOs reporting to risk management are the exception rather than the rule at the world’s largest financial institutions. Moreover, at one of the two global banks with their CISO in the risk organisation, the CISO’s role is a relatively thin policy/oversight role two levels removed from the CRO. Much of the influence remains in IT, although without the CISO title.

Where the CISO reports to the CIO, independent oversight from the risk organisation tends to come in the form of information risk management oversight, an extension of operational or enterprise risk management.

The people staffing these roles are having to become increasingly technical to provide the effective challenge to ‘test’ the robustness and resiliency of the CISO organisation. However they also need to be well rounded communicators capable of articulating technical issues to a CRO who invariably lacks technical understanding of IT issues, but is in a position to influence strategy given they report directly to CEOs and sit on Management Boards.

It appears culture and people also have key roles to play. If the CRO ‘trusts’ the effectiveness of the CIO/CISO function, they won’t feel the need to take on direct management of information security, but rather have someone technical on their staff who can work in partnership with the CIO function to ensure controls are aligned to industry best practice and firm wide risk and control standards.

How are information security and IT risk functions structured?

It’s no secret that the role of the CISO can differ from company to company both in size of role and responsibility. Consequently, information and cyber security functions can hugely vary depending on how the firm is structured and what type of individuals they have in these sorts of roles.

But regardless of there being structural differences across the market one thing remains consistent across all organisations. To have a truly coherent, collaborative and effective information security function and strategy, your technology and risk management functions must be aligned in their thinking and approach.

It is less about ‘who owns what’ and more about ‘how firms best achieve a robust and best in class information security function,’ that has buy-in and support from the business, the board, and is effective across the entire organisation.

The relationship between first line and second line has and will continue to evolve over time.

Whether risk management is more focused on
risk assessments, vulnerability assessments and deep dives, whilst technology is focused on the more technical aspects of IT security, collaboration across functions must be encouraged and independent challenge has to be present.

**Conclusion**

As the cyber security threats continue to evolve and become increasingly prevalent in a world that is ever more digitally focused, the CISO role will continue to grow in significance and complexity.

With this shift in construct and firm wide visibility, the profile of the CISO is mirroring this change.

Whether reporting to the CIO, COO, CRO or elsewhere, we can expect it to differ from organisation to organisation for a few years yet.

Until we reach a stage when the maturity of the information security functions and broader understanding of the issues in this space has improved, we can anticipate that firms will continue to wrestle with the alignment of accountability of defending themselves from cyber-attacks and data breaches.
2016 CISO Market Moves:

Martin Roberts joined Henderson as CISO, having previously been Information Risk Manager for Virgin Atlantic.

Symantec’s Cheri McGuire named CISO of Standard Chartered bank.

Lynn Miller joined AXA as UK & US CISO, who had previously been a security consultant.

Jeanette Hanna-Ruiz has joined NASA as CIO for IT security, joining from Microsoft.

John McClurg, Dell’s CISO has joined Cylance (cybersecurity products and services company).

Adrian Asher joins the London Stock Exchange as CISO, previously group CISO for HSBC.

Simon Jenner joins Booking.com as CISO, from JPMorgan where he had been CIB CISO.

Thien La joined Wellmark Blue Cross Blue Shield as CISO.

Max Caceres is joining PDT Partners in July as CSO and head of infrastructure, from Arcesium.

Lin Lu, Americas CISO for Deutsche Bank, is joining Freddie Mac as CRO for IT and information security, reporting to the CRO.

Amex’s Former Chief Privacy Officer Andy Roth moves from Dentons to Cooley to help build out their Privacy and Data Protection Practice.

Reto Haeni joined PwC from Microsoft as Switzerland Head of Cyber Security, Partner.

Vishal Salvi joins Infosys as CISO, joining from PwC.

Brian DiPietro joined MUFG Union Bank as CISO, from JPMC.

Lisa Humbert joins MUFG Union Bank as chief IT risk officer, from BNY Mellon where she held the same role.

Tom Killelea, former CISO of Amazon, has been appointed to Capital One’s board of directors.

Steven Harvey joined Santander Consumer as CISO, from HSBC where he was the North America CISO.

Anthony Johnson joined JPMorgan Chase as Corporate and Investment Bank CISO, from Fannie Mae where he was CISO.

Douglas DeGrote joins Allianz Life as CISO, from Xcel Energy.

Andrew Turner joined Vantiv as CSO, previously the SVP of cyber security for Visa.

Bill Walker joins Mortgage Guaranty Insurance Company as CISO, from US Bank.

Royal Hansen joins American Express as the CISO, from Goldman Sachs.

Devon Bryant joins the Federal Reserve Bank as CISO, from ADP.

George Stathakopoulos joins Apple to oversee its corporate digital defenses, from Amazon where he was vice president of information security.

Al Tarasiuk has been appointed CISO of Deutsche Bank, an internal appointment following the departure of Rolf Riemenschnitter.

Gary Warzala joins Fifth Third as the CISO, from PNC.

Morian Eberhard has joined Zions Bank as CISO, from MUFG Union Bank where he was deputy CISO.

John Holland joins PNC Bank as Chief Technology Risk Officer, from Credit Suisse.

Jim Motes joined Kohler Co as VP Information Security from Rockwell Automation where he was CISO.