The state of cybersecurity at financial institutions

There's no "one-size-fits-all" approach

Measuring what "good" looks like when it comes to cybersecurity at financial services companies is difficult at a time when shifting business priorities and exponential technology forces are changing how many organisations approach their management of cyber risks.

Jim Eckenrode
Managing Director
Deloitte Center for Financial Services

Sam Friedman
Insurance Research Leader
Deloitte Center for Financial Services

A recent Deloitte study surveyed chief information security officers (CISOs) from over 50 companies about how they are discharging their responsibilities in protecting the digital fortresses at banks, investment management firms, insurance companies, and other financial services institutions (FSIs).[1] While the findings may not represent the full diversity of practices in the industry due to the small sample size, learning from the experience of peers can help FSIs avoid having to reinvent the wheel in efforts to protect their people and systems against the latest cyber threats.

Overall, the study found organisations are working within a broad spectrum of cybersecurity strategies, structures, and budget priorities. The findings suggest that clear differences exist within the industry based on company size, maturity level, and even ownership structure.

While it's important to have an adequate budget for cybersecurity, how a program is organised and governed may be equally if not more impactful than how much is spent relative to a company's overall IT budget or revenue. Indeed, many companies with below average cybersecurity budget allocations managed to achieve a high program maturity level, while some that had higher than average spending were actually less advanced. This dynamic could, in part, reflect the challenges larger, more complex global organisations often face in advancing capabilities versus their smaller counterparts.

If money is not the sole criterion of cybersecurity effectiveness, what factors differentiated the risk management approaches and practices of adaptive respondents from their lower maturity level counterparts? Here are a few observations:

Accountability starts at the top.
Almost all board and management committee members at responding companies were keenly interested in their company's overall cybersecurity strategy. However, those from adaptive companies suggest their boards are more likely to delve into the details of the cybersecurity budget, specific operational roles and responsibilities, as well as the program's general progress than are boards of less advanced peer companies. Respondents from informed companies (see image below), which fall two tiers below adaptive on the maturity scale, reported their boards were typically significantly less interested in reviewing current threats, program progress, and security testing results.

Cybersecurity maturity levels

Partial
Organisational cybersecurity risk managment practices are not formalised, and risk is managed in an ad-hoc and sometimes reactive manner.

Repeatable
The organisation's risk management practices are formally approved and expressed as policy.

Informed
Risk management practice are approved by management but may not be established as an organisation-wide policy.

Adaptive
The organisation adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.

Source: NIST framework as decribed in the FS-ISAC / Deloitte Cyber Risk Services CSO Survey.

1. The survey upon which this article is based was fielded by the Financial Services Information Sharing and Analysis Center (FS-ISAC), in conjunction with Deloitte's Cyber Risk Services practice.

Shared responsibilities make a difference.
More than one-half to three-quarters of respondents, depending on the sector, had a fully centralised cybersecurity function. Among the respondents from the largest participating companies, two-thirds reported a centralised approach. However, respondents from adaptive companies were more likely to favour a hybrid approach—featuring centralised functions, but with each business unit and/or region given strategy and execution capabilities and coordinating with one another.

Multiple lines of defence are maintained.
Most respondents from adaptive firms said their organisations tended to have two separate, independent lines of cyber defence—the first involving security at front line units, and the second being organisation-wide cyber risk management operations.

Cyber risk exposure is distributed.
Nearly one-half of respondents at the informed maturity level said their organisations did not buy any insurance to specifically cover cyber risks. In contrast, two-thirds of those from adaptive companies said their organisations had purchased adequate cyber insurance to cover almost all expected loss scenarios, while one-quarter had insurance to cover at least one-half of their anticipated exposure.

Outside support is sought.
Respondents from companies with less mature security programs were more likely to externally source their cybersecurity functions or personnel than were adaptive companies. However, across the board, the most prevalent outside source of help was with "red team" operations, in which a company tests its preparedness to be secure, vigilant, and resilient given the threat of a cyberattack.

FSIs may not be allocating enough resources.
For the largest FSI companies, analysis of available survey data seems to suggest that their cyber risk management budgets can range anywhere from 5 percent to 20 percent of the total IT budget, with a mean of about 12 percent. One-half of the large FSI companies reported that cyber risk management spending was $20 million or less. Given the potential operational disruption, reputational damage, investigation and customer costs, and remediation expenses that could emerge from a single successful breach, this may not be enough.

Type of ownership makes a difference.
Publicly held FSI companies responding were likely to spend more than their privately owned counterparts for cybersecurity. Among large public FSI companies, about one-third had a budget in the $4 million to $20 million range. This contrasts with respondents from large private FSIs, nearly all of whom indicated that their cybersecurity budgets were in the $4 million to $20 million category. This dynamic likely reflects concerns at public financial institutions over a potential multiplier effect from a high-profile breach, which could roil shareholders and analysts as well as undermine market capitalisation.

Meat and potatoes over dessert.
Survey respondents spent more than two-thirds of their cybersecurity budgets on operational activities, vs. less than one-third on transformational initiatives, with cyber monitoring and operations taking up the biggest share of budget and staff allocations. By size, respondents from large companies indicated that less than one-third of their cyber risk management budgets was allocated to transformational initiatives, while those from midsize and smaller companies reported allocating only around one-quarter of budgets to transformation. Although the way respondents defined "operational" vs. "transformational" may be partly responsible here, our survey sample seems to suggest that spending on cyber risk management may need to pivot to keep up with the level of spending on innovation by the business overall.

CISO reporting relationships vary.
More than one-half of CISOs responding from smaller companies reported directly to the chief executive officer, which likely reflects a flatter organisational structure. At the largest responding companies, the CISO was more likely to report to the chief information officer (CIO), chief operating officer, or chief risk officer (CRO). Half of the midsize respondents said their CISO reports to the CRO.

Innovation is a top priority.
Respondents rated mobile, cloud, and data/analytics as the top-three priorities for adoption at their companies in the next two years, while embedding cyber defences into these new digital initiatives took top rank as the most important business issue with security implications. When it comes to new investments, innovation and emerging technology are top-of-mind for CISOs, with cloud, data and analytics, and social media topping the list of technology items that warrant attention at the large firms.

"The financial services industry in Ireland is facing an ever increasing volume of regulations. Currently we have GDPR, NISD, PSD2 with TIBER following up closely behind. While compliance with regulations is important, organisations should not presume that being compliant is being secure."

Jacky Fox,
Director, Cyber,
Deloitte Ireland LLP

Where might FSIs go from here?

While this survey represents a small sample of the financial services community, the results nevertheless indicate steps companies can consider as they continue to upgrade their cybersecurity capabilities and maturity level. As a whole, companies should keep raising their game to stay on top of evolving cyber exposures while enabling secure innovation. To help improve the balance between risk and innovation, financial institutions should consider the following actions:

Proactively engage the board.
Provide board members with the details of how management is addressing this critical exposure. Heightened attention will likely not only keep top management more focused on perfecting their approach and improving metrics, but such high-level scrutiny should also resonate throughout the organisation.

Engage the entire organisation in cybersecurity.
With so few full-time employees devoted to cybersecurity, everyone in the organisation should understand and embrace their vital role and responsibilities in detecting intrusions, reporting red flags, and maintaining good security hygiene to help prevent events from happening in the first place and limit the damage if they do occur.

Provide multiple lines of defence.
Companies should aim to embed cybersecurity practices and personnel within business units and regional offices to support the central cyber risk management team. As it should be everyone's job to manage cyber risk, make sure awareness and duties permeate the organisation, and share accountability.

Alter the mix of a CISO's responsibilities.
Last but not least, to do their jobs effectively, CISOs should be reporting beyond the CIO and regularly interact outside the IT department. Most CISOs already wear a number of hats, but unfortunately many are often focused on their traditional roles as technologists and guardians. As the job has become more complex, however, they should strive to spend two-thirds of their time as strategists and advisors to better support their management teams and boards.[2]

2. Deloitte Cyber Risk Services CISO Transition Lab analysis, Deloitte Financial Advisory Services LLP.

The four faces of the CISO

Chief information security officer
Secure | Vigilant | Resilient

Strategist
Drive business and cyber risk strategy alignment, innovate, and instigate transitional change to manage risk through valued investment.

Current	15%
Desired	32%

Guardian
Protect business by understanding the threat landscape and managing the effectiveness of the cyber risk programme.

Current	41%
Desired	12%

Advisor
Integrate with the business to educate, advise, and influence activities with cyber risk implications.

Current	12%
Desired	35%

Technologist
Assess and implement security technologies and standards to build organisational capabilities.

Current	33%
Desired	12%

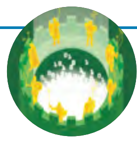
Note: Through research conducted at Deloitte's CISO Lab sessions, a divergence was discovered in the time spent in each of the four roles CISOs are performing vs. what is likely to be a more desirable allocation of responsibilities in a world of evolving cyber risks. As indicated above, CISOs should move more into strategic and advisory roles, rather than spend the bulk of their time, as they are likely to be currently, as guardians and technologists.

SourceL Khalid Kark, Monique Francois, and Taryn Aguas, 'The new CISO: Leading the strategic security organization," Deloitte Review 19, July 25, 2016.

Getting to the next level on cybersecurity.
As cybersecurity is expected to continue to be an integral function for financial institutions, improving capabilities will likely be an ongoing challenge as threats keep evolving in scope, technique, and sophistication. FSIs should keep adapting to stay one step ahead of threat actors that intend to do them harm.

While benchmarks can help financial institutions assess their readiness to handle cyber risk, remaining secure, vigilant, and resilient also likely requires the industry to look beyond its own experiences and continue working with broader communities facing the same threats. At a minimum, financial institutions should closely follow cyber war stories to learn from the experience of peers. This could help FSIs avoid having to reinvent the wheel in efforts to protect their people and systems against the latest cyber threats.

This article is sourced from
The state of cybersecurity at financial institutions
Deloitte.com/Insights



Irish Financial Services Partner Team

David Dalton
Financial Services Lead
Deloitte Ireland LLP
ddalton@deloitte.ie
+353 1 407 4801

Petri Heinonen
Banking Lead
Consulting
peheinonen@deloitte.ie
+353 1 417 2225

Donal Lehane
Insurance Lead
Consulting
dlehane@deloitte.ie
+353 1 417 2807

Brian Forrester
Investment Management Lead
Audit and Assurance
bforrester@deloitte.ie
+353 1 417 2614

Michael Flynn
Real Estate Lead
Financial Advisory
micflynn@deloitte.ie
+353 1 417 2515

Pieter Burger
Aviation Finance Lead
Tax and Legal
piburger@deloitte.ie
+353 1 417 2446

Gerry Fitzpatrick
Banking
Audit and Assurance
gfitzpatrick@deloitte.ie
+353 1 417 2645

David Reynolds
Banking
Consulting
davidreynolds@deloitte.ie
+353 1 417 5729

John McCarroll
Banking
Audit and Assurance
jmccarroll@deloitte.ie
+353 1 417 2533

Sean Smith
Banking
Risk Advisory
seansmith1@deloitte.ie
+353 1 417 2306

David Kinsella
Banking
Risk Advisory
davkinsella@deloitte.ie
+353 1 417 2529

Sinead Moore
Banking
Audit and Assurance
simoore@deloitte.ie
+353 1 417 2979

Ciara Regan
Insurance
Audit and Assurance
cregan@deloitte.ie
+353 1 407 4856

Conor Hynes
Insurance
Tax and Legal
chynes@deloitte.ie
+353 1 417 2205

Glenn Gillard
Insurance
Audit and Assurance
ggillard@deloitte.ie
+353 1 417 2802

Eimear McCarthy
Insurance
Audit and Assurance
emccarthy@deloitte.ie
+353 1 417 2685

Matthew Foley
Investment Management
Audit and Assurance
mfoley@deloitte.ie
+353 1 417 3861

Darren Griffin
Investment Management
Audit and Assurance
dagriffin@deloitte.ie
+353 1 417 2376

Niamh Geraghty
Investment Management
Audit and Assurance
ngeraghty@deloitte.ie
+353 1 417 2649

Brian Jackson
Investment Management
Audit and Assurance
brijackson@deloitte.ie
+353 1 417 2975

Christian MacManus
Investment Management
Audit and Assurance
chmacmanus@deloitte.ie
+353 1 417 8567

Michael Hartwell
Head of Audit
Audit and Assurance
mhartwell@deloitte.ie
+353 1 417 2303

Colm McDonnell
Head of Risk Advisory
cmcdonnell@deloitte.ie
+353 1 417 2348

Brian O'Callaghan
Aviation Finance
Audit and Assurance
bocallaghan@deloitte.ie
+353 1 417 2475

Deirdre Power
Head of Financial Services Tax
Tax and Legal
depower@deloitte.ie
+353 1 417 2448

Padraic Whelan
Real Estate
Tax and Legal
pwhelan@deloitte.ie
+353 1 417 2848

Martin Reilly
Head of Financial Advisory
mreilly@deloitte.ie
+353 1 417 2212

Daniel Gaffney
Digital Finance
Consulting
dgaffney@deloitte.ie
+353 1 417 2349

David Conway
Deloitte Digital
Consulting
daconway@deloitte.ie
+353 1 417 2853

Valarie Daunt
Human Capital
Consulting
vdaunt@deloitte.ie
+353 1 417 8633

Deloitte.