How do you know you're investing in the right cyber risk strategies?

EY
Building a better working world

The better the question. The better the answer.
The better the world works.

Across Asia Pacific, financial institutions are making million-dollar cyber investment decisions to mitigate threats. Such investment decisions need to rely on facts and insights to deliver the right return on investment: where threats are mitigated effectively and institutions return to their target risk appetite. We need a fact-based and structured approach to help Asia Pacific banks, insurers and asset managers achieve this.

As more regulators require businesses to take a structured approach to managing cyber risk, few financial institutions can demonstrate they are investing in the right cyber risk mitigation strategies.

Ever since cyber threats arrived on financial institutions' risk registers, boards and management have been making mitigation decisions based on the collective experiences of internal security experts and external consultants. But this doesn't necessarily align to the structured approach required by regulators. Financial institutions are now expected to approach cyber risk decisions in a similar manner to the way they would other risk domains, such as credit risk.

The current approach sometimes results in a false sense of security, where boards may mistake action for effective protection, where managers rest easy because "we're using the latest technologies," and where strategies are considered successful if an institution simply avoids being "the slowest gazelle in the herd".

A quick comparison with the strictly quantified procedures for allocating capital investment illustrates the dangers involved in continuing with this approach.

If institutions cannot quantify the value at risk from a cyber threat and the quantum a particular set of cyber control investments will deliver, how can they meaningfully decide how much to invest and where? How do they know cyber investments are properly focused on their critical assets to mitigate their key threats?

Key actions

- Develop a top-down model to quantify cyber risk, enabling board and management to understand its quantifiable impacts
- Define metrics and risk indicators that measure the effectiveness and coverage of controls on your key assets
- Connect an integrate data sources to provide the facts to support these metrics
- Automate data collection and use analytics tools to generate and communicate cyber risk insights via dashboards that support the range of views required by various stakeholders, including: executives, board and control owners

Key outcomes

- Understand how resilient you are to defend against your key cyber threats
- Identify how much a major cyber incident could cost, how much to spend and how much this will buy down risk
- Improve prioritization by recognizing when further investment provides diminishing returns
- Better forecast when you will return to risk appetite

Do you have an aggregated view to answer the burning questions of the board, senior management, business and functional managers, service providers, control owners, and risk and compliance teams?

- How do we quantify the financial, reputational and customer impacts of a cyber attack?
- How does cyber risk roll up into broader operational risk?
- How are we protecting our critical assets in each business function?
- Are our security initiatives enabling business capabilities and improving our overall security posture?
- How effective are our controls?
- Is the money spent on cyber security helping reduce value at risk?
- Is our investment focused correctly?
- Where can we invest to drive the best risk reduction?

How can we provide the board and senior management with the facts on cyber risk?

We must stop calculating cyber risk metrics based only on things we "can" measure (data from key control systems) and get a handle on what we "should" be measuring (threat scenarios and the value at risk).

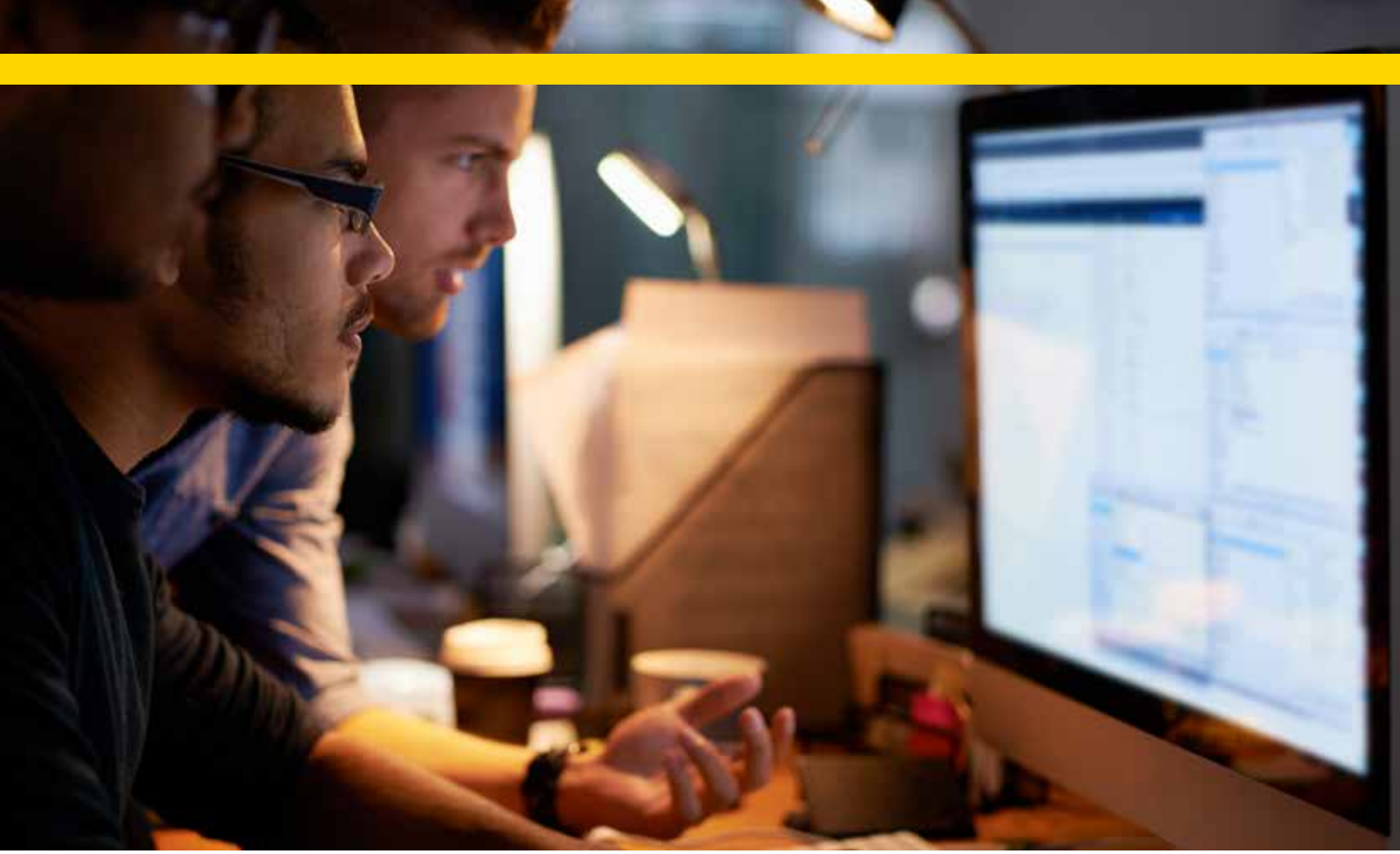
To do this, institutions need a structured, integrated approach to capturing and measuring the facts needed to make risk-based decisions. This requires aggregating metrics and mapping cyber threats across the value chain to quantify their likely business and financial impacts.

Three steps to fact-based cyber risk decisions

1. **Model — Improve cyber understanding of the business value chain**

To measure cyber risk, institutions must define metrics and cyber risk indicators by:

- Breaking down cyber risk scenarios into modular cyber events mapping them to the threat and attack lifecycle (e.g., cyber kill chain), including the critical respond and recover actions
- For each step in the attack chain, identifying key controls in place to mitigate these actions
- Defining metrics and risk indicators that measure the effectiveness of these controls
- Leveraging the critical information asset register and measuring the coverage of these key controls across critical information assets
- Developing a structured model for how each control contributes to mitigating the threat (resilience or protective index)



2. Quantify — Translate cyber risks into business outcomes

To provide management with the information and insights to enable effective and high-quality risk management, cyber risks must be quantified using a range of lenses, including at an aggregate organizational and more granular business unit level.

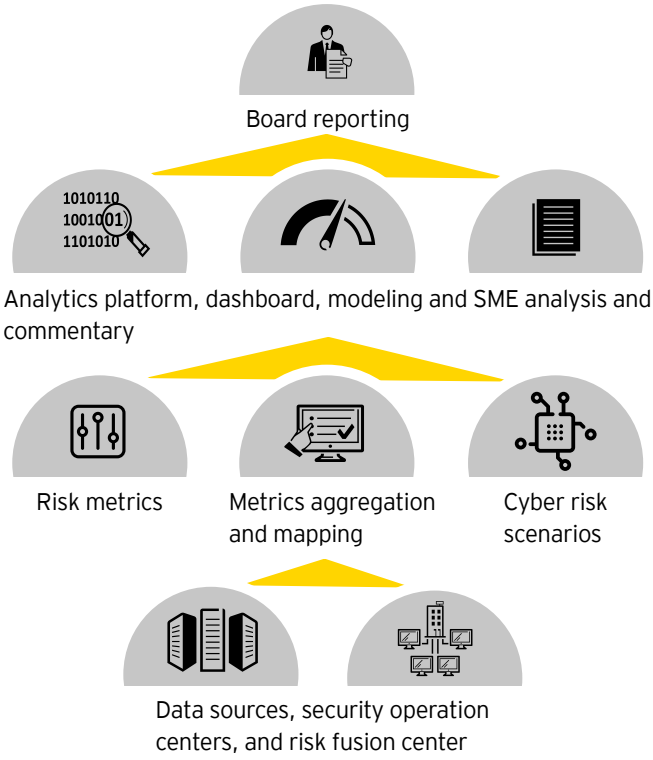
By leveraging best practice in operational risk modeling, measures of resilience and their uplift can be translated in business terms, such as Value at Risk. This supports executives and boards to have a tangible "dollars and cents" discussion. Once directors know that a particular cyber threat is putting US$250m of value at risk, they have a much greater likelihood of deciding on an appropriate control action.

3. Communicate — Answer the question: "Are we investing enough in cyber?"

Modelling and quantifying cyber risk generates significant amounts of data, which stakeholders struggle to make sense of. Boards and executives need dashboards that provide real-time insights from aggregated risk, control and business unit views.

Dashboards and other cyber risk reports are vital decision support tools. They help inform discussions about cyber risk, including identifying which risks to avoid, which to accept, which to transfer through insurance and which to mitigate by investing in specific control uplift.

This approach provides a structured method to measure an institution's ability to defend against attacks. It also allows risk committees to forecast a return to appetite from the uplift program. Boards can identify which controls will deliver the greatest return on investment, allowing investment to be prioritized.



Without a structured, rigorous and data-led approach we will continue to make million dollar investments based on opinions – not facts.

We can and must improve our ability to support senior executive and the board in managing an institution's cyber risk.

We need to move from relying on opinion to using more quantified data to drive decision making.

We need to recognize we can model cyber threats via structured scenarios and their associated controls to mitigate these threats.

We must understand these models need to take account of both control effectiveness and coverage across the institution's key assets.

We must embrace the data aggregation challenge and make appropriate investments in technology to support this.

Contacts

Australia

Anthony Robinson
Partner, Financial Services
Anthony.Robinson@au.ey.com
+61 2 9248 5975

Hong Kong

Jeremy Pizzala
Partner, Financial Services
Jeremy.Pizzala@hk.ey.com
+852 2846 9085

Simon Chandran
Executive Director, Financial Services
Simon.Chandran@hk.ey.com
+852 2846 9888

Singapore

Sean Gunasekera
Executive Director, Financial Services
Sean.Gunasekera@sg.ey.com
+65 6718 1162

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 000279-19Gbl

ey.com