Toolkit C

Board-Level Cybersecurity Metrics

Which cybersecurity metrics should be included in a board-level briefing? This question is deceptively simple. Similar to virtually every other division and function within the organisation, the cybersecurity function collects and analyses a tremendous volume of data and there is little consensus on which are the critical few pieces of data that should be shared with a board audience. Adding to the challenge is the fact that cybersecurity is a relatively new domain, with standards and benchmarks that are still developing or evolving.

Ultimately, directors will need to ask members of management to define the cybersecurity information, metrics, and other data that is most relevant to them given the organisation's operating environment – including industry or sector, regulatory requirements, geographic footprint, and so on. More often than not, boards see a high volume of operational metrics which provide very little strategic insight on the state of the organisation's cybersecurity programme. Metrics that are typically presented include statistics such as "number of blocked attacks," "number of unpatched vulnerabilities," and other stand-alone, compliance-oriented measures, that provide little strategic context about the organisation's performance and risk position.

As a starting point, directors can apply the same general principles used for other types of Board-level metrics to cybersecurity-related reporting.

The following recommendations provide a starting point for the types of cybersecurity metrics that board members should consider requesting from management.

1. Have we developed metrics based on cyber-risk appetite?
   Definition of risk appetite is discussed in Principle 4. In addition, Principle 2 points out the importance of reputational risk and legal risk which helps focus on some potentially important aspects affecting risk appetite.
   Metrics on risk appetite is a fundamental question for the Chief Information Security Officer (CISO) and the Chief Risk Officer (CRO)—and other appropriate officials with these responsibilities. This type of collaboration can produce qualitative and quantitative data points for presentation to the board that provide context around cyber-risk appetite.

   "Linking relevant quantitative metrics to well-designed qualitative statements is important to measure the level of compliance of the institution with the risk appetite statement. Often more than one indicator is needed to adequately reflect a given risk appetite statement. The metrics selection process should ensure that (a) the metrics have a clear link to the statement, (b) data required to measure the metrics are available or can be collected in a timely fashion, (c) the metrics are measuring risk (rather than pure performance) and the design of the metrics is forward looking where possible, and (d) the metrics are simple and easy to interpret for an audience less familiar with the topic. The limited availability of internal (and external) historic data for potential cyber risk metrics makes the calibration of thresholds challenging. Therefore, alternative calibration approaches need to be used to establish meaningful thresholds."[87]

[87] Oliver Wyman, When The Going Gets Tough, The Tough Get Going Overcoming The Cyber Risk Appetite Challenge, April 2018

2. What Value chain metrics do we have that indicate risk to the company? One organisation has implemented a cybersecurity risk "index" which incorporates several individual metrics covering enterprise, supply chain, and consumer-facing risk, depending on the materiality of the issue or asset.

   For example,

   - If a company is dealing with a large customer base, risk indexes may focus, among other things, on customer risk.
   - If the company is dealing also with a large supplier group or partnerships, risk indexes may move in the direction of supplier vulnerabilities.
   - If intangible assets are a major value to the company, a cyber risk index can focus on the asset protection.

   Thus, it is fundamental to ascertain what values are at risk from Cyber-attacks and the potential losses, whether financial or reputational: Cyber Value-at-Risk and Cyber scenario losses can be assessed on this basis and are part of the fundamentals of developing risk appetite.

   Value chain relationships typically pose increased risk for companies given the degree of system interconnectivity and data-sharing that is now part of everyday business operations.

   - How do we assess the cyber-risk position of our suppliers, vendors, JV partners, and customers?
   - How do we conduct ongoing monitoring of their risk posture?
   - How many external vendors connect to our network or receive sensitive data from us? This is a borderline operational metric, but it can help support discussions with management about residual risk from third parties.
   - There are service providers within the cybersecurity marketplace that provide passive and continuous monitoring of companies' cybersecurity postures. A growing number of firms use these services to assess their high-risk third-party relationships as well as their own state of cybersecurity.

3. Metrics on **budget utilisation** may be useful.

   - How much of our IT/technology budget is being spent on cybersecurity-related activities?
   - How does this compare to our competitors/peers, and/or to other outside benchmarks? These metrics will support conversations about how management determines "how much spending is enough," and whether increasing investments will drive down the organisation's residual risk. Additional follow-on questions include these:
     - What initiatives were not funded in this year's budget? Why?
     - What trade-offs were made?
     - Do we have the right resources, including staff and systems, and are they being deployed effectively?

4. Metrics on the effectiveness of the organisation's cybersecurity programme and how it compares to those of other companies is clearly of interest at board level.
    - Board-level metrics should include the reporting of the several aspects composing the maturity scale of the cybersecurity programme.
    - Board-level metrics should highlight changes, trends and patterns over time, show relative performance, and indicate impact.
    - External penetration-test companies and third-party experts may be able to provide an apples-to-apples comparison within industry sectors.

5. While operational metrics are the domain of the IT/Security team, it may be beneficial for directors to understand the breadth and depth of the company's cybersecurity monitoring activities for the purposes of situational awareness.
    - What operational metrics are routinely tracked and monitored by our security team?
    - How many data incidents (e.g., exposed sensitive data) has the organisation experienced in the last reporting period?
    - How timely has the identification and resolution of those incidents been?

    These metrics will assist conversations about trends, patterns, and root causes.

6. What metrics do we use to evaluate **cybersecurity awareness** across the organisation?
    - Data about policy compliance, the implementation and completion of training programmes, and the like will help to inform about insider risks at various seniority levels and in various regions and divisions.

7. Metrics on incident management and reputational risk.
    - Did an incident have a reputational impact causing loss of customers or sales?

8. How do we track **the individuals or groups that are exempt from major security policies**, activity monitoring, etc.? These measures will indicate areas where the company is exposed to additional risk, opening the way for discussions about risk/return trade-offs in this area.

Developing Cyber Economic Metrics

Cyber risk is now clearly a board-level issue. The challenge, however, is how to effectively and precisely communicate the financial impact of cyber incidents to the board. Before boards can make informed decisions on how to manage cyber risk, they must first have the ability to translate cybersecurity data into financial metrics. Board directors will need to work with management to outline the most relevant cybersecurity information given the organisation's operating environment, including industry or sector, regulatory requirements, geographic footprint, and so on. To get started, the following board-level cyber risk recommendations provide a starting point that boards should consider requesting from management:

- What are **our quarterly expected loss ratio** metrics related to our cyber-risk condition across our various business units and operating environments?
- What is the **financial impact** related to our cyber risk **worst-case** scenario?
- How are we measuring and prioritizing our **control-implementation activities and cybersecurity budgets** against our financial exposure to cyber risk? Have we adopted operational metrics such as number of incidents, time of response, measured full impact of incident, etc?
- Have we connected our control implementation strategy and cybersecurity programmes, including budgets, with our cyber-risk transfer strategy?
- Based on our financial performance targets, how can cyber risk impact our financial performance? What is our **annual cyber risk expected loss value**?
- What is our cyber risk remediation plan to achieve our target expected loss tolerance level? Is our plan producing a net positive financial return?
- How does our cybersecurity programme align cyber risk based expected loss ratio analysis and expected loss tolerance targets? How are we measuring, tracking, and demonstrating how our **cybersecurity investments** are **reducing our financial exposure** to cyber incidents and delivering cybersecurity **return on investment**?
- How are we measuring and aligning our cyber risk based expected loss ratio analysis and cybersecurity planning with our cyber insurance risk-transfer plan?
- How do we measure the effectiveness of our organisation's cybersecurity programme and how it compares to those of other companies?

Source: Secure Systems Innovation Corporation (SSIC) and X-Analytics