Executive UPDATE
CUTTER CONSORTIUM
Access to the Experts
BUSINESS TECHNOLOGY & DIGITAL TRANSFORMATION STRATEGIES

Cybersecurity Reporting: What Does the Board Want?

by Aurobindo Sundaram

In today's digital world, cybersecurity is top of mind for both management and boards of directors. Hardly a day goes by without news about a large security incident. Consequently, management and boards are being held more accountable than ever before; after the Equifax data breach in 2017, for example, the company's CEO, CTO, and CSO all retired. Indeed, every non-executive director (NED) I've encountered in my professional capacity knows, has knowledge of, or has been involved in some type of security incident that led to significant losses.

So, given this heightened cybersecurity environment, what should you provide in response to a board request for assurance that the company is performing its fiduciary duty? Moreover, what information should you provide to assure the board that it is appropriately protecting the company?

The Answer

You should provide confidence. That's it. Boards want confidence that management is appropriately mitigating cybersecurity risks. Confidence can take a few different forms:

- Confidence in the leader(ship) of cybersecurity for the company.
- Confidence that there is management support for the program.
- Confidence that there is an appropriately executed security program.
- Confidence that the security program is forward-looking.
- Confidence that security tradeoff decisions are made appropriately, with due consideration of commercial, regulatory, and security interests.

The attentive reader will note that I have not mentioned content (technical/nontechnical, risk-based, qualitative/quantitative, case studies) or format (heat maps, graphs, text, reports/presentations). In this *Executive Update*, I propose a five-section standard presentation template for the board. I assume the CSO will be the role briefing the board, as boards like to hear from the subject matter expert.

Section A: Industry Update and Company Implications

Every NED reads the newspapers, airline articles, and front-page Web items and sees what we all see: a seemingly never-ending string of stories about ransomware, large data exposures, bugs, vulnerabilities, regulatory fines, and more. However, these stories are never sufficiently explained, and their implications never revealed in the news. It behooves the CSO to be on top of industry occurrences, to be able to explain them in a fashion that NEDs who may not be familiar with technology can understand, to explain what the implications to the company are, and to lay out the steps the company is taking to mitigate the risk.

Consider, for example, the numerous stories about ransomware attacks from 2017 (e.g., WannaCry, NotPetya) and the losses they caused affected companies. A strategic CSO would explain how the ransomware spread so quickly (possibly with a contagious disease spread analogy) and point out that the company was also at risk, but that the risk did not manifest because of the company's strong, metrics-driven patch management program. A timeline of the ransomware event in the industry, overlapping with actions the company took to mitigate the risk internally, would also be useful. Remember what the CSO must project: confidence.

Section B: Company Cybersecurity Posture

This section is not intended to be tactical (i.e., metrics, which are discussed in Section D) but is certainly operations-related and should dovetail with the strategic update discussed in Section E. The company cybersecurity posture covers various interrelated areas, such as:

- **Risk assessment.** The CSO should assure the board that the company has appropriately considered the universe of cybersecurity risks and its potential impact and is implementing appropriate measures to mitigate the identified risks. I prefer a standard heat map with associated explanations (see example in Figure 1), but there are many (all imperfect) ways of communicating a risk assessment's results. Pick one that's consistent with the way your organization communicates business risk and use it.

- **Key incidents and trends.** In every organization, there will be security incidents of varying impact. The CSO should brief the board on key incidents, their root causes, failures in controls, lessons learned, and projects initiated to ensure continuous improvement. Also, any trends in incidents or control failures (e.g., three incidents during the prior quarter when attackers emailed finance staff and they all acted out of process [i.e., they were phished]) and what has been done to counter them should be presented

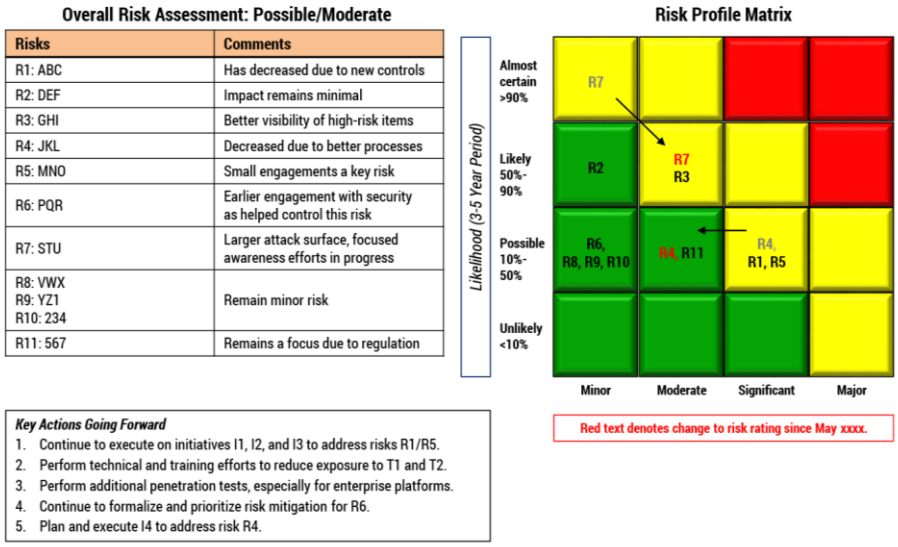

Figure 1 – Sample risk assessment heat map.

to the board. There are few things that give the board greater confidence than knowing that, while there will be incidents, there is a measured, analytical process for handling them and ensuring that lessons learned are incorporated into the cybersecurity program.

- **Key projects.** This update must be consistent with the risk assessment and key incidents update. The reason? You don't initiate a project unless it's (1) strategic (see Section E), (2) to address a significant risk as indicated by the risk assessment, or (3) to address control failures or gaps that led to incidents.

Section C: Relevant Cybersecurity Education

NEDs are often high-level executives who are not used to being the least knowledgeable on *anything* in *any* room. However, as a group, they are not cybersecurity experts. The field of cybersecurity has moved (and will continue to move) so swiftly that even experts in the field are left behind. NEDs may have such questions as:

- What is "the cloud" and what are its security implications?
- What is blockchain, why is it so cool, and why can't someone just hack it?
- What is the Dark Web? What information is on it? Is our data on the Dark Web? How would we know?
- What is virtualization and is it more secure? What are terms like "bakery," "containers," and "Docker," and how do they result in better security? Or do they?
- What is encryption at rest and what does it guard against? Why can't we encrypt everything?

Often, NEDs, like any other humans, are loath to show their ignorance of a topic. To build relationships with NEDs, and in turn build their confidence, CSOs must take the opportunity to educate the board on a single security-related topic at every briefing. This may be something recently in the news (e.g., SQL injection), something that aligns with company strategy (e.g., cloud or mobile everywhere), or something exciting and sexy (e.g., the Dark Web). A thoughtful explanation of the topic, implications for the company, and what the cybersecurity organization is doing to address these implications is an excellent idea.

Section D: Indicators of Operational Efficacy (Metrics)

This section is where the rubber meets the road when it comes to communicating cybersecurity to the board. Far too many CSOs have caught themselves in a blunder by communicating metrics that are too technical, don't have a correlation to risk, don't have a correlation to business value, or are not controllable. The smart CSO ensures that indicators of operational efficacy align with the risks communicated in Section B. Consider this example: a key risk might be exposure to attacks from publicly exposed websites; a key mitigation would be a vulnerability management program; and a metric would be the number of systems scanned, the number of open high-risk vulnerabilities, and the average time to remediate a high-risk vulnerability. CSOs should use the following criteria to select metrics:

- Metrics should be specific.
- Metrics should be controllable (e.g., number of viruses blocked is an indicator but not a metric).
- Metrics should be actionable (i.e., there should be a way to improve them).
- Metrics should directly correlate to risk and business performance (i.e., if they are not measuring aspects of your risk assessment, you're probably doing them wrong).
- Metrics should be straightforward and contain as little ambiguity as possible.
- Metrics should be comparable, either to best practice or to industry benchmarks.

In a hypothetical example, the three biggest risks for a corporation may be its external Web footprint, phishing and social engineering, and third-party vendor management. Appropriate metrics may be:

- Visibility of external Web footprint (0%-100%), high-risk vulnerabilities on external Web footprint, and mean time to remediate a high-risk vulnerability.
- Results from phishing simulations of employees.
- Percentage of high-/medium-/low-risk vendors that have had assessments completed.

Section E: Indicators of Strategic Direction

NEDs don't only want to know that security threats are being addressed efficiently. They also want to know that leadership is looking ahead of the curve. Cybersecurity is a fast-moving field and what is state of the art today is often obsolete tomorrow. So too with threats: while some threats are universal and long-lived (e.g., social engineering), others come and go quickly. The CSO must give the board confidence that there is a measured, strategic, forward-looking direction of progress. The CSO might, for example, extrapolate the risk assessment results from Section B to position cybersecurity strategy toward a three-year plan to implement multi-factor authentication for all employees. As another example, the CSO might provide a strategic direction for logging and monitoring, which focuses on quicker risk detection and mitigation:

- **Today, year 0** — manual logging and monitoring
- **Year 1** — automated monitoring with alerting
- **Year 2** — orchestration of mitigation activities to include automatic blocking of alerted traffic
- **Year 3** — integration of threat intelligence feeds into monitoring and orchestration framework

Conclusion

Any presentation to the board does not need to exceed about 10 well-written slides or three to five well-written pages. A diligent CSO will divide his or her presentation into the sections above and use them consistently at every briefing (i.e., industry update, cybersecurity program, training, operations, strategy), providing the board with all it needs from a confidence perspective.

About the Author

Aurobindo "Robin" Sundaram is Head of Information Assurance & Data Protection at RELX Group, an FTSE 100 listed company. Mr. Sundaram is responsible for creating and developing security and risk management policies, procedures, and standards; collaborating with CSOs to implement these policies; creating and enhancing fraud-detection technologies; investigating and responding to security incidents; and ensuring compliance with information security frameworks. He regularly reports on information security to RELX Group's board of directors, CEOs, and CTOs. Previously, Mr. Sundaram spent seven years at Schlumberger, a leading oilfield services corporation, where he implemented its information security program. During his tenure, objectives reported to the board were set for information security across the 50,000+ strong organization for the first time in Schlumberger's history. Mr. Sundaram was also closely involved in the design of the technical security architecture for the 2004 Summer Olympic Games in Athens, Greece. His thought leadership has led to several published papers in the security field, and he was recognized as a finalist for Information Security Executive of the Year in 2007 for the southeast region of the US. Mr. Sundaram holds a master of science degree from Purdue University and an MBA from Emory University. He can be reached at aurobindo.sundaram@relx.com.