5 Rs to Demystify Cybersecurity

Readiness, resilience, resources, reporting, results

By Eileen Kamerick and Mark Trembacki

"We were surprised because you don't expect something like this to happen," the COO of the largest containership company in the world was quoted as saying when their computer systems were rendered inoperable by a cybercrime-generated computer malware in late June. This happened despite the company management and board's extensive efforts to protect the company from just such an event.

Unfortunately, this scenario haunts many directors. Nearly 60% of directors find it challenging to oversee cyber risk, according to the National Association of Corporate Director s(NACD) 2016-2017 Public Company Governance Survey. Cyber risk also was ranked as the top risk for boards in the 2016 *Board Practices Report* by Deloitte's Center for Board Effectiveness and the Society for Corporate Governance.

There are, however, practical, actionable steps to ensure that when a cyberattack hits, your company will be both ready to address the threat and resilient enough to recover from it.

Technology has moved from an enabler to a core business imperative in virtually every organization because of technology's pervasive presence in processes, customer delivery and communication protocols. Cyber risk has moved from the IT department to a full-fledged enterprise risk.

Leveraging a flexible and uncluttered framework — what we call "The 5 Rs" — is key. Understanding cybersecurity issues will support the board's governance obligations, propel innovation, protect reputations and enhance financial performance. For cyber risk, it is possible to follow the old adage "nose in, fingers out" from a board governance perspective.

The 5 Rs framework represents a straight-forward and easy-to-remember approach for board oversight.

Readiness: The implementation of foundational cybersecurity practices, often called cyberhygiene — policies, assessment, training — points to an organization's overall state of cyber preparedness.

Resilience: A cyber incident is not a matter of "if," but "when." Ensuring the organization can operate through and recover from an event is essential.

Resources: The availability and allocation of human, financial and technological resources are critical inputs that must be deployed in a balanced manner.

Reporting: Clear, consistent, jargon-free reporting supports board engagement and awareness on cybersecurity topics.

KEY POINTS OF BOARD FOCUS

READINESS

- ☑ Have we identified and categorized the data we are trying to protect – what are the "crown jewels" of the company?
- ☑ Have we articulated a cyber risk appetite to guide decisions?
- ☑ What risk assessment framework have we selected and why?
- ☑ Do we have a comprehensive set of policies in place? What is the update frequency?
- ☑ What is the training and awareness program? Does it include contractors and consultants as well as employees?
- ☑ Do major decision processes (M&A, third parties/vendors, strategy, financial, etc.) include a cyberfilter?

RESILIENCE

- ☑ Do we have a current business continuity and disaster recovery plan in place? Does it include cyber specifics?
- ☑ How frequently do we test the plans through "table-top" scenarios?
- ☑ Is there an identified group of experts we can quickly call upon in a breach to support response and recovery?
- ☑ Does our planning approach extend to third parties such as vendors and suppliers?
- ☑ Do our plans include internal and external communication plans covering all channels, including social media, and have clear responsibilities?

RESOURCES

- ☑ Do we maintain a broad view of resources – human, technical, financial?
- ☑ Does the organization have the right cyber talent and leadership?
- ☑ What is the talent pipeline for cyber-related positions?
- ☑ Can we benchmark our spending to other similar organizations?
- ☑ How should the next dollar be spent to plug known gaps?
- ☑ What risk transfer mechanisms (insurance) are available to us and how have we utilized them?

REPORTING

- ☑ Are board and committee cyber reporting protocols in place covering both qualitative and quantitative aspects?
- ☑ Are the measures relevant by allowing for internal comparisons and/or external benchmarks and trends?
- ☑ Is the reporting risk-adjusted?
- ☑ Have leading indicators been included?
- ☑ What external experts are available to the board to bolster cybersecurity awareness and fluency?
- ☑ Do we understand regulatory expectations and can clearly demonstrate compliance?

RESULTS

- ☑ A cyber-aware culture is embedded throughout the organization.
- ☑ Employees understand their crucial role in combatting cybersecurity.
- ☑ All major business decisions include a cyber risk lens.
- ☑ Responses to cyber incidents are decisive and serve to contain financial and reputational damage.
- ☑ Cyber investment decisions are balanced, transparent and measured.
- ☑ Third parties are part of the organization's cyberecosystem.
- ☑ Activities, actions and decisions are risk-adjusted

Results: Driving results means answering the question, "What does success look like?" A clear vision will guide, motivate and inspire.

5 Rs implementation considerations

Implementation should be tailored to each company's industry and operations specifics as well as the cyber risk management organizational maturity. Several challenging board-level topics include:

- Board and management roles for cyber risk should follow the same paradigm for the division of board and management responsibilities — the board maintains an oversight and advisory role while management is responsible for day-to-day execution and operations.
- Separate committee oversight does not relieve the full board of its core oversight responsibilities to identify, mitigate and manage cyber risks. Committee involvement varies by company and industry, ranging from audit committee oversight to separate risk and technology committees. Moving cyber risk away from jam-packed audit committee agendas may be required to create adequate committee time.
- Outside experts can help deepen understanding of cyber risk through periodic "deep dive" briefings from third-party experts, including cybersecurity specialist firms, government agencies, and industry associations. Existing independent advisors (counsel, auditors) can leverage their first-hand knowledge of the company's operations with broad cyber risk trends.
- The nominating and board governance committee should determine cyber-risk expertise need. Like other desired expertise (M&A, HR, legal, etc.), embedding cyber into the recruitment process will help ensure well-rounded board members.

As Holly Gregory, a governance expert and Sidley Austin LLP partner, states:, "Not all companies will require a director with deep technical expertise, but as companies become ever more dependent on information technologies and the risks of cybersecurity breaches grow, many boards could benefit from having one or more directors who are sufficiently fluent…in these areas."

Agenda management also becomes an important driver of overseeing cyber risk as an enterprise risk and should:

- include cyber security regularly on board and committee agendas.
- include a cyber filter in key decisions such as M&A, new initiatives, capital expenditures.
- maintain a direct line of communication with the chief information security officer.
- have board members participate in "table top" exercises testing incident response and disaster recovery plans.

Incorporating The 5 Rs framework provides a useful tool to break down cyber security into digestible pieces to increase directors' understanding and confidence on this critical issue. ■

For cyber risk, it is impossible to follow the old adage "nose in, fingers out" from a board governance perspective.

Eileen Kamerick *serves as non-executive director on three public company boards: Associated Banc-Corp where she chairs the corporate governance committee. She also chairs the audit committee for both Legg Mason closed end mutual funds and Hochschild Mining, plc. She serves as an adjunct professor of corporate governance and finance at University of Chicago Law School, Washington University in St Louis College of Law and University of Iowa College of Law. She is co-founder of The Governance Partners, a governance and performance improvement consulting firm.*

Mark Trembacki *is the founder of Risk Management Levers, Inc., a consulting firm focused on risk management, acquisition integration and change management. He is an adjunct professor at the University of Illinois Urbana-Champaign teaching Enterprise Risk Management. Mark has a MBA in Finance from The University of Chicago, a BS in Accounting from The University of Illinois at Urbana-Champaign, and is a CPA. He is a qualified SEC Financial Expert and a NACD Governance Fellow.*