

For Boards, the Best Cybersecurity Defense Is a Good Offense

By Robert Snodgrass and Rod Hackman

Complex digital systems are the central nervous system controlling your company's most vital assets and business outcomes. Their importance only exacerbates the growing complexity and rapidly changing nature of cyber risk. As boards face significant cybersecurity governance, disclosure, regulatory, and legal challenges, they often find themselves playing defense.

Cyber risk transcends typical business risk. Familiar defensive measures and compliance requirements are necessary but alone do not constitute effective governance. Further, they are often communicated using technical language that lacks the business context boards should demand.

To effectively govern, boards must go on the offensive by taking a proactive approach that centers on three core areas.

Organization. By solidifying an organizational hierarchy with clear roles and responsibilities, an enterprise establishes a foundation for processes that proactively protect against cyber threats. This also creates a knowledge base among leadership to drive education and culture. Boards can consider the following actions:

- Create a cybersecurity organization to fit the size of the enterprise. For smaller companies, that might mean outsourcing a chief information security officer (CISO). For larger enterprises, functions could be assigned to leaders of an in-house team, including a chief risk officer, chief information officer, or CISO.
- Appoint a chief cybersecurity officer to lead the team. This person should be a peer of organization executives, to whom they may offer respected perspectives and directives across enterprise functions. They should have an independent reporting channel to executive leadership.
- Establish an internal management and a chartered board risk committee to oversee enterprise and cyber risk.
- Identify and evaluate existing baseline cybersecurity controls that impact all systems in the enterprise.
- Establish a cybersecurity framework and procedures based on the cyber-risk committee's recommendations. Start with the National Institute of Standards and Technology's cybersecurity framework and modify as needed.

Education. Cyber risk is a form of systemic risk. Controlling it requires a working knowledge of underlying systems. Otherwise, risk protection tools and methods lack context and can be suboptimal.

Enterprises need to be defined within the context of a system—a regularly interacting and interdependent group of elements,

subsystems, and assets. For example, the elements of enterprise as a system (EAS) include assets and processes that interact with one another both internally and externally and with people.


Boards can govern the EAS with the following process:

- **Phase 1:** Produce a high-level business process map of the EAS using common business language.
- **Phase 2:** Produce a detailed business process analysis and board summary. Break down the larger Phase 1 elements to better understand overall processes and interactions. Approach these elements incrementally based on relative importance.
- **Phase 3:** Utilize outside advisors to identify and determine the efficacy of relevant cybersecurity controls against the specific elements identified in Phase 2. Provide recommendations to the board to remediate gaps.
- **Phase 4:** Develop and articulate the risk appetite, risk indicators, and associated thresholds that the enterprise accepts in pursuit of value. Optimize the EAS to reduce the threat landscape and improve control efficiency, adjusting the use of cybersecurity tools accordingly.

Through these phases, the board and other executives share a contextualized picture of the EAS in understandable business language. The EAS should be reevaluated whenever changes are introduced, such as new digital systems or mergers and acquisitions.

Culture. Once the board signals its priority of cybersecurity through organizational and educational steps and has a business context for areas of greatest risk, it can do the following to ensure all constituents embrace this shared responsibility:

- Emphasize the importance of addressing cyber threats before they become a reality.
- Communicate emerging cyber threats and incidents through established channels.
- Market the importance of cybersecurity and reward good behavior.

These initiatives, as part of comprehensive and thoughtful changes to the three focus areas, will put boards on the offensive against cybersecurity. 



ROBERT SNODGRASS is a director with RSM's Security and Privacy Risk Consulting practice. **ROD HACKMAN** is the firm's executive advisor for board excellence.

RSM is an NACD partner providing directors with critical and timely information, and perspectives. RSM is a financial supporter of the NACD.