NATIONAL DIRECTORS INSTITUTE | NDI Executive Exchange

TOP TAKEAWAYS

Maximizing ROI in Your Cybersecurity Program

1. **Treat Cybersecurity as an Enterprise Risk.**
   Cybersecurity is an enterprise risk that requires an enterprise solution. Boards have traditionally viewed cybersecurity as an IT problem, that perception by board's is changing however with recognition by many of the need for a holistic view of security. Organizations will not be able to predict and prevent every threat; however, establishing a robust, enterprise-wide cybersecurity program will maximize coverage against threats and allow organizations to detect and respond to attacks quickly.

2. **Recognize the Likelihood of Attack.**
   The key questions for directors today are "*When* we breached, h*ow long* will it take to *realize* that we have been breached?" and "Have we taken the appropriate steps to respond quickly, mitigate the impact, recover, and minimize liability and risk? The commoditization and sophistication of cyber-attacks continues to increase at a rapid pace and boards must recognize the need to address cybersecurity in a manner that conforms with the evolving standard of care.

3. **Be Proactive and Agile.**
   Many boards experience analysis-paralysis when it comes to cybersecurity. Organizations with little cybersecurity experience will benefit from first identifying and implementing the low-cost, high-return tasks to identify, protect, detect, respond, and recover when it comes to cybersecurity. Once a security program is in place, organizations must monitor compliance efforts and exposure to ensure policies and practices are continually reviewed and improved.

4. **Establish Relationships with Experts.**
   Use of third party contractors for cybersecurity prevention and response is on the rise across industries. Retaining experts in-house is often no longer attainable because of the vast demand for cybersecurity expertise. It is critical that organizations establish business partner relationships to identify, defend against, detect, and respond to cybersecurity threats before they occur.

5. **Invest in Recovery.**
   Boards must focus on how the organization will recover from a cybersecurity incident. Companies that address cybersecurity may score well on industry measurements for reducing the frequency of incidents, but continue to score poorly for reducing the magnitude of an incident. Companies fail to sufficiently invest in disaster recovery and business continuity, each of which relate directly to the severity of an incident and are critical elements of an enterprise cybersecurity program. Experts estimate that Target could have achieved an 80% reduction in its loss if it had a robust disaster recovery and business continuity plan in place.

6. **Train Employees.**

Training employees is the lowest cost and highest return approach to address cybersecurity. Cybercrime relies on the human desires to trust and help and training enables employees to understand how those qualities are routinely exploited by cyber criminals and how to act differently to address security threats. Training employees and having policies in place will, however, be insufficient if policies are not enforced and the organization fails to establish a culture that values security.

7. **Measure against Industry Standards.**
Benchmarking against peer firms for cybersecurity programs has become largely irrelevant. In the event of an incident, insurers, regulators, and consumers will want to know how an organization compared to international and industry best practice standards and the "evolving standard of care" – not how the organization compared to its peers.

8. **Understand Risk and the Avenues to Recovery.**
In order to address risk, it is critical to identify and understand both what puts an organization at risk – data, people, suppliers, systems – and how those risk factors interact and materialize in the normal course of business. Similarly, in order to recover from an incident, organizations must identify and understand recovery avenues that are both operational, such as disaster recovery and business continuity plans, and financial, such as insurance coverage and contractual relationships.

9. **Practice Addressing Threats.**
Many sophisticated organizations do not simulate security incidents and therefore are not adequately prepared to address incidents when they occur. Merely maintaining security policies and a response plan are insufficient and will make the organization slow to respond and ineffective following an incident.

10. **Conduct Diligence and Enforce Contractual Protections.**
As the use of contractors increases, contractor diligence, contractual protections, and ongoing monitoring and enforcement are critical. Contractors remain a key security threat. Strong contractual obligations with service providers to maintain security and permit auditing are critical but worthless at best, and liability-generating at worst, if they are not enforced.

For more information on Maximizing ROI in Your Cybersecurity Program, please feel free to contact the moderator directly:

Jim Kalyvas
Foley & Lardner LLP
jkalyvas@foley.com