CYBERSECURITY PRINCIPLE # 1 FOR BOARDS – IT'S NOT JUST ABOUT "IT"

It has now become clear that cyber-risk needs oversight at the board of directors level. The problem is that most corporate boards are comprised of "digital immigrants" -- people not born into the digital world they now inhabit -- and therefore need to learn how to understand cyber-risk.

That educational process has been undertaken by the National Association of Corporate Directors in **in conjunction with AIG and the Internet Security Alliance (ISA)**. In January, they published the second edition of the "Cyber-Risk Handbook" for corporate boards. The handbook states that the very first principle boards need to understand is that cybersecurity is not an "IT" issue," -- it's an enterprise wide risk management issue.

In the past 25 years, the nature of corporate asset value has changed significantly, shifting away from the physical toward the virtual. Along with this rapidly expanding digitization of corporate assets, there has been a corresponding digitization of corporate risk – loss of IP and trading algorithms, destroyed or altered data, declining public confidence, disruption to critical infrastructure, and evolving regulatory sanctions. Each of these risks can adversely affect competitive positioning, stock price, and shareholder value.

Cyber-risk is viewed the same way as other critical risks – in terms of risk-reward trade-off. This is challenging in the cyber arena due to the growing complexity of cyber threats and companies' desires to deploy new and emerging technologies to increase profitability and improve customer experience.

These competing pressures mean conscientious and comprehensive oversight at the board level is essential. Managing and mitigating cyber-risk impact requires strategic thinking, and it starts with realizing cybersecurity is an enterprise-wide risk management issue, not merely an IT issue.

Historically, corporations have categorized information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding is fed by siloed corporate structures that leave internal functions and business units feeling disconnected from responsibility for the security of their own data. However, deferring responsibility to IT inhibits critical analysis and communication about security issues, and hinders the implementation of effective strategies.

Some of the highest-profile data breaches to date have little to do with traditional hacking. Economically driven strategic decisions such as production strategies that use complex supply chains across multiple countries and the degree of interconnection that corporate networks have with partners, suppliers, affiliates, and customers can magnify cyber-risk. Similarly, mergers and acquisitions requiring integration of complicated systems can increase cyber-risk. While these decisions have "IT" components to them, the appropriate analysis of them goes well beyond the IT department.

Similarly, how to manage. Several significant cyberbreaches did not actually start within the target's IT systems, but rather from vulnerabilities in one of its vendors or suppliers.

As a result, directors should ensure that management is assessing cybersecurity not only as it relates to the organization's own networks, but also with regard to the larger ecosystem in which it operates.

Boards must engage management in a discussion of the varying levels of risk that exist in the company's ecosphere and take them into consideration as they calculate the appropriate cyber-risk posture and tolerance. They should also understand what "crown jewels" are in most need of protection and ensure their teams have a protection strategy in place.

Further, the **board should instruct management to consider not only the highest-probability attacks and defenses, but also low-probability, high-impact attacks that would be catastrophic.**

While including cybersecurity as a stand-alone item on board and/or committee meeting agenda is becoming a widespread practice, the issue should also be integrated into full-board discussions involving new business plans and product offerings, mergers and acquisitions, new-market entry, major capital investment decisions, etc.

On **June 21, 2017, NACD, in partnership with ISA**, will be hosting a Cyber Summit in Chicago to bring together experienced directors and cybersecurity experts to share real-world insights and critical action steps. Among the issues that will be raised for the directors to consider are:
- Do we have an enterprise-wide, independently budgeted cyber-risk management team?
- Is the budget adequate?
- How is the budget integrated with the overall enterprise risk management process?
- Where do management and our IT teams disagree on cybersecurity?
- What is enterprise strategy to address cloud, BYOD, and supply-chain threats?

Unless boards are considering cybersecurity in these larger contexts they run the risk of attenuated and ineffective cyber strategies.

Written by ISA Senior Director, Stacey Barrack