BRC
BOARD RISK COMMITTEE

BOARD RISK REPORT

December 15, 2020

By Shamla Naidoo

In today's world, businesses were already undergoing large scale digital transformation—the current pandemic has accelerated that process. Both B2B and B2C companies increasingly rely on technology to interact with customers. New transformation activities go beyond simply modernizing older technology to include rapid adoption of transformational digital technologies. This accelerated change heightens the risk of data theft, compromise, and digital disruption. Those risks can and should be managed.

SECURING THE BUSINESS

Boards routinely refresh business strategy to protect and grow shareholder value. For many organizations, the convergence of business and cyber strategies is becoming more important every day, garnering board attention. Boards are realizing that siloed cyber strategies will fall short and may not be aligned with business strategy. When strategies are properly aligned, technology can fuel growth rather than inhibit it.

What Boards Should Do:

- Encourage business leaders to converge business and cyber strategies. Disconnected strategies are inefficient and can obscure true risks.
- Ensure that the strategies are regularly refreshed with mutual alignment to business outcomes.
- Identify and evaluate new risks that may be created or amplified by new technology or the evolution of strategy.

ALWAYS INNOVATE

Emerging technologies (e.g., Artificial Intelligence and Machine Learning [AI/ML], blockchain and quantum computing) let businesses build products and services at scale and faster than previously possible. While risks are often perceived as reasons not to adopt new products and services, the application of effective risk management processes can accelerate rapid execution of business strategy.

What Should Boards Consider?

- Ensure your organization has a framework capable of adaptation to rapidly-changing risk landscapes. Be clear about what risks are absolutely unacceptable versus risks that can be measured and managed with confidence.
- Determine if your organization is maximizing its investments in critical technologies.
- Ensure management is addressing obstacles that prevent adopting new technologies at an accelerated pace.
- Benchmark your cyber risk management plan against best-in-class competitors.

PRACTICE SAFE BUSINESS IN THE 5G ENABLED INTERNET OF EVERYTHING

Many physical devices are connected to the internet today, from appliances to Barbie™ dolls, automobiles to Zoom™ cameras. As 5G is more widely deployed, the speed, capacity, and ubiquity of internet access will increase. Even standalone manufacturing equipment can benefit from connectivity, assuming cyber risks are properly managed. Faster, 5G-enabled network services will democratize the internet and offer reliable real-time access to time-sensitive data and have the capacity to change the world. For example:

- Vehicles will be more autonomous and will be able to respond quickly to diverse circumstances
- Connected manufacturing machines can modify formulae automatically and quickly when needed.
- Transmission of medical information from ambulances to hospitals and doctors can save patient lives.

What Should Boards Consider?

- Does your organization maintain an inventory of connected devices, and appropriate processes to secure them?
- Does your organization understand the full operational impact if connectivity is lost or disrupted?
- Does your organization possess the skills and capabilities required when operational technology and information technology merge? Where can these skills be found?

PROTECT CRITICAL DIGITAL ASSETS TO ENSURE FUTURE BUSINESS GROWTH

How are you protecting your crown jewels? Data is ubiquitous in today's organizations and some of that data may be considered corporate crown jewels. Mission critical data may be contained or implicit in strategy, planning, engineering, marketing, and M&A documents. Intellectual Property may be disclosed in design prototypes, or hardware and software code that propels company products. When crown jewel data is stolen or tampered with, future business performance may significantly erode.

What Should Boards Consider?

- Corporate leaders must be accountable for identifying and tagging all high value Intellectual Property.
- Ensure the cybersecurity plan includes specific measures to protect Intellectual Property.
- Determined nation state actors and criminals represent an ongoing risk to high-value information assets. The security measures protecting those assets should be commensurate with the risk to the business.
- Don't assume that trusted insiders won't take malicious actions with IP. Make sure the insider threat program is robust.
- Boards should ensure that management proactively plans for:
- when to engage with law enforcement when Intellectual Property is stolen; and
- when to pursue prosecution for intellectual property theft.

"When digital transformation is done right, it's like a caterpillar turning into a butterfly, but when done wrong, all you have is a really fast caterpillar."

George Westerman
MIT Sloan Initiative on the Digital Economy

ABOUT THE AUTHOR

Shamla Naidoo is a Managing Partner at IBM where she advises CEOs, board members, and executives on digital transformation, innovation, and strategic risk management. She was formerly IBM's Global Chief Information Security Officer (CISO), where she was responsible for securing the company's digital footprint. Her mission included the protection of IBM's critical information assets, including the world's largest patent portfolio. In her leadership roles at high-profile companies and on advisory boards at both public and private companies, she has built a track record of helping companies create value while aggressively managing risk.

WHO WE ARE

The Board Risk Committee (BRC) is a non-competitive thought leadership peer forum dedicated to Board Risk Committee members and Chief Risk Officers (CROs). The BRC is a trusted place for the exchange of ideas, best practices, and topics of interest. BRC is affiliated with The Santa Fe Group (SFG). SFG is a strategic advisory company providing unparalleled expertise to leading financial institutions, healthcare payers and providers, law firms, educational institutions, retailers, utilities, and other critical infrastructure organizations.

CONNECT WITH US