SUCCESSFULLY ASSESSING AND MANAGING YOUR CYBER RISK

nextLevel
BUILDING ENTERPRISE VALUE

Do you know where you're most vulnerable to cyber attack?

Cyber security threats to your business are constantly increasing and constantly evolving. It's easy to get overwhelmed and paralyzed, not knowing how to allocate limited resources to comply with regulations and protect your assets. But with the right approach and strong leadership, cyber risk vulnerabilities can be understood and your exposure mitigated.

In this edition of *Executive Issues & Insights*, we explore key insights drawn from the extensive C-suite and Board experiences of the NextLevel team on successfully assessing and managing your cyber risk.

NextLevel Case Study

Significant reduction in cyber security exposure

A HIPAA-regulated organization that needed to support large volumes of Personally Identifiable Information (PII) and electronic Personal Health Information (ePHI) was concerned about their cyber security exposure. In addition they needed to comply with both HIPAA (Health Insurance Portability and Accountability Act) regulations as well as their Business Associate Agreements (BAA) with their key customers. The company was growing very rapidly; a significant cyber security breach or failure to demonstrate adequate controls could cause unrecoverable harm to their business.

Although the company had made significant investments in cyber security, they were not sure if the investments were properly placed. They wanted to find out if there were significant unknown exposures that, if exploited, would impair their ability to aggressively execute on their strategic objectives.

(more)

NextLevel Insights

Set the tone on cyber security from the top

The C-suite and Board should set the level of cyber awareness. Often there is a gap between company governance and those responsible for cyber security. Understand the nature, diversity and dimension of the threat and reinforce the importance of cyber security through policies and procedures. This creates a company atmosphere of cyber awareness that is your first level of defense.

Understand the key threats that could harm your business

Not all cyber threats have the same business repercussions. Framing questions in business terms will help you clarify where your focus should be. Make a clear connection between the risks and vulnerabilities in terms of the business and regulatory outcomes of a breach.

Take a risk management perspective

Treat cyber risk management as part of your overall enterprise risk management process. Understand that the threat is constantly evolving; rather than trying to eliminate all cyber risk, allocate resources that will protect your most valuable data and assets first. Don't fall into the trap of having too many Number One cyber security priorities.

(more)

SUCCESSFULLY ASSESSING AND MANAGING YOUR CYBER RISK
(continued)

(continued)

A NextLevel Cyber Security Executive was brought in to help them make these assessments and take the steps to prioritize and address any cyber security risks.

The NextLevel Executive worked with the company to identify the key threats that could harm their business as well as assess their current security and control environment. He next established a clear security and control framework to provide guidance and understanding. Based on the key business threats, he prioritized, recommended and supported the implementation of required controls, activities and technical solutions.

As a result, the organization was able to fully satisfy BAA security audits by their key customers and focus on the most important security improvements. They established a pragmatic cyber security roadmap moving forward to enable on-going visibility and risk management, and significantly reduced their cyber security exposure and potential liability.

THE CYBER RISK PROBLEM IS NOT A SINGLE PROBLEM—IT IS THOUSANDS OF PROBLEMS SPREAD OVER THE YEARS OF TECHNOLOGY YOUR COMPANY HAS ACQUIRED."

Cyber risk can be successfully assessed and managed, but leadership must be aware and proactive.

(continued)

Have a security framework

Develop a cyber security framework that delineates your specific vulnerabilities and the administrative, physical and technical controls that would address them. Know what controls will best protect your information and assets so you can allocate resources appropriately. This framework should be communicated to stakeholders both internally and externally to align everyone to a common set of goals.

Assume you will be breached

No matter how good your systems are, if your business uses computers, you are vulnerable to cyber attack from many different vectors. Do you have a system for detecting if an attacker has gotten in? The average time an attacker is in a system before discovery is 172 days, and 90 percent of the time, discovery is by an external party. Have a contingency plan based on *when* a breach will occur, not *if* it will.

Bring in outside expertise

Schedule regular independent third-party assessments of your cyber security system in the same way you would schedule an audit of your finances. From a risk management perspective, it is important to get an outside assessment that lets you know if there are areas you have missed—a "heat map" of where you need to focus.

KEYS TO SUCCESSFULLY ASSESSING AND MANAGING YOUR CYBER RISK

- **Your leadership:** Are you setting the level of cyber security awareness from the top?
- **Your biggest vulnerabilities:** Do you understand what they are in business terms?
- **Your perspective:** Does it allow you to prioritize resources according to threat?
- **Your security framework:** Do you have a system that delineates vulnerabilities and the controls to address them?
- **Your assumptions about cyber risk:** Are you operating from an assumption of *when* you are breached, not *if?*
- **Your external audits:** Do you have regular third-party assessments of your cyber security systems?

More Information

To learn more about how NextLevel can help you successfully assess and manage your cyber risk, call us at (800) 833-NEXT or email info@nlbev.com.

nextLevel
BUILDING ENTERPRISE VALUE