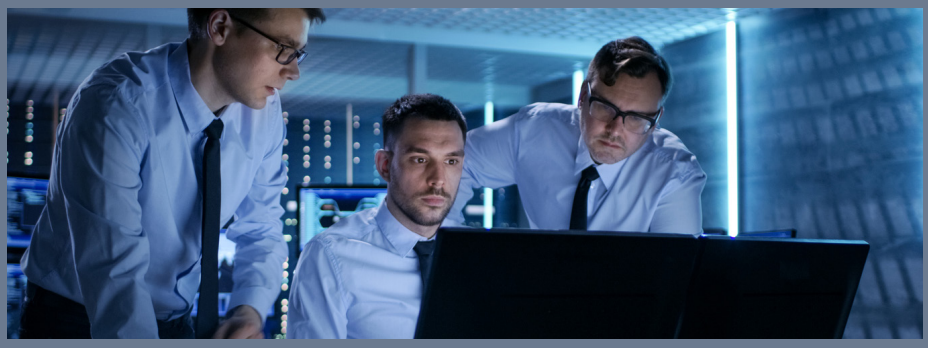
DESIRED STATE ROADMAP™: CYBER RESILIENCE

nextLevel
BUILDING ENTERPRISE VALUE

When a cyber breach occurs, do you have a specific action plan?



For most companies, the likelihood of a cyber attack is not a matter of "if," but "when." Will you know what to do first and how to respond as you work your way through damage control, public messaging, and eventual restoration? A breach response plan will help improve response time, minimize damage, avoid costly mistakes, and bring you into compliance with increasingly complex regulations.

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 how to develop a roadmap to cyber resilience.

NextLevel Case Study

Healthcare Company Reduces Risks, Saves Costs with Cyber Breach Response Plan

A healthcare company was addressing areas of vulnerability as part of a comprehensive cyber security road map. The company had cyber risk insurance, but did not yet have a breach response plan. The CIO recognized the potential risks of not being able to respond quickly and appropriately to a cyber attack, and that the company was exposed to potential penalties from strict new federal, state, and international regulations.

The CIO brought in the NextLevel partner who had prepared the original cyber security road map to develop a cyber breach response plan. First, the NextLevel partner analyzed the outside service providers for breach response support, including legal counsel, forensics, and public relations teams. He then considered the internal resources needed to manage these services and who would have responsibility for taking the actions required in the first hours and days following a breach discovery.

He analyzed key decision points the

(more)

NextLevel Insights

Assess the threat environment and your vulnerabilities

Different industries, such as manufacturing, retail, and healthcare, face different types of cyber threats. Is your company exposed to theft of customer lists or credit card data? Healthcare records? Confidential emails, trade secrets, or intellectual property? Cyber extortion? Evaluate the risk level of potential breaches based on the threat, probability, and business impact. Assess your preparedness, including whether you are capturing sufficient information to determine what was breached and its impact.

Know your contractual and regulatory responsibilities

Identify in advance your contractual obligations to customers regarding notification and response time in the event of a cyber breach so you aren't trying to look up this information in the middle of a crisis. Also know your cyber insurance policy notification stipulations. Similarly, identify the state and other governmental jurisdiction regulations you are subject to. There will likely be different requirements for each contract and regulation, so know all the layers at which you are responsible.

Establish your breach response service providers

Have contracts in place for the service providers that will be supporting you for both cyber response and business continuity in the event of a breach, e.g. outside counsel, forensics, PR, and call center. You will also want to pre-negotiate approval and rates for these partners with your cyber insurance provider so they can get working immediately when you need them.

(more)

DESIRED STATE ROADMAP™: CYBER RESILIENCE
(continued)

(continued)

company would face and came up with guidance, responsibilities, and timelines for them. He then created a checklist of actions, responsibilities, deliverables, and timelines for all phases of a breach response, from discovery to customer care and restoration. He also pre-negotiated with the cyber insurance company what outside services would be allowed under the policy, thus saving critical response time.

After being presented with the complete action plan for a breach response, and going through tabletop exercises to rehearse it, the executive team was reassured that they had a complete list of specific steps and responsibilities in case of a breach. The company significantly reduced its risk of fines and other penalties and saved $250,000 in annual costs by eliminating redundant services while also reducing the risk of finger-pointing due to overlapping roles.

"DURING A CYBER BREACH IS NOT THE TIME TO BE MAKING NEW FRIENDS."

In the middle of a cyber breach, you want to know the experts who will serve you and already have relationships firmly in place.

(continued)

Pre-determine staff responsibilities and timelines

Have a checklist that outlines the key decisions that will need to be made, who is responsible, the criteria for making those decisions, and the timeline. This will help you avoid gaps and duplication of effort.

Plan communications strategies in advance

Know what you want to disclose when, and whom to contact. Establish attorney-client privilege early on; although you will want to document your response, anything that you communicate before you've brought on counsel can be discoverable in legal action. Planning can help you avoid releasing hasty or inaccurate statements while still keeping customers and the public informed.

Practice your response plan regularly

Educate management and employees on cyber security; they are the front line in protecting your business. Also hold tabletop exercises to practice your response and reinforce responsibilities. Then refresh periodically to account for personnel turnover and changes to the threat environment.

Plan to follow up on lessons learned.

After an immediate crisis is over, analyze any areas where there were delays or lack of clarity. Use that information to revise your checklists and practice drills to improve future responses. Also critical is a plan to harden your systems to avoid similar breaches.

KEYS TO DEVELOPING A ROADMAP TO CYBER RESILIENCE

- **Your vulnerabilities:** Do you know the threats and your company's weak spots?
- **Your responsibilities:** Do you know your regulatory and contractual obligations?
- **Your breach response service providers:** Do you have contracts already in place?
- **Your staff responsibilities and timelines:** Do you have checklists that delineate who is doing what, when?
- **Your communications strategies:** Are they planned in advance?
- **Your response plan training:** Are you practicing it regularly?
- **Your follow-up:** Are you analyzing the aftermath to harden your systems?

More Information

To learn more about how NextLevel can help you develop a roadmap for cyber resilience, call us at (800) 833-NEXT (6398) or email info@nlbev.com.

nextLevel
BUILDING ENTERPRISE VALUE