Cybersecurity Law Report
An Acuris company

cslawreport.com

September 16, 2020

BOARDS OF DIRECTORS

Twelve Steps for Engaging the Board of Directors and Implementing a Long-Term Cybersecurity Plan

By Brian Craig, *Lewis Brisbois Bisgaard & Smith*

After a serious cybersecurity incident (think a paralyzed encrypted network or ruinous business email compromise), you'll want to outline the path to "never again" for the top of your organization. To make successful, measurable, long-term cybersecurity happen, it will require top-down support and significant resources. The following is a 12-step "cheat sheet" for effective board engagement after an incident.

See also "How CISOs Can Use Digital Asset Metrics to Tell a Coherent Cyber Story to the Board" (Jun. 3, 2020).

1) Use the Momentum

Once the breach coach, forensic analysts and IT team have resolved your immediate cybersecurity nightmare, everyone will be sold on the business need for something different. This is the moment to propose a top-down board-level cybersecurity solution. Tell the board you plan to conduct a detailed security audit and to measure progress as you close all identified gaps to achieve an industry-standard cybersecurity certification for the organization. With a broad "go-do-it!" consensus, you will have the support you need to execute the plan outlined in the next eleven steps.

Set expectations with the board that cybersecurity is a continuous evolution and that an effective plan will need to be durable, but the plan will enable the business to obtain an organizational cybersecurity certification. The certification process could be 18 months long, so secure the board's commitment to support the entire journey with sufficient financial and human resources.

2) Leverage Your "A" Players

The incident response team that just rescued the company may be the best place to start looking for human resources for a long-term response plan. Set up a team meeting and include the following internal and external professionals to help the company's resiliency.

- An external cybersecurity lawyer is perfectly positioned (especially after participating in your breach response) to assess risk, manage project execution, engage the board and the C-suite, assert legal privilege, and lend significant gravitas to changing organizational cybersecurity behavior.

©2020 Cybersecurity Law Report. All rights reserved.

- The external forensics and incident response squad that just learned where the bodies are buried and has cutting-edge threat knowledge and tool sets that some in-house teams lack, is a great resource to conduct the initial post-incident cybersecurity certification scoping audit (gap analysis). These professionals can also execute penetration testing, red team reviews and other initiatives during the months it will take to address all the gaps.
- Your internal IT team ensures progress, compliance and that the network functions properly. This team has a big stake in the success of an incident-response plan initiative. Assemble the team so you know who will be accountable for all of the tasks it will take for delivery. Without them you cannot reach certification.

3) Ring-Fence the Budget

Security can be a verbal priority but the budget to achieve it is an afterthought. Moreover, various members of the C-suite will hold different parts of the budget. The general counsel, chief financial officer, chief human resources officer and chief information officer may all lay claim to budgets and initiatives with critical cybersecurity implications. After a crippling data incident, however, you will have everyone's attention. So, use this opportunity to gain the commitment across budget-holders and ask for the money needed to succeed. Then, make them stakeholders in your success and brief everyone monthly on the progress against the plan.

4) Change the Way You Describe the "Problem"

Cybersecurity issues are often perceived by boards and execs as a technology problem. This is because cybersecurity is usually driven by the IT team as a budget line item (often for hardware solutions) as opposed to an enterprise-wide compliance challenge. Yes, you might need new end-point detection and response tools, but you will also need to change the way people take responsibility for security. This will take a cultural change within the organization.

In your plan, everyone will have a heightened level of security awareness through training and therefore be contributors to enhancing your security posture. Knowing how to spell "phishing" is just a small part of the change. You will need to change board-level thinking from "this is a technology problem" to "this is a people problem," and use your A-team to help deliver that message.

5) Make Progress Steady and Measurable

Just as it takes more than 15 minutes to "crash-stop" an ocean-going super tanker, it will likewise take time to change your cybersecurity. Create a plan that will last 18 months or longer so you have time and the long-term commitment to succeed. This will also allow you to spread costs out over time and have the time to assess progress, since the ability to measure your progress will inform future decisions. The company directors and the C-suite care about achieving business goals, but they will not support a plan without measurable progress points along the way.

©2020 Cybersecurity Law Report. All rights reserved.

Steady progress is also more likely to change organizational culture so that cybersecurity becomes second nature.

6) Conduct a Risk Assessment

Consult with your A-team to understand which security standard fits your organization's business by analyzing risks. A comprehensive post-incident audit will set the scope of the task ahead and help identify what needs to be done. Some of this work has already been done as part of the incident response, but you will need to take it a step further. Maybe it's Cyber Essentials Plus, NIST 800-171, or ISO 27001. Regardless of the standard you choose, you will have an objective measure of success and your progress plan can be easily charted. Now, use your A-team to determine how far off the standard you are and develop your plan to get there.

7) Mind the Gap

Following the initial post-incident risk assessment audit, identify the gaps in compliance against your chosen cybersecurity standard and plan to bring the company into compliance by addressing deficiencies to achieve certifications. Because this usually involves a shake-up in the "way things have always been done," it is best to use your A-team, as opposed to internal staff, to help push forward needed changes.

8) Stay Realistic

Use your detailed gap analysis to set a realistic budget for your plan. Consider a subscription model where the budget is committed up front but is only payable with each monthly deliverable to prevent budget erosion. With the work and costs spread over 18 months, ideally in equal installments, there will be a measure of budget certainty and a cadence of progress. Conducting regular meetings with stakeholders also helps to keep everyone informed and on plan.

9) Generate and Protect Progress Reports

The board will thrive on a dashboard-style report that shows progress and challenges, and measures success. Your C-suite will need a different level of granularity to support the program in areas that impact their budget contributions or bailiwicks. Communicating progress to employees at large will also help them invest in the initiative. Your A-team should produce draft reports for you and be available to present at board or C-suite meetings. Treat these reports as privileged. The cyber lawyer on your A-team can help with confidential communications and with preserving privilege where it applies.

10) Consider Any Regulatory Overlay

Federal and state legislation set forth various requirements for information security programs, data breach responses and other cybersecurity-related activities. The New York State Department of Financial Services' Cybersecurity Regulation is a great example. The cyber lawyer on your A-team can work with your GC and IT team to ensure that your operations comply with all applicable laws, while allowing the GC and internal IT staff to manage cybersecurity measures on a day-to-day basis.

©2020 Cybersecurity Law Report. All rights reserved.

11) Review Trading Partner Contracts

Your A-team is in a good position to analyze the risks associated with potential breaches of your trading partners' networks. Determine whether your trading partner contracts protect your business in the event that a trading partner suffers a data breach and adjust contract provisions as necessary.

12) Train Employees and Monitor Cyber Measures

As part of an ongoing cybersecurity program, your business will benefit from delivering training to employees at all levels on an ongoing basis. Engaging your A-team to stage mock data breach scenarios and lead related discussions will educate your employees, thereby bolstering your company's overall cybersecurity. Your A-team may also work with your internal IT department to conduct penetration testing, assess perimeter protection, review information security policies, and implement system hardening measures.

Brian Craig is a partner in the Washington D.C., office of Lewis Brisbois and a member of its data privacy and cybersecurity practice. For over 25 years, Brian Craig has been helping senior executives and boards of directors manage risk and compliance challenges, including responding to serious data breach incidents and implementing cybersecurity and data protection compliance programs in industries with data, engineering, financial and regulatory components, such as consumer goods, telecommunications, information technology, financial services and defense.

©2020 Cybersecurity Law Report. All rights reserved.