The cyber incident response plan: The power is in the process

May 31, 2022

Life is a journey, not a destination – and the same can be said of the cyber incident response plan.

A plan is worth only as much as the process put into it

Every cyber expert, regulator and standards body will say you should have a cyber incident response plan. We agree. What these authorities don't tell you is that not all plans are created equal. Without the proper process, most aren't worth much.

Too many organizations approach preparing incident response plans focusing on the deliverable. They want a cyber incident playbook they can dust off and rely on in the heat of crises.

An incident response plan is better conceived of as a vehicle for issue identification, problem solving, collaboration and continuous learning. The true value of an incident response plan comes from the act of preparation itself, if – and only if – you prepare it the right way.

What is a cyber incident response plan?

An incident response plan is a documented set of procedures that spells out how an organization will respond to a cyber incident. It establishes the internal decision makers and external incident response team, including legal, forensics and communications. It plays an important governance function, establishing roles and responsibilities and empowering the team to make important decisions. It identifies the different phases of response – containment, investigation, remediation, mitigation and closure. An incident response plan is a practical tool that provides concrete steps to take and organization-specific issues to work through. Good plans include key information such as contact information, contractual and statutory notification obligations, and so on.

A plan may be required

Many organizations are required to have a plan by either regulation or contract. For example, the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) standard requires responsible entities to have incident response plans for certain systems. Other organizations have agreed to have a plan in place as part of a cybersecurity rider to an important contract.

How do most organizations prepare plans?

The pressing need for an incident response plan invites the problem: organizations assign work, compile templates and pay experts for input. Oftentimes, a technical person who has good knowledge of incident response prepares the draft, using a template from a vendor.

We know this is the case because we are often asked to review draft incident response plans. We engage by analyzing plans for consistency with regulatory standards and guidance, alignment with general incident response practices, and logic and clarity. We mark up drafts, as lawyers often do. Our engagement adds some value, but building your plan this way only gives you a document – the real opportunity to support incident response readiness has been lost.

There is a better way to plan

We propose that all organizations engage in what we're calling a "facilitated plan review."

We advise you do the following, and do it now:

- Assemble the incident response team and work through the draft in a series of meetings, ideally with facilitation by experienced incident response counsel;
- Methodically go through each part of the plan and incident response process – containment, investigation, remediation, mitigation and closure; and
- Confirm what the plan means to individuals in practice, what issues it raises, what's missing and how it needs adjusting.

By undertaking the above process, you will identify issues unique to your organization that no template will contemplate. You will test your plan against the typical requirements and constraints of incident response practice (provided by your expert facilitator). And, most importantly, you will develop a shared understanding of the plan among all team members, enhancing your readiness. Done well, the learning is palpable and the experience energizing.

If legal counsel facilitates, the sessions will be privileged, and you will flag legal issues and incident response pitfalls as you go. Your team will take careful notes and amend the plan, either as you go or at the end of the process.

The cost of this more engaged process is the time spent by the team members and, if you use legal counsel, legal fees. That being said, the process is both high in value and essential to your organization's cyber incident response readiness.

Conducting a facilitated plan review is the first step to getting ready. Only after this process should you invest in a tabletop or paper drill exercise. You can then use tabletops and paper drills to develop playbooks for various scenarios, adding to the teams' documented learning. Then revisit parts of the plan periodically, again using a discussion-based format. In between these sessions, create a knowledge-sharing platform for team members to share information about cybersecurity developments.

Takeaways

We encourage you to conduct a facilitated plan review to support continuous learning and true cyber incident readiness. This should be your desired outcome, not the plan itself. When your team faces its first incident, the plan will only be as good as the team tasked with implementing it. If your team has developed the plan with the rigorous process outlined above, you will be ready to address the unknown and chart a course to the optimal response.

Reach out to Dan Michaluk, Eric Charleston, or your regular BLG lawyer if you have questions about preparing a cyber incident response plan.

By

Daniel J. Michaluk, Eric S. Charleston

Expertise

Cybersecurity, Privacy & Data Protection

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749