How to Create Your Cyber-Incident Response Plan

By Sandra Anderson and Anne Lockner
InsideCounsel
July 25, 2016

You keep hearing it— it is not a matter of whether a cyber-security incident will hit your company, but when. An incident can include a number of events, such as suspicious network activity; theft or loss of physical assets like laptops, phones, or thumb drives; malware; credit card theft; phishing attempts; ransomware; or website defacement. Are you ready for any of these? Does your company have a response plan? Is it written down? Are others aware of it? Has it been tested?

These are all things that you should do now, rather than wait until you are forced to make up a plan as you go. But how do you do it? It isn't easy. It is not something you can buy off the shelf.

Any response plan worthy of being relied upon must be custom tailored to your company and regularly updated as threats, technology, and your company evolve. This article provides you with a starting point on how to create such a plan.

Choose a point person.
The response team point person will be in charge of overseeing the execution of the plan, communicating with the incident response team, and directing members of the team as necessary. This person should be a lawyer. This will allow your communications to be kept privileged while you investigate and decide how to handle the matter. In addition, lawyers are often the best equipped to evaluate the risk assessments that companies face when a cyber incident occurs.

Determine who your response team should consist of.
The team should ensure that you have the knowledge, political capital, and skills to accomplish what is necessary while at the same time remaining nimble enough to move quickly and decisively as events unfold. The membership of these teams will vary depending on the company, but should include representatives from the following teams: executive, IT and security, legal, operations, and public relations. Others to possibly include might be representatives from your finance and HR departments.

What data do you have and where is it?
This is a crucial element of any cyber–incident-response plan, but also one that in-house lawyers are rarely able to oversee on their own; they need to work with members of the IT department to ensure this portion of the response plan can be operationalized. The first step is getting an understanding of what kind of data the company has and which of that data carries the most risk. Employee and customer data, including point-of-sale credit card data, all contain Personal Identifiable Information (PII) that could cause numerous problems if it were misappropriated.

Trade secrets, financial, and other competitively-sensitive data are other categories that are likely targets. Once you know what data you have, you need to know where it is stored. For instance, does your company host it or does a third party?

Who is preventing an incident from happening and detecting one when it does?
The best plans are ones that detect and halt efforts to infiltrate your computer system in the first place. Companies often outsource this role to third-party security firms who specialize in protecting your systems and detecting intrusions. These experts work with the company's IT group and the company's other third-party hosting vendors to monitor systems for any items of concern and then respond accordingly.

Containing and investigating the incident.
Upon learning of an incident, consider the threat level of the incident. What kind of data was at risk? Is it proprietary or confidential, or does it contain PII? Or is it irrelevant or public information? You'll likely want to have your security firm investigate all incidents regardless of how mundane the data is that was compromised because such an incident could serve as a backdoor for a broader and more damaging breach. Any incident that resulted in the compromise of sensitive data should be investigated forensically.

You will likely want outside counsel to hire a forensics firm to maintain confidentiality. But keep in mind that if credit card data is implicated, you may be required to disclose this fact to your acquiring merchant and credit card brands that you accept. And they may require you to hire a forensics firm that is certified by the PCI Security Standards Council (known as PFI-certified firms) to conduct an investigation. There are relatively few PFI-certified firms and, following the law of supply or demand, they can be very costly.

Legal plan.
There are numerous legal aspects to an incident response plan. What jurisdictions are in play? Is notice required (law enforcement, customers, Attorneys General, third parties)? Are there any indemnity rights or obligations? Does the company have any legal exposure resulting from the incident and, if so, to what extent? Does the company have any cyber insurance? There are several steps a company can take early on to avoid or at least mitigate legal exposure and they should all be considered as early as possible.

Test your plan — on your terms.
One way to test your cyber-incident-response plan is to wait for an incident and see how it works. We don't recommend that. The far better option is to undertake a table-top exercise that allows you and your team to walk through a hypothetical incident to identify any weaknesses.

Is there confusion as to who is calling whom at a vendor? How will you navigate privilege issues if a third party you must deal with to contain the breach turns out to be an entity that could be adverse to your client? Can the team even find the plan you worked so hard to develop?

There is no plan that will address every event that could occur. Rather, it is intended to position you and your team to communicate effectively and respond appropriately.

It also helps to develop an understanding of your priorities based on an objective assessment and not an assessment made under extreme conditions. By being proactive in creating a plan, you can ensure that the company — and its customers, employees, and investors — are adequately protected.

First published on InsideCounsel, July 25, 2016