Building Your Cyber Incident Response Plan

EVERY COMPANY should have a cyber incident response plan. The question is no longer if a data loss may occur, but when. Therefore a companies should have a clear, communicated, written and practiced plan in place before any incident occurs. Small and medium sized businesses can no longer assume that they will escape the impact of data security breaches. In fact, most small and medium sized businesses have already been victims of cyber-attacks. Companies often don't pay attention to cyber security issues until some major incident happens. More than 60% of businesses surveyed by AT&T had an IT security breach in 2015, and 42% of those organizations said that the breach had a significant negative impact on their business. Yet only 34% of organizations believe that they have an effective incident response plan.

Incident response plans provide risk management benefits to organizations, help to fulfill legal obligations, and aid in recovery and the resumption of operations. A thoughtful reaction to data loss will result in better decision-making and will minimize risk and loss. Moreover, such plans are often required by law or contractual obligations. A good plan is good business – it's the right thing to do and it helps to build and protect your brand.

How should you start?

- Identify and locate your data. Companies should inventory the information and types of data that they collect or possess. They should identify and document the location and method to access this data, and categorize it based on criticality or sensitivity.
- Evaluate the data held. Is there a legitimate need for collecting it or continuing to store it? Does it serve a fundamental business purpose or a clear marketing purpose?
- Reduce and eliminate unnecessary data. Whenever possible, limit the scope of collection and reduce storage to the bare minimum to achieve the limited purpose for which the data was collected. Implement a systematic, routine program for destroying data.
- Secure the company's network and the data located on it – Place components of network in locked space. Evaluate other security options and policies.
- Form a team to develop the plan. The incident response team should include key people with authority and availability. Each member should be assigned distinct responsibilities and have authority to act within scope of his or her assignment.

Once you have identified the data and handling practices and have formed the team, the real work starts to prepare the plan.

- Identify necessary outside resources, which are often legal, technical and public relations. Remember that the business must continue to operate during the incident, so internal resources may be limited. Also, internal experience may be limited.
- Meet at least monthly to prepare and make decisions in advance of an incident.
- Pre-draft important communications. These should include a notice that will be posted on the company's website, reminders to employees about company policy regarding communicating with the media, and press releases.
- Plan what to do if the email system becomes unavailable.
- Evaluate your cyber insurance coverage. Does it cover remediation costs or just liability? Does it cover incidents or merely "breaches," and is the definition of "breach" sufficiently broad? Will it respond to losses due to fraudulent actions of others or attacks by state actors?
- Impose contractual obligations on third party contractors, including the obligation to notify you in the event that they become aware

of a cyber incident and to cooperate in any investigation.

- Evaluate capacity for handling a call center.
- Identify criteria for notifying law enforcement and regulatory agencies.
- Identify clear roles for each team member, including who is the primary point of contact, who will physically secure premises, and who will isolate affected equipment.

Plans are no help when they merely sit on the shelf. The team should review the plan on a regular basis, at least annually, and should run tests and simulations, also called tabletop exercises, to make sure each team member knows his or her role and to look for ways to improve or tighten the plan. Personnel will need to be trained in their responsibilities

When a cyber security incident strikes, you should be prepared. Immediately alert the Incident Response Team and take steps to fix the problem. Document the date, time, location, duration and remediation efforts related to the incident. Isolate the affected equipment and safely take it offline. Take precautions to preserve physical and electronic evidence and secure the premises. Remove hacker tools and malware. Include legal where appropriate to preserve attorney-client privilege during the investigation.

Notify all necessary company employees and vendors, and then begin implementing next actions. Identify the person who discovered the incident and get a statement from that person that includes as many details as possible. Determine what type of data was compromised and develop a list of affected company departments or individuals. Confirm whether data was deleted, modified, encrypted or viewed. Inventory equipment and confirm whether any is missing.

After the emergency phase, the next stage of incident response will involve notifications, press releases, law enforcement, review of contractual obligations, and update of company policies. Discuss the breach with outside counsel and other service providers. Determine whether to notify law enforcement or administrative agencies. Consider whether third parties have obligations to the company based on their actions or inactions. Discuss if a press release or public notification will be made and when. Review employee actions to determine whether a violation of law or policy occurred.

The best way to handle any emergency is to be prepared. By following the steps above, you can be sure of three things: you're not secure (even the best security is subject to breach), and you're not done (information security requires constant vigilance), but you have gone a long way toward ensuring that your business can recover from a cyber incident with a minimum of risk. ■

William R. Denny is a Partner at Potter Anderson & Corroon LLP in Wilmington, Delaware. Mr. Denny's practice includes cybersecurity, data privacy and commercial litigation.