PUBLICATION

Ready, Set, Go: Preparing and Testing for Data Security Events

Authors: Zachary B. Busey, Samuel Lanier Felker
October 20, 2017

Baker Donelson's Data Protection, Privacy and Cybersecurity attorneys are pleased to continue a series of client alerts that address significant cyber-threats to your business and discuss ways you can protect your business with thoughtful and timely planning before an emergency arises. Proper planning includes recognition of the threats, assessment of the risk, and then examination of the facts and tools at your disposal to mitigate the risks. The series will address your options, from adopting appropriate IT policies and procedures to acquiring contractual indemnity and insurance for specific loss risks. When there is a recommended technical solution available, we will consult with leading expert vendors and provide their input. We often hear that in today's tech environment, it's not a matter of whether you will be hacked or attacked, but when; therefore, we want to help you be well prepared for future challenges.

Our series will help you get ahead of the game. We offer guidance on shopping for cybersecurity insurance; protecting your business from DDoS attacks (Distributed Denial-of-Service attacks) and ransomware; establishing a smart data management plan; evaluating vendor relationships; handling disgruntled employees and other internal threats; and testing for data security events.

Preparing and Testing for Data Security Events

Target, Ashley Madison, Sony, Home Depot – the data security events at these companies define the last few years of data security. With 2017 nearing an end, the IRS, Equifax, and the SEC have joined this list. These events draw our attention because they are large-scale and highly publicized. Absent from this list are the thousands of events impacting day-to-day operations of companies across the country. In today's tech environment, it's not a matter of if your company will experience a data security event, but when and to what degree. Is your company ready?

Companies prepare for events all the time: power outages, product launches, hiring and firing of staff, inclement weather, theft, media announcements, etc. While companies do so in different ways, from large scale to small, the steps are the same: (1) identify potential security events; (2) develop a plan; (3) review and test the plan; (4) revise the plan; and (5) repeat as needed.

Identify Potential Security Events

When it comes to data security, identifying potential security events starts with knowing the data a company has and where it is stored. Say, for example, a company keeps hardcopies of personnel and employee medical files. Those files could be copied or physically taken. At the same time, when a company's website is susceptible to a DDoS attack, their wireless devices can be overtaken and used during that DDoS attack. Electronic data can be copied by employees or stolen by hackers, as the system has become unsecure. Additionally, electronic data, when shipped or transmitted – whether internally or externally – can be intercepted. Finally, an employee could click on a malicious link or download a file which would allow outsiders access to the company's system. The scope and severity of the event(s) will vary based on the size of the company and the nature of their business.

Develop a Plan

Your plan has two parts. The first part is prevention. The hard copies of personnel and employee medical files should be secured in locked file cabinets and in a file room to which access is monitored and logged. Website traffic should be evaluated and additional server resources should be available in the event of a DDoS attack. Wireless devices should be protected by passwords, preventing their use in a DDoS attack. A company's most sensitive electronic data ought to be encrypted. Networks should be secured with passwords; and access should be monitored and logged. Third-party providers and outside holders of electronic data should sign agreements affirming the implementation of controls and security, and employees should be trained and regularly reminded to avoid malicious links and downloads.

The second part is reaction. When a hard copy file is stolen or electronic data is copied, a company has to know who to notify, internally, externally, or both. In the event of a DDoS attack, an individual or provider has to be told to allocate additional server resources. Statutes and regulations also drive reactions, often requiring companies to notify state agencies, consumers, or both in the event data is stolen. A reaction plan should include when legal counsel is consulted. Engaging counsel early in the process better positions a company to maintain confidentiality over certain communications about the event.

Review and Test the Plan

It seems obvious, but a plan should be reduced to writing and distributed to those involved. Your plan should also be reviewed by those involved, including legal counsel. Like any workplace policy, those involved should acknowledge in writing their receipt and review of the plan. This written acknowledgment provides the basis of discipline, up to and including termination, should an employee or third-party vendor fail to execute their responsibilities under the plan.

Testing the plan is vitally important. As with every part of this process, the extent and sophistication of any testing will vary from company to company. Testing can be simple, such as talking through reactionary measures on a call or in a meeting. A company, however, should not stop at simple. More sophisticated testing has become commonplace. Companies need to simulate events, and whether staging a file theft or a hacking incident, companies need to experience these events in real time. Penetration testing (or pen testing) can be utilized. Pen testing is typically done with the assistance of a third party and often without company employees knowing the test is occurring. The goal of a pen test is to determine vulnerabilities in a company's systems and network. Common approaches mimic hacks and other cyber events, such as DDoS and brute force attacks. Other examples include staging the theft of a hard copy file, sending an email to test whether employees click malicious links, or calling employees to see if they provide access credentials.

The harder a company tests a plan – i.e., closely simulating real-world, real-time scenarios – the better a plan will be. Briefings for board members and the c-suite help companies ensure that these issues are taken seriously and given the necessary resources. The ultimate goal is to identify strengths and weaknesses of any plan, and then develop options for emphasizing strengths and addressing weaknesses.

Revise and Repeat

A plan's first draft should not be the only draft. Through testing and review, plans should be revised and updated. In general, this process should be repeated regularly. It must be repeated each time technology is updated, a company decides to retain a new category of data, or a company begins storing data in a different way. If you have any questions or would like additional information regarding event planning and testing, please contact Zachary Busey, CIPP/US or any member of the Firm's Data Protection, Privacy, and Cybersecurity Team.