LINDABURY

McCormick, Estabrook & Cooper, P.C.

Attorneys at Law

Who is Part of Your Company's Breach Response Team?

As a potential target of a hack, do you have a response team and plan in place to respond?

Cybersecurity & Data Privacy

Responding to a Cybersecurity Breach — Establish Your Response Team

It is a day that virtually every business owner fears, when you receive word from your IT department that your company's computer system has been hacked. A million thoughts rush through your head, but they all come back to one question: *what do I do right now to protect my company, my employees and my customers?* The answer is may seem daunting, but an answer does exist.

Establishing Your Cyber-Response Team

1. The first step to be taken upon learning of a cyber-breach is to understand what type of breach occurred.
   - employee negligence like losing a laptop or flash drive containing personally identifiable information ("PII") or protected health information ("PHI")
   - malicious insider behavior, such as the disgruntled or dishonest employee who steals company information
   - perhaps the most wildly publicized breach as of late, hacking and cybercriminal activity

2. In order to understand what happened and how best to react, assemble a team of cybersecurity professionals who can assist with all facets of the cyber-breach. This means engaging individuals who possess expertise in Information Technology and are experienced in evaluating the severity and scope of a cyber-breach.

3. Do not attempt to cure the cyber-breach on your own such as by running anti-virus software, as that may cause more harm than good. Cybersecurity response professionals possess unique training and experience that allow them to:
   - identify the type of cyber-breach
   - craft a response to preserve or restore lost data
   - possibly unlock data that has been "captured" by malware such as a Ransomware attack
   - preserve the evidence of the cyber-breach (which may become invaluable to the defense of any subsequent litigation that may arise)

4. Consult with legal counsel to determine what laws and regulations are implicated by the cyber-breach and what type of response is warranted. Depending on the nature of the breach, different state and federal laws could be implicated, which will guide how to respond to insure that the response itself will pass governmental scrutiny.

   New Jersey Law
   - defines a "breach" as occurring when customer's personal information was or is reasonably believed to have been accessed by an unauthorized person. N.J.S.A. 56:8-163(a)
   - disclosures must be made with contacting the Division of State Police, Department of Law and Public Safety.

5. Involve executives, department heads and human resources to help determine which employees' and customers' respective information has been accessed and how to communicate that information to them.
   - Keep your own employees advised of the breach to insure their own privacy concerns are protected
   - Keep in mind that someone must be prepared to explain to your employees how to respond to inquiries from customers as well
   - It may also mean engaging public relations professionals to craft a response to the public, as a poor response to a question from the media can be damaging to your company

Plan for the breach before it ever happens and partner with the people who can properly respond on your behalf. Establishing a cyber-response team before any attack ever occurs provides a company with the agility to move quickly and a response team to assist you in determining if there was a breach of personal information, thereby improving your chances of satisfying any legal notice requirements should that fateful day arrive.

For Specific Questions Concerning Your Company's Cybersecurity, Please Visit lindabury.com or Call 908.233.6800 to Speak to Any of Our Cybersecurity & Data Privacy Attorneys