Blogs
December 18, 2018
Is Your Business Prepared for Holiday Hacking?

There is often an upsurge in hacking and online scams during the holidays, and businesses are not always prepared to respond. Here are five key steps you can take immediately to protect and defend against breaches:

1. **Image your systems.** Image your systems as soon as possible and retain this data for at least 90 days. It is critical to be able to capture the system before infiltration in order to detect all signs of unusual activity, and thus determine the full scope of the breach. Having a "pre-holiday" image gives you something to compare to if a breach happens over the holidays. It also allows a forensic investigator to conduct a truly independent investigation, which can lend credibility to your own internal investigation.
2. **Monitor signs of unusual activity.** Maintain the same level of IT coverage as you normally do in order to monitor and detect signs of unusual activity. There may be a tendency to have minimal IT staff over the holidays, but in the event of an attack, this makes your business vulnerable and less likely to identify an infiltration early. Though employees tend to take time off during the holidays, ensure your business has adequate staff coverage to monitor key systems, even if it needs to be done remotely, or ensure that temporary IT staff are adequately trained.
3. **Be ready to follow your incident response plan.** Make sure you have an incident response plan, even if it's in draft form, and be ready to follow it. Incident response plans reduce confusion post-incident and lower costs. In addition, regulators may look to this in the case of an investigation after a security incident or breach, as well as whether or not your business exercised reasonable security more broadly.
4. **Identify an alternate communication method in case your systems are compromised.** Coordinate an alternative method of communication in case your systems are unavailable or compromised. Anticipate that you may not be able to communicate electronically, and establish a designated phone number or other method of communication and circulate it to members of your control team (the key players who will be involved in responding to the security incident).
5. **Be ready to contact outside counsel and forensic investigators.** Know the numbers of your outside counsel and forensic investigators and contact them immediately. Prompt investigation best positions you to understand the incident, and certain types of data exposure implicates legal notification requirements, some of which occur under tight deadlines. Outside counsel can advise you on the requirements with which you must comply and in what time frames, as well as how to provide notice in a way that minimizes negative publicity and litigation risk.

Authors

Explore more in

Privacy & Security