It's Not 'If', It's 'When'

Is Your Business Ready to Respond to a Data Breach?

Taylor Gast

Greater Lansing Business Monthly
August 8, 2017

AUTHORS/ CONTRIBUTORS
Taylor A. Gast

PRACTICE AREAS
Cybersecurity and Data Privacy
Technology Law

It's 4:00 p.m. on a Friday afternoon when I receive a call from a company 's legal director. The director tells me that a company executive was traveling when the executive received an urgent email that appeared to be from the company's CEO, asking for a document containing sensitive information of all the organization's employees. After forwarding the requested document, the executive realized that the email was not from the CEO's email address, but from a similar address- now a criminal holds sensitive information.

Unfortunately, this scenario and its variations are the new normal; cybercrime now represents the second-most reported economic crime. Local businesses that fall victim to cyberattacks often assumed that they were too small to be a target, or their IT security was strong enough to protect them.

SHIFTING THE FOCUS FROM PREVENTION TO PREPARATION

The reality is that all businesses are targets of cybercrimes, because all businesses hold some degree of sensitive employee or customer data . Businesses are also increasingly compromised by diverse types of breaches such as ransomware, which is designed to lock down company files until a ransom is paid. Whether a cyberattack involves phishing like the beginning scenario, ransomware, wire transfer fraud or one of many constantly evolving threats, businesses often feel serious and long-lasting damage.

While relying solely on installing preventative measures previously seemed sensible, companies are increasingly focusing on the strength of their incident response plans. A comprehensive and practiced plan can be the difference between a relatively inexpensive remediation and an incident so costly, time-intensive and harmful that business operations or reputation may never recover for a company.

INCIDENT RESPONSE PLAN BASICS

Each business's needs and issues are unique, and the best time to prepare for a data breach is still before one occurs. We recommend that businesses considering their incident response plans start with the following basic considerations.

1- HIRE AN ATTORNEY

Although the affected company is a victim of a crime, many cyberattacks subject the company to its own liability. The company may find itself a defendant in lawsuits brought by everyone from consumers and shareholders to credit card companies . In a lawsuit, all relevant internal communications and documents are available to the other parties in discovery. However, engaging an outside attorney as soon as possible after a breach can, if properly structured, prevent undesirable disclosure of sensitive communications and work product, as well as communications with breach remediation vendors.

2 -REMEDIATION: ACT FAST

The business should quickly determine the nature and scope of a cybersecurity incident to remediate it. When necessary, the company should contact an IT vendor to investigate and fix the problem. The company should also ascertain whether data was exfiltrated - copied, transferred , or retrieved from a computer or server- which is important in determining the company 's legal requirements after a breach.

3 -RANSOMWARE: SHOULD YOU PAY?

Although the most common question is whether to pay the ransom, there lies no easy answer. We suggest weighing the value of the encrypted files against the possibility that the attacker refuses to decrypt them or leaves a "backdoor" open for future attacks. The business should consider whether data recovery options or insurance for cyber-based incidents might help. If the business pays the ransom, it's also worth discussing with a tax attorney whether that ransom is deductible.

4 -BREACH NOTIFICATIONS

Most states, including Michigan , have passed data breach notification laws requiring businesses that experience a data breach to notify affected individuals. State laws differ in which incidents require notification, how quickly notification must be sent and whether any other action is required, such as notifying a state agency. Often, we must consider several states' laws when a business has customers or employees across the nation.

5- *DAMAGE CONTROL*

Throughout and after the remediation process, the company should consider reputational harm, both internally among employees and externally among customers and vendors. The reputational effects of a data breach are often more long-lasting than others.