Chicago Daily Law Bulletin®

Volume 162, No. 244 Serving Chicago's legal community for 161 years

So your company has been hacked — now what? FTC offers some guidance

This year has been a rough one for data breaches, proving that even the most sophisticated companies, from social media companies to technology giants, are not immune.

In March, hackers tricked an employee at Snapchat into e-mailing them sensitive personal information belonging to 700 current and former employees and stole information belonging to approximately 1.5 million customers.

In May, LinkedIn saw 117 million e-mail and password combinations stolen in 2012 published online. And this year hackers stole information belonging to approximately 1.5 million customers of Verizon Enterprise Solutions, which ironically provides IT services and data breach assistance to businesses worldwide.

And in September, after multiple media outlets reported on the story, Yahoo confirmed that it suffered the biggest data theft of all time from a single website, when a hacker working for a foreign government stole personal information, including users' e-mail addresses, passwords, full names, dates of birth and telephone numbers, from at least 500 million Yahoo user accounts in late 2014.

Even federal agencies aren't adequately immune. In February, hackers breached the U.S. Justice Department's database and stole information on 10,000 Department of Homeland Security employees, and a subsequent attack on the Internal Revenue Service compromised the personal information of more than 100,000 American taxpayers.

That huge data breaches involving consumers' personal information make headlines is clear. What's less clear, from the perspective of businesses, is what steps hacked organizations should take to address and remedy their situations, whether they're in the middle of the hacking crisis or discovering data breach long after the fact.

No comprehensive federal law governs data breaches; 47 states (and the District of Columbia, Puerto Rico, the Virgin Islands and Guam) each have their own laws governing the responsibilities of businesses and other organizations.

While the requirements vary significantly — and a number of states amended their data security and breach notification laws this year, as a result of the increasing numbers of data breaches — each of these states requires some form of notification to consumers and government agencies in the event of a data breach.

To guide companies handling data breaches and notification requirements the Federal Trade Commission recently released "Data Breach Response: A Guide for Business."

The new guidance provides details on how to secure the organization's systems, address the breach and notify the parties involved. The agency also offers an accompanying video on how to handle a data breach.

As soon as a data breach is discovered, the FTC recommends that the first order of business is to quickly secure operations by mobilizing a breach response team to prevent any additional data loss. The actual steps will depend on the size and nature of the company as well as the scope of the data breach. But, in general, the FTC advises securing all physical areas potentially related to the breach and changing access codes.

All affected equipment and hardware should be taken offline — although machines shouldn't be turned off until investigators have a chance to examine them. If any data has been improperly posted online, remove the information and contact search engines to be sure the posted data has not been stored or cached.

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law, as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.

An effective breach response team should include representatives from the legal, information security, information technology, operations, human resources, communications and investor relations departments, according to the FTC. An organization may consider hiring outside forensic investigators to determine the source and scope of the breach, collect and analyze evidence and outline next steps to take.

"Good communication up front can limit customers' concerns and frustration, saving your company time and money later ..."

Regardless of who is conducting the investigation, the FTC recommends consulting legal counsel with privacy and data security expertise who can advise on federal and state laws that may be implicated by a breach.

The breach response team, whether internal or external, should interview the individuals who discovered the breach as well as employees who may be affected by the breach, such as customer service staff.

The next step is to work with forensics experts to fix the vulnerabilities caused by the data breach. The FTC suggests starting off by asking the following questions:

- What types of information was compromised?
- How many people were affected?
- Were security measures such as encryption enabled when the breach occurred?
- Was the company's network segmentation plan — a setup to keep a breach on one server from leading to a breach on another server — effective in containing the data breach?
- Who had access to the data at the time of the breach and was such access necessary?
- What remedial measures are recommended by the forensics experts?

The company should also look at any service providers involved to determine if they had access to personal information and whether their access privileges should be limited. This is also a good time to audit the actions service providers are taking to guard against any data breaches.

A communication plan is key to reach all affected constituencies, including employees, customers, investors, business partners and others that may be impacted.

"Good communication up front can limit customers' concerns and frustration, saving your company time and money later," the guide advises. What information should be released and when requires balancing the need to prevent disseminating misleading or incomplete information with the risk of withholding key details that could help consumers to protect their information. The FTC suggests that companies try to anticipate questions and post clear, plain-language answers on their websites.

Finally, a significant portion of the guide is devoted to notifying law enforcement, other affected businesses and the affected individuals.

In addition to state laws, other federal and state regulations may apply to organizations in certain industries, such as a breach involving health data. If the breach involves electronic health information, the organization may be subject to the FTC's Health Breach Notification Rule, which requires notifying the agency and, in certain cases, the media.

Organizations covered by the HIPAA Breach Notification Rule must notify the secretary of Health and Human Services and, in some cases, the media.

In the event of a data breach, companies should contact the local police department immediately to report the situation and the potential for identity theft. If the local police aren't familiar with investigating information breaches, the FTC recommends contacting the local office of the FBI or U.S. Secret Service. If mail theft is involved, the U.S. Postal Inspection Service should be notified.

Other businesses may need to be notified. For example, if account access information such as credit card or bank account numbers has been stolen, but the company doesn't maintain those accounts, the company must contact the institutions that do, so they can monitor the accounts for fraudulent activity. If names and Social Security numbers have been stolen, the FTC urges organizations to contact the major credit bureaus — Equifax, Experian and TransUnion — for advice, particularly if the breach involves a large group of people.

Unfortunately, hackers who steal names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft.

"People who are notified early can take steps to limit the damage," the guide points out. In deciding whom to notify and how, consider: state laws, the nature of the compromise, the type of information taken, the likelihood of misuse and the potential damage if the information is misused.

The guide suggests that businesses designate a point person in the organization to release information to those affected by the breach. The FTC offers sample letters, websites and toll-free numbers to communicate with people whose information may have been compromised.

Many businesses also offer at least one year of free credit monitoring or other support such as identity theft protection or identity restoration services, particularly if financial information or Social Security numbers were exposed.

The FTC recommends being as transparent as possible by clearly communicating what is known about the breach, including how it happened, what information was taken, how the stolen information was used if known, what actions are being taken to remedy the situation and how to reach the relevant contacts in the organization. Some companies update consumers on their websites. "This gives consumers a place they can go at any time to see the latest information," the guide explains.

The organization also should encourage individuals who discover that their information has been misused to file a complaint with the FTC via IdentityTheft.gov, the guide notes. This information is entered into the Consumer Sentinel Network, a secure, online database available to civil and criminal law enforcement agencies.

The guide emphasizes the FTC's role as a partner in responding to data breaches, offering contact information for individualized guidance and resources such as the agency's consumer response center, which fields calls from people affected by data breaches and a national victim complaint database.

With all of the information it provides, a key takeaway from the FTC guide is that hackers are unlikely to be deterred from finding new ways to steal consumers' personal information, so organizations need to be prepared for when — not if — they suffer a data breach.