Before and After a Data Breach:

The Game Plan

by Maureen Fulton

If you have received a call from a client asking how to handle a possible data breach of company systems or data, you are not alone. The frequency of data breaches has increased so quickly, and data breaches are so frequently in the news, that it is no longer surprising to hear about the latest Marriott, T-Mobile, or Equifax incident involving personal information. But behemoth companies are far from the only businesses at risk of having their systems breached. In Verizon's investigation and analysis of more than 41,000 security incidents occurring in 2019, 43% of breaches involved small business victims.[1]

Maureen Fulton

Maureen Fulton is the chair of Koley Jessen's Data Privacy and Security practice area. Maureen dedicates her practice to advising businesses in developing comprehensive privacy and data security programs. Maureen guides companies in navigating through state, federal, and international privacy laws and regulations. She also performs data privacy and security due diligence for buyers and sellers in merger and acquisition transactions. Maureen has worked with businesses to obtain certification under the EU-U.S. Privacy Shield and to ensure compliance with the General Data Protection Regulation (GDPR) and California Consumer Privacy Act of 2018 (CCPA). She has assisted clients in preparing for and remedying data breach incidents and identifying the associated litigation risks. Maureen is a member of the International Association of Privacy Professionals and has frequently presented on data privacy and security issues.

In Verizon's investigation and analysis of more than 41,000 security incidents occurring in 2019, 43% of breaches involved small business victims.[1]

Such companies are unlikely to have a staff teeming with IT professionals and thus need outside counsel to advise them on the steps to take to prepare for data breaches, as well as the best procedures to follow once a data breach or possible data breach has occurred. That's where you come in.

Now more than ever, your clients need your help to protect their data. This article addresses (1) tips for your clients in an effort to help them prevent security incidents; and (2) advice you can provide to your clients in the moments, hours, and days after a security incident occurs at their company.

Before Any Data Breach Has Occurred

Here are five tips that your clients and their employees should consider following to protect against malware, hacking, and ransomware from infiltrating their system and disrupting their operations:

1. Train Employees to Avoid Clicking on Suspicious Links and Opening Unfamiliar Attachments in Emails

According to Verizon's 2019 Data Breach Investigations report, 94% of malware that was found on computers as part of a security incident arrived via an email.[2] The number one type of cyber-attack involving social engineering[3] is a phishing attack sent via email, which often tricks users into installing malware on their work computer.[4] Scammers are working

nonstop to try to access companies' confidential information, largely through this method.

To prevent phishing attacks, implore your clients to institute training for employees that teaches them to be cautious when clicking on links or opening attachments in emails. The training should emphasize that for each email that employees receive, they should look carefully at the subject line and the sender to ensure legitimacy of the content.

Employees should not click on a link unless they are sure they know the sender's email address is correct by closely examining the email address. Employees should not open any attachments unless they were expecting an attachment to be sent. If an email seems "off", they should not reply—instead, they should delete the email, or send to the company's IT team. If an employee receives an unfamiliar call that was not expected asking for confidential or private information, employees should ask for their call-back number and the name of their supervisor, then hang up and further investigate before providing any information to them.

2. Require Stronger Passwords and Multi-Factor Authentication for Sign-Ins

Your clients might have a password strength requirement for employees signing onto the company's network, such as minimum character length, use of special characters, or another strategy. To the extent businesses can bolster those requirements by mandating employees use longer passwords (as one example, a 15- to 20-character passphrase) that is changed every 90 to 120 days, you should recommend that your clients make that change. If your clients have the ability to enable multi-factor authentication for network sign-in, which requires confirming via a text message or phone call in conjunction with a password in order to log on, recommend making that change to them. What are initially minor inconveniences with respect to signing onto the system will become routine. For many companies, enabling multi-factor authentication is one of the easiest fixes to institute, yet goes a long way toward protecting a company's systems and data.

3. Institute and Enforce Company Cybersecurity Policies

Your clients should institute cybersecurity policies to let employees know what is expected of them to protect their business' systems and data. For example, if they are able, they should enact a policy that remote workers should only use company-approved computers and are not allowed to download any work information onto a personal computer that has not been approved for work use. As another example, clients should institute a directive prohibiting workers from connecting to public WiFi on their work or company-approved laptops. These policies will minimize data theft or compromise and set clear guidelines for businesses to follow.

4. Use the Telephone for Any Sensitive Business Such as Wire Transfers or Sharing Confidential Information

When conducting any sensitive company matters, it is best for your clients to pick up the phone and call. They should ask for double or triple confirmation for wire transfer transactions or when sending or receiving company confidential information. If anything in an email seems off or even not as straightforward as employees would like, a verbal confirmation will ease their minds.

5. Offer Resources to Answer Employees' Cybersecurity Questions

Recommend to your clients that they offer resources for employees so employees have somewhere to go if they have questions about a strange-looking email or website, or how they can complete a transaction in the most secure manner. Your clients' system is only as strong as their weakest employee and ensuring open lines of communication will help protect against intruders. They should offer a dedicated email address or contact person for employees to be able to call with questions or concerns.

After A Data Breach Happens

If your client is concerned that company data may have been compromised, there are several steps they can take to best prepare themselves in the initial stages of a potential data breach.

1. Conduct an Initial Consultation

Speak with your clients by phone to ask when they first discovered an issue and how long they think the issue has been going on. Ask them to provide any initial thoughts about when and how the possible breach first occurred. Ask your clients whether they have lost access to any part of their system.

From a business standpoint, the goal is to ensure that your client's operations can continue, but without jeopardizing any part of the company's system. If the company's network is potentially still being compromised by the threat actor, your client should consider whether the company's system needs to be taken offline.

You should also ask your client whether they have insurance coverage for cyber breaches. If your client has a cyber insurance policy, they should contact their insurer to determine whether coverage exists.

2. Review the Types of Data on the System

Work with your client to conduct a "data mapping" exercise to the extent possible, determining what types of data is held on the server(s) and where such data is located. If your client holds any data that is potentially subject to the Health Insurance and Portability and Accountability Act, there are certain requirements at play for privacy and security.[5]

The type of data that was accessed or acquired by the bad actor could determine whether data breach notifications need

to be made to individuals. Every state has its own data breach notification law.[6] Although there are patterns in the laws, the data that each state considers to be "personal data," and the requirements of notifications, can vary widely. If the client controls data of individuals located in many different states, a complete analysis of the relevant laws is recommended. If credit card information is part of the data that was compromised, the company could have to take on an additional requirement—paying for credit monitoring services for the affected individuals.[7]

3. Forensic Investigation

Even if your client has a solid internal IT department, it is recommended for them to have an outside forensic company that specializes in breach response perform an analysis of your client's situation. Ideally, you as counsel can engage the forensic firm so an argument can be made that any reports generated as a result of the investigation can be protected by attorney-client privilege.[8] Utilizing a third party will help your client to ensure that any lingering issues from the breach have been resolved and determine whether the root cause of the breach can be determined.

4. Law Enforcement

If the breach event was a phishing or ransomware scheme that resulted in your client losing monetary funds or control of their systems, it is important to contact local, state, or federal law enforcement early to give them a chance to recover the lost money or offer advice on negotiating with the threat actors. This strategy might not be appropriate for general data breaches, although some state statutes require consultation with law enforcement to determine whether an incident should be classified as a "breach" (and thus notification requirements triggered).[9] Again, review of the relevant laws is essential.

5. Public Relations

Depending on the scale of data breach incident that has occurred, it may be necessary for your client to make one or more public statements regarding the breach. This statement may be in the form of a letter to the affected individuals, a notification to the attorneys general in the state(s) where the individuals whose information was breached are located, or even a press release or press conference. If issues are currently ongoing that require notification to clients because there is a delay or stoppage in services, one approach would be a simple statement that the company is experiencing technical issues and is working to solve them as quickly as possible. If the number of customers affected is large, your client may want to consider engaging an outside public relations firm or a call center.

Helping your clients through this stressful time will be challenging yet rewarding.

Endnotes

1 2019 Verizon Data Breach Investigations Report, p. 5. Verizon examined 41,686 security incidents for its 2019 report, of which 2,013 were confirmed security incidents. *See id.*, p. 4.

2 2019 Verizon Data Breach Investigations Report, p. 13.

3 Social engineering is "the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data." "Social engineering explained: How criminals exploit human behavior," Josh Fruhlinger, September 25, 2019, CSO Online, *available at* https://www.csoonline.com/article/2124681/what-is-social-engineering.html.

4 "Top cybersecurity facts, figures and statistics for 2020," CSO Online, March 9, 2020, *available at* https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.

5 The HIPAA Privacy Rule establishes national standards to protect individuals' medical records by setting limits and conditions on when disclosures of protected health information may be made without authorization by the individual. *See, e.g.*, 45 C.F.R. § 164.512. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure confidentiality and security of protected health information. *See, e.g.*, 45 C.F.R. § 164.306.

6 *See* "Security Breach Notification Laws," National Conference of State Legislatures, March 8, 2020, *available at* https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

7 *See, e.g.*, "Equifax Data Breach Settlement," Federal Trade Commission, January 2020, available at https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement; in which Equifax was required to make credit monitoring services available to individuals affected by its 2017 data breach.

8 At least one court has held that such investigations would be protected by the attorney-client privilege, at least on the facts present in that situation. *See In re Experian Data Breach Litig.*, 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017) (court held that but for law firm instructing forensic firm to complete investigation in anticipation of litigation, the investigation report would not have been "prepared in substantially the same form or with the same content."). More recently, a court has held that such investigatory reports by forensic analysts were not privileged despite being commissioned by a law firm because the report at issue was made for a business purpose, rather than in anticipation of litigation. *See In re: Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 2019 WL 7592343, at *5 (E.D. Va. Dec. 19, 2019).

9 *See, e.g.*, data breach notification laws in Connecticut (Conn. Gen. Stat. § 36a-701b et seq.); Florida (Fla. Stat. § 501.171 *et seq.*); and Missouri (Mo. Rev. Stat. § 407.1500 *et seq.*).