2021 Annual Conference
June 16-18, 2021
Atlanta, GA

"When is a Ransomware Attack or Business Email Compromise a Reportable Data Breach?"

I. In all this chaos, we didn't think to consider if there was a reportable data breach

Ransomware and Business Email Compromise are the Most Frequent Cyber Attacks

Ransomware attacks have exploded in the past few years. They have become more targeted and more severe. Many types of ransomware attack backups in the cloud as well as shadow copies within individual systems, making it nearly impossible to recover data without the decryption key. Attackers increasingly post "proof of life" in ransomware attacks, meaning that they post some of the victim's data to online to pressure the victim into paying the ransom.

Business email compromises occur with nearly equal frequency as ransomware attacks. Hackers usually use phishing campaigns or malware planted prior to launching a ransomware attack to compromise business email accounts. Once the business email account is compromised, hackers lurk in the account watching the email traffic, who the account communicates with, what resources the owner has access to and how they communicate with others. At some point, the attackers may use the email account as a launching pad for other email account compromises or to perpetrate a fraudulent funds transfer or invoice manipulation.

All fifty states have data breach laws

All fifty states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have data breach notification laws. There are differences among them, but they generally require the victim of a data breach to report the event to law enforcement and to notify affected individuals. The thresholds for reporting differ. One state may require that all affected individuals be notified of the breach, while other states have thresholds that exempt small breaches from reporting. The type of data breached also serves as a threshold for determining whether a breach much be reported. Personally identifying information (PII) and Personal Health Information (PHI) generally trigger the notification requirement. States differ on whether data that has been "accessed" but not "acquired" or exfiltrated must be reported. They also differ on whether encrypted data can be breached. Many states require notice when encrypted PII has been breached when the private key has also been breached.

States also have different definitions of PII. Most states define PII as a person's first and last name along with some other type of information, such as social security number, financial

account number or date of birth. An increasing number of states include email address along with the password as PII. Also increasing is the number of states that include biometric information, such as fingerprints, retinal scans and DNA sequencing as PII.

Insurers have special requirements for data breach reporting. States that have adopted the NAIC Insurance Data Security Model Law generally require that insurers, report breaches involving "non-public" information, which includes confidential business information that is not otherwise classified as PII.

Financial services companies operating in New York are subject to the NY Department of Financial Services Cyber Security Regulation. The regulation echoes the NAIC Model Law, requiring data breach reporting to the DFS in the event of certain cyber security incidents.

And that is why you need to bring in an expert

Lawyers trained and experienced in data breach and cyber security are critical in determining whether a reportable data breach occurred. It is not sufficient to use in-house information technology resources when a company suffers a ransomware attack or business email compromise. An in-house IT group typically is not aware of the patchwork of laws governing data breach reporting. They are usually focused less on the law and more on getting the business back up and running. By the time counsel gets involved, evidence and important documentation may be gone due to well-meaning internal IT staff trying to remediate the incident.

Even professional incident response firms may overlook notification requirements. After all, their job is to investigate and remediate the incident. Providing legal advice is not their mandate.

In-house lawyers also are usually ill suited to determine if there has been a reportable data breach. In-house counsel have many things to balance and many compliance and legal considerations across the entire business. Data breach notification requirements can differ widely and can be an esoteric field.

Bringing in an experienced data breach and cyber security attorney at the earliest stages of an incident can streamline the investigation and make the response more effective and legally compliant. A good data breach attorney will know what types of ransomware strains are more likely to involve data exfiltration and they can identify what types of data trigger notification requirements in each of the states and territories. These lawyers also have networks of incident responders, ransomware specialists, credit monitoring and remediation firms and vendors who make large-scale notifications. Rather than having an internal IT department or law department reinvent the wheel, engaging specialized counsel can dramatically reduce the costs associated with a cyber incident.

And that is also why businesses need cyber insurance

Cyber insurance has evolved from a product that only covered a data breach to policies and endorsements that cover a broad range of cyber related incidents. When cyber policies only covered data breach, typically only incidents that the insured suspected was a breach were reported. And, coverage for an investigation ceased when no breach could be proven. With expansion of coverage to ransom negotiation and payment, cyber attacks, misdirected payment fraud and other types of computer-related fraud, it is increasingly important that claims staff recognize the potential for multiple coverages to be implicated in a single incident and to fully

investigate, remediate and identify any reportable data breach that occurred during the incident.

For example, a business email compromise claim can be confirmed with a fairly straightforward investigation. However, in order to determine if data was exfiltrated and what data was affected, a more in-depth investigation is often required and may involve multiple mailboxes. The insured may be satisfied with a brief investigation, but the insurer and the insured can both be exposed to risk if a data breach occurred and was not reported. If a data breach is not identified or reported, the affected individuals may suffer identity theft, business email compromise of their own or misdirected payment or invoice manipulation fraud. The insured and insurer are in a much more defensible position if a thorough investigation is completed and competent counsel engaged to advise on applicability of breach notification laws. Finding out that an investigation was inadequate a year or two after an incident can result in reputational harm and additional expenses.

In ransomware cases, negotiating and paying the ransom is a frequent first step. If an insured has a viable backup, restoring the data is a first step. Getting the company back up and running tends to be the focus of a ransomware incident. And, facing large and unexpected expenses associated with a ransomware event can pressure an insured to shut down an investigation prematurely. However, data breach is common in ransomware attacks and a fulsome investigation can determine if data were accessed or exfiltrated. Additionally, attackers have engaged in "double extortion" by perpetrating the attack and then coming back to extort the victim again for not reporting a data breach.

Cyber insurance provides necessary resources for responding to business email compromise and ransomware. In order to ensure the response is sufficient, however, it is essential to evaluate each and every cyber claim to determine if there was a reportable data breach.

II. Common issues in investigations

Ransomware

Anyone who has been involved in a ransomware incident response can tell you that it is chaotic and an enormous amount of pressure. Business continuity is a priority, as is reputational harm and preservation or restoration of data. Data breach is rarely a concern that takes center stage, even though it may be the most costly exposure, other than the business interruption. Because the overarching goal of ransomware events is to get the business back up and running, many businesses pay the ransom and move on to decrypting their systems as quickly as possible. If they have viable backups, they restore the data and get back to business. However, in doing so, evidence necessary to determine whether there was a data breach and what individuals may be affected can be destroyed.

Business Email Compromise

Similarly, when investigating a business email compromise, the concern is to protect the business. Investigators tend to focus on whether payments or goods were fraudulently diverted, whether multiple email accounts were compromised and whether financial account information was exposed. Yet, business email accounts can contain a great deal of PII and non-public information. For example, emails to and from payroll, accounting, human resources, accounts payable or business unit managers can contain PII relative to current or former employees, applicants, vendors, business plans or intellectual property. To ensure full compliance with data

breach notification laws, it is essential to fully investigate business email compromises and determine if a data breach occurred.

Misdirected Payment Fraud and Computer Fraud

The focus in misdirected payment and computer fraud cases is to determine how the fraudster obtained the information necessary to perpetrate the fraud and to stop the bleeding. That includes determining if the attacker is embedded in an email account or some part of the computer network, what financial information may have been compromised, how much money was lost and if it can be clawed back. Because financial transactions take place very quickly and being able to track them and get the money back before the bad actor withdraws it and escapes is critical, the potential of a data breach during the event can be overlooked or given short shrift.

III. Best Practices and Tips

Businesses need a cyber security program and an incident response plan

About half of the states require that businesses exercise reasonable cyber security. That is usually interpreted to mean that they have a written cyber security program that includes an incident response plan. Written cyber security plans usually follow one or more, or some combination of the cyber security frameworks developed by the National Institute of Standards and Technology (NIST Framework), the International Standards Organization (ISO) 27000 series or others.

An incident response plan should be written and developed in coordination with company leadership, the in-house legal department, information technology security, physical security, risk management, corporate communications and relevant business units. The document should address who the incident response team will consist of, including identifying team members outside of the organization, such as outside cyber and privacy counsel and incident response firms as well as ransomware specialists that are licensed and able to negotiate and pay cryptocurrency ransoms. Due to the United States Department of the Treasury's Office of Foreign Assets Control regulations, enforcement remit and their October 1, 2020 Ransomware Advisory, if a ransom is paid, it is absolutely essential that the payer ensure that the payee is not on the list of sanctioned individuals and entities. Because failure to complete a check of the sanctions list can result in fines and other penalties, and because sanctions can be applied on a strict liability basis, identifying a reputable and responsible ransomware specialist is of particular importance.

Once a plan is created, it is just as important to practice as it is to have the plan. Every cyber incident is different. Every incident requires at least a slightly different response and modifications to the response team. The more practice your team has by working through tabletop exercises, they better prepared they will be to confront, respond to, remediate and learn lessons from actual incidents. Not practicing is a set up for failure. At the first sign that the plan "doesn't work," teams are tempted to throw it out the window and ad lib.

Resources

Breach Reporting Laws: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

NIST Framework: https://nvd.nist.gov/800-53
ISO 27000 Series: https://www.iso.org/isoiec-27001-information-security.html
United States Treasury, OFAC, Ransomware Advisory: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001