RE-ISAC Weekly Cybersecurity Report

Real Estate ISAC Information Sharing and Analysis Center

Serving the Commercial Facilities Sector

04 April 2019

This report is **TLP AMBER**. **TLP AMBER**: Limited disclosure, restricted to participants' organizations. Sources may use **TLP AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share **TLP AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

Find RE-ISAC on Social Media!

BEING HELD LIABLE

IN BRIEF: Over the past month alone, there have been high profile reminders that nefarious cyber actors continue to not only develop new tactics, but continue to shape and evolve. Ransomware, business email compromise, and scams continue to dominate the headlines while businesses big and small continue to grapple with securing vulnerabilities and closing gaps. And as customers recognize the impacts of a cyber-related incident or breach, they are going to court to hold businesses liable for failing to secure their confidential information. Understanding the legal aspect of incident response only adds to the actions organizations must execute, but also ensures that organizations know the laws and regulations that govern data breaches, as well as any industry or sector specific rules and requirements. Effective preparedness can help organizations to take proactive control over their security - providing a high level of security and also understanding their weaknesses.

KEY TAKEAWAYS & RECOMMENDATIONS.

- With each day, organizations continue to face new and evolving threats that include ransomware, business email compromise (BEC), and any number of scams, persistent and opportunistic, that can have disastrous consequences for all types of businesses.
- With each threat, organizations are being held liable for the impact and the perception of lack of security that resulted in an incident or breach.
- Key to understanding liability, organizations need to develop and maintain an understanding and adherence to the various laws, and regulations that are being enacted to protect consumer rights.
- It's important for organizations take an active approach to security which comes with a recognition that incidents may happen, which then shifts the discussion to preparing an appropriate response and breach notification.
- Recognizing the threats, knowing the laws and regulations, and being prepared to respond before an incident occurs will help organizations achieve a state of preparedness that can benefit the organization when one does.

DISCUSSION. Cyber threats continue to evolve at a rapid pace, yet their foundation is still rooted in basic concepts. Ransomware, business email compromise (BEC), and other scams continue to present challenges to organization that can have disastrous consequences for all types of businesses, regardless of the number of employees. Consider some of the following incidents:

- On 13 March, clothing and camping equipment retailer Kathmandu in Australia revealed that an 'unidentified third party' may have had access to its online ecommerce website for over a month. The attack may have resulted in

capture of customer personal information and payment details entered during check-out. This attack screams of Magecart or the growing popularity of 'formjacking', which typically involves embedding malicious JavaScript code in online payment pages.

- In the wake of the 15 March New Zealand mosque shooting, the CISA warned on the potential of New Zealand-Related Scams and Malware Campaigns in which fraudulent emails requesting donations from charitable donations contain links or attachments that direct users to phishing or malware-infected websites.

> The US Supreme Court rejected a bid by online shoe retailer Zappos to throw out a class-action lawsuit after customers in the complaint that misuse can occur at any time, even years later, and long before fraud is discovered.

- On 19 March, global aluminum producer Norsk Hydro was forced to shut down its plants and worldwide network after a security breach led to access to files being blocked and passwords changed to user accounts across several of its corporate and production control systems. "A few days later, two US-based chemical companies – Momentive and Hexion – announced they had also been hit by cyber-attacks and had shut down IT systems to contain the incidents. Both are owned by the public equity firm Apollo Global Management." These attacks apparently occurred earlier than the one on Norsk, on 12 March.
- Beazley Breach Response (BBR) Services identified some concerning statistics involving ransomware and BEC after analyzing 3,300 incidents involving their clients in 2018:
    - 71% of ransomware attacks targeted small businesses, with an average ransom demand of $116,324 and a median of $10,310.
    - The highest ransom demanded from its insureds was of $8.5 million or 3,000 Bitcoin, while the highest ransom paid by one of its clients was of $935,000.
    - Small-to-medium sized companies were the most sought over targets because they will usually spend a lot less on securing their computing systems and information than larger firms, making it a lot easier for malicious actors to compromise their systems. Out of all SMBs impacted by ransomware, the ones 'that do not lockdown Remote Desktop Protocol (RDP) are at higher risk of being attacked' according to Beazley, a group of global insurance professionals
    - BEC attacks accounted for roughly 24% of the overall number of breach incidents reported to Beazley Breach Response (BBR) Services, a drastic boost from the 13% reported for 2017.
    - The highest BEC claim paid by the insured was of over $2.5 million, while the average cost of a BEC claim was around $70,960.
    - Attackers of all skill levels were involved, from those that used ransomware-as-a-service (RaaS) platforms [FilesLocker, Saturn, Data Keeper, Princess Evolution, GandCrab] in their campaigns to highly skilled threat actors who used ransomware to attack specific targets with goals "clearly beyond extortion.
    - Besides abusing weakly protected RDP daemons, attackers also used sextortion campaigns to dupe their victims into downloading ransomware malware or droppers that will eventually infect the compromised machine with ransomware.
- Arizona Beverages, is recovering after a massive ransomware attack last month that highlighted a couple issues. Not only was the company warned by the FBI previously about an apparent Dridex malware infection, but many of the back-end servers were running old and outdated Windows operating systems that are no longer supported. The company is "still rebuilding its network almost two weeks after the attack hit, wiping hundreds of Windows computers and servers and effectively shutting down sales operations for days until incident response was called in, according to a person familiar with the matter."

The above represent a sampling of the types of attacks organizations face. The *RE-ISAC Daily Report* addresses the latest threats and breaches that impact the Sector. But in many cases, the incident, is just the beginning of the challenges. More and more, **organizations are being held liable for the impact and the perception of lack of security that resulted in an incident or breach**. Organizations are expected to protect sensitive customers' sensitive data, and when that fails, individuals may file lawsuits independently or join class action lawsuits against those organizations resulting in significant

financial impacts. Even in breaches in which a third party vendor or provider is responsible, the organization may still be held liable for failing to holding that third party responsible for protecting that sensitive data. And the future may be more challenging as "Courts are making it easier for victims to sue companies that suffer a data breach, and regulators are probing these firms more aggressively with the aim of levying large fines."

According to the Insurance Information Institute, some of the key areas organizations need to consider as the result of a breach include:

- **"Liability**—You may be liable for costs incurred by customers and other third parties as a result of a cyber-attack or other IT-related incident.
- **"System recovery**—Repairing or replacing computer systems or lost data can result in significant costs. In addition, your company may not be able to remain operational while your system is down, resulting in further losses.
- **"Notification expenses**—In several states, if your business stores customer data, you're required to notify customers if a data breach has occurred or is even just suspected. This can be quite costly, especially if you have a large number of customers.
- **"Regulatory fines**—Several federal and state regulations require businesses and organizations to protect consumer data. If a data breach results from your business's failure to meet compliance requirements, you may incur substantial fines.
- **"Class action lawsuits**—Large-scale data breaches have led to class action lawsuits filed on behalf of customers whose data and privacy were compromised."

Two recent cases further show the landscape that confronts organizations who have been targeted and their rights and responsibilities. It also highlights the importance of having legal representation a part of security planning teams as well as incident response teams. On 25 March, **the US Supreme Court "rejected a bid by online shoe retailer Zappos to throw out a class-action lawsuit by customers who said their personal information was stolen by hackers in 2012**." This ruling has stopped efforts by organizations to limit their liability in data breaches. Zappos argued that the customer's data was not harmed by the breach, yet the customers in the case argued that misuse can occur at any time, even years later, and long before fraud is discovered. In another incident, a case was dismissed against Buck Law Firm that was the victim of an attack in which an attacker routed money owed to Deutsche Bank to a cybercriminal's account. In a series of legal maneuvers, Buck Law Firm tried to claim that even though they provided payment to an attacked account, they should not be held liable for paying the correct amount to Deutsche Bank. The Court dismissed the case because "Virginia law doesn't allow companies to bring negligence claims against organizations that are hit with a data breach based on 'a duty to safeguard the private information of another individual.'"

Along these the lines of liability consideration also must be made to existing and emerging laws and regulation. Adherence to change the liability of the incident, but ensuring incidents are reported in accordance with these to ensure that additional penalties are not imposed.

- Two years ago Europe ushered in the General Data Protection Regulation (GDPR) on 25 May 2018, in order to "ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals." Specifically, Article 33 of the GDPR provides the requirements for the notification of a personal data breach to the supervisory authority.
- Canada also implemented similar breach notification standards through the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") that went into effect on 1 November 2018.

- California introduced the California Consumer Privacy Act (CCPA) earlier this year, which has often been described as 'GDPR Lite' and will come into law in 2020. The National Council of State Legislatures (NCSL) provides a listing by state or territory of security breach notification laws.

MITIGATION. Security is hard and requires not only constant awareness of the threats, but also organizational requirements, laws, and regulations. The threats to the Commercial Facilities Sector will only continue to evolve and adapt in order to pry away the sensitive information that the Sector works to protect. And despite the best efforts, there will always be vulnerabilities and gaps that are identified that could be exploited. Therefore, having a defense in depth will help mitigate the potential risk. But bigger than that is ensuring that organizations take an active approach to security and develop a security strategy that can be translated into a security plan that encompasses security processes and procedures and a risk management program. Unfortunately, incidents will still happen and it will be important that organizations can respond in kind. Taking into consideration some of the laws and regulations some of the key considerations and information includes:

- **Other Requirements.** While we were not able to identify clear Commercial Facilities Sector specific requirements, there may be other requirements that may apply to the incident. One such example lies within the HIPAA requirements for health care stipulates that "covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate."
- **Work with others.** When preparing form notice letter templates, as well as when modifying the templates for use in response to an actual or suspected breach, the form notice letter should be reviewed by the company's:
    - Legal counsel.
    - Human resources.
    - Chief information officer (or equivalent officer).
    - Public relations and corporate communications teams.
- **Take your time.** While most notifications stipulate a timeline within 72 hours, organizations can, and often should, use as much time as possible to fully understand the situation and the impacts. Rushing to notify can result in partial or incomplete information that may have additional impacts. It's more important to be right than it is to be first to notify.
- **Sample Template.**
    1. Organization information, to include primary business address.
    2. What happened. This should be a clear and concise statement about what type of incident occurred.
        a. Who may have been responsible?
        b. What was the cause, i.e., malicious attack, negligence, accident?
        c. What type of attack or exploit was used?
    3. When the incident happened. Addresses not only the date when the breach was identified, but also the time in which the attacker was able to access the information.
    4. Who is impacted?
    5. What information was compromised?
    6. What steps have been taken and what is being done to ensure this attack is mitigated or that will not happen again?
    7. What customers should do should they notice any unusual activity.
    8. What services the organization is providing in the wake of the breach.
    9. Who should customers contact?