Cybersecurity Threats: A Year in Review and a Look Ahead

In confronting unprecedented circumstances, insurers and insureds need to confirm that their business insurance policies and data security practices protect them from any operational interruptions.

The Legal Intelligencer
December 19, 2023
By David J. Shannon

As we close out the year, the threat of cybersecurity attacks targeting entities in both the private and public sectors is increasing at an alarming rate. Businesses and governments alike are encountering new and innovative tactics from organized threat actors seeking to exploit vulnerabilities in their computer systems, networks and software. In confronting these unprecedented circumstances, insurers and insureds need to confirm that their business insurance policies and data security practices protect them from any operational interruptions. Here's a look at what we've seen this year and what we might expect in 2024.

Cryptojacking

While crypto mining and cryptocurrency generally affect crypto-related businesses, nefarious actors have begun to hijack unrelated companies' IT infrastructures to crypto mine. Crypto mining, the process of solving mathematical equations or puzzles to generate Bitcoins or other cryptocurrencies, has always been resource intensive. While each Bitcoin is worth tens of thousands of dollars, the upfront cost of the required infrastructure dissuades many who would be interested in crypto mining. Realizing this, threat actors have begun hijacking, or "cryptojacking" the robust IT infrastructure of established industrial and cloud services companies for use in crypto mining operations. Cryptojackers are able to generate cryptocurrency while leaving the affected company with the bill for the large amount of electricity, cooling and server use involved.

The results of successful cryptojacking involve IT infrastructure slowdowns or crashes, which lead to potential liability for loss of business interruptions and third-party claims. Affected companies will also incur the costs of conducting a breach incident response, especially if the entity is an IT service provider to other businesses. To prevent avoidable losses, companies need to ensure that their cyber insurance not only covers the incident response to a potential data breach, but also for business loss, business interruption and the replacement costs for damaged hardware.

Ransomware

On a separate front, organized ransomware outfits continue to be a growing threat to entities in both the private and public sectors. Threat actors operating in this sector

seek to infiltrate a business's or government's network with the goal of encrypting all data on their servers. Once encrypted, the hackers offer to sell a decryption key to the affected party. More recently, ransomware groups have begun to simply copy all of the data on the affected entities' servers and forego encryption. In this scenario, hacking groups threaten to release the often sensitive information to the public unless a ransom is paid.

In response to this, businesses and governments have adopted more stringent security training for personnel. Additionally, the Biden administration recently released a "national cybersecurity strategy" plan, which focuses on proactively bringing threat actors to justice, in addition to providing software developers with more resources to add better security features to their products.

Phishing

Although the threat of ransomware attacks is great, companies and governments have a growing number of tactics to defend against these types of disruptions. The most crucial defense against ransomware attacks is technologically savvy employees. It is important for employees to be aware of these types of attacks, which are usually initiated through phishing attempts, and how to defend against them. Additionally, IT departments have the added responsibility of monitoring third-party software libraries that power their systems. As most software vulnerabilities appear in third-party libraries, it is essential that companies catalog all necessary third-party software and monitor them for known security vulnerabilities. Doing so will prevent company software from becoming vulnerable to infiltration attempts, which will decrease the risk of ransomware attacks.

Unfortunately, threat actors adapt rapidly to the precautions that public and private sector entities take to prevent cybersecurity incidents from occurring. As these criminal organizations pivot, they find themselves transforming, as well. There are now more active "affiliate" hacking organizations than ever before, which directly impact how interactions with these threat actors play out. Additionally, with the recent AI revolution, experts expect that AI will soon be used to write malicious ransomware software for threat actors. With automation soon to free up resources at these hacking collectives, these criminal enterprises are becoming more selective in their targets. More of these attacks are now targeting law firms, as they are massive repositories of client information and are usually well-covered by cyber insurance, which increases the ransoms that can be paid to these groups. Finally, while phishing attacks have been prevalent for more than a decade, threat actors are now designing more sophisticated and believable phishing attempts.

Building a Defense

With cybersecurity risks continually emerging, employers need to ensure that they are as prepared as possible to defend against these threats. While a diligent IT department is needed to fend off the majority of threats, rank and file employees tend to be targeted by threat actors, as they have been proven to be the weakest cybersecurity link in organizations of all sizes. Robust cybersecurity training and awareness programs are integral to the safety and security of irreplaceable organizational data. Forward-thinking IT departments should also

be regularly backing up critical company data in case of a successful attack.

It is imperative that companies and governments protect themselves against evolving cybersecurity threats. As the strategies and tactics of the threat actors in this space change, so do the ways that public and private sector entities can defend against them. Moving into 2024, every government and business should prioritize securing their IT infrastructure, ensuring that their cyber insurance policies fully protect them from any liability, and educating their employees on emerging threats.

David J. Shannon chairs both the privacy and data security practice group and the intellectual property, technology and media litigation practice group at Marshall Dennehey. He may be reached at djshannon@mdwcg.com.