Chicago Daily Law Bulletin®

Volume 163, No. 36 Serving Chicago's legal community for 162 years

Your money or your (business) life: 'Ransomware' raises the stakes

New developments in cyberattacks could make organizations long for the good old days when all they had to deal with were network breaches.

In a network breach, hackers typically use stolen credentials to access a business' IT infrastructure to make off with sensitive data belonging to employees and customers. Organizations of all sizes and types have experienced data breaches — even tech giant Yahoo, which disclosed in December that hackers stole personal information from more than 1 billion customer accounts in 2013.

More recently, however, cyberattackers are taking their activities to whole new level by extorting money directly from targeted organizations through ransomware attacks, according to a new guide published by the National Institute of Standards and Technology, part of the U.S. Commerce Department.

The "Guide for Cybersecurity Event Recovery," released in December, helps organizations recover from increasingly sophisticated cyberattacks, including those known as ransomeware. Hackers use ransomware to "encrypt the organization's critical data, such as personal data or business data, after they have infiltrated the systems, then demand a monetary payment in digital cash formats, such as bitcoin," the guide explains.

In the first three months of 2016, 17 percent of all ransomware attacks around the world targeted businesses, which translates to a ransomware hit on a business every two minutes. By the end of September, according to National Institute of Standards and Technology, the ransomware attacks escalated to almost 24 percent — or an attack every 40 seconds.

Ransomware continually evolves, with new players like Cerber, Locky and CryptXXX joining more established troublemakers including CTB-Locker, CryptoWall and Shade. Ransomware propagates primarily through spam attachments and "exploit kits," which hackers use to find and use security vulnerabilities in software applications to spread malware.

A popup message is the common method for announcing that a ransomware attack is underway, informing users that their data has been encrypted and the only way to regain access is to pay a fee to the attacker. The attack holds the data hostage by making it inaccessible, resulting in a disruption of the business.

If the organization fails to pay, the data remains encrypted or is deleted. The ransomware may spread to other systems and take additional data hostage, according to the report.

The number of companies experiencing ransomware attacks tripled between the first and third quarters of 2016, according to the Kaspersky Security Bulletin 2016 published Dec. 8 by digital security solution provider Kaspersky Lab.

Nerissa Coyle McGinn

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.

Ransomware propagates primarily through spam attachments and "exploit kits," which hackers use to find ... security vulnerabilities in software applications to spread malware.

Even more disheartening, one in five small- and medium-sized businesses that pay the ransom never get their data back. And there is also evidence that ransomware became more sophisticated and efficient last year by becoming more targeted and exploiting new infection paths.

The National Institute of Standards and Technology guide is the first to consolidate information about responding to and recovering from cyberattacks, including ransomware. While intended for U.S. government agencies, the institute says the information provided should be useful to any organization in any industry sector.

In the simplest of scenarios, recovering from a cyberattack may involve a system administrator rebuilding a system or restoring data from a backup. But, as the rise of ransomeware attacks last year demonstrates, it's usually far more complicated than that.

Recovery is the last component in the risk-management cycle and is preceded by identification, protection, detection and response, the National Institute of Standards and Technology guide explains.

Specifically, recovery involves the development and execution of the recovery plan that was created prior to a cyberattack, followed by continuous improvement efforts to mitigate the likelihood and impact of future attacks.

Most businesses have become highly dependent on technology to function, so organizations need to focus on how to carry on during and after a cyberattack. "Organizations must understand how to be resilient, planning how to operate in a diminished capacity or restore services over time based on services' relative priorities," the institute's guide points out. Therefore, an effective recovery plan is critical.

The institute guide recommends a number of steps that businesses should take to prepare for a cyberattack, including creating a blueprint for operating in a diminished capacity during or following the attack and to restore services over time; identifying and training key personnel who will be responsible for defining recovery criteria and related plans; and creating and maintaining a list of the internal and external people, processes and technologies that enable the business to operate.

A well-thought-out recovery plan is key. Businesses should not only develop recovery processes and procedures, but they also should practice those recovery processes to ensure effective coordination of the recovery team and the timely restoration of services. Recovery planning should include formally defining the conditions under which the recovery plan would be invoked, specifying who has the authority to invoke the plan and how the recovery team will be notified, identifying milestones for "intermediate recovery goals" and developing an organization-wide recovery communication plan.

As the institute guide points out, recovery planning is not a onetime activity. Continuous improvement of the plans, policies and procedures requires implementing a feedback loop that includes individuals who have a role in recovery activities and involves conducting regular cyberattack recovery exercises and tests to identify weaknesses in the organization's technologies and processes, documenting and analyzing the results of the tests and then using the lessons learned to strengthen the relevant plans and processes.

Why place so much emphasis on recovery? Because 100 percent prevention is no longer possible.

As the number of major cyberattacks continues to mount every year, hacking of some sort seems all but inevitable for most businesses. "There has been widespread recognition that some of these cybersecurity events cannot be stopped and solely focusing on preventing cyberevents from occurring is a flawed approach," the institute guide concludes.

As Kaspersky Lab reports, cyberattacks hammer some industries harder than others, but research shows that all sectors are at risk. The industries most often targeted by ransomware hackers include education, IT and telecommunications, entertainment and media, financial services and construction.

And organizations are paying up.

In 2016, VESK, the United Kingdom's largest managed cloud computing provider, paid nearly $23,000 to get back into one of its systems. Disturbingly, hospitals are becoming a favorite target, which could have serious consequences for patients, notes Kaspersky Lab. Hackers locked Hollywood Presbyterian Medical Center in Los Angeles out of its own computer system until it paid $17,000.

Ransomware is only the latest in the line of hackers' malicious activities. Until tools are developed to neutralize cyberattack or at least stay one step ahead of them, a strong recovery plan may be an organizations' best bet to minimize the damage hackers can cause their businesses.

The institute guide offers a fundamental action plan for organizations of different sizes and from different industries that can be tailored to fit a business' individual needs.