Mitigating Risk

Protect your Business Against Ransomware

RANSOMWARE HAS BEEN one of the top cyber threats in the past several years. In December 2018, Delaware Guidance Services, a Wilmington-based mental health provider, was hit by a ransomware attack that impacted sensitive medical and financial information of about 20,000 children. Ransomware has also hit major cities, including Baltimore and Atlanta. The attack on Baltimore, which began on May 7, 2019, crippled city services and is expected to cost the city over $18 million. As of July, all services have not yet been restored and the effects will linger for months.

The global cyber risk and insurance company Beazley has reported a dramatic increase in ransomware attacks, increasing 105% in the first quarter of 2019 compared to the first quarter of 2018. The financial losses can be staggering. Businesses lose revenue while their data, computers and servers are inaccessible, and they spend enormous sums to bring their systems back online. In addition, companies can find themselves facing legal liability from regulatory enforcement actions and shareholder and customer lawsuits. Financial damage is expected to exceed $11 billion in 2019.

What Is Ransomware?

Ransomware is a type of malicious software, or malware, that blocks users' access to computer files or devices. It does this by encrypting the data, making it unreadable unless the victim pays a ransom and receives a decryption key from the hacker. Once the victim's computer is encrypted, the hacker will display a screen or webpage that explains how to pay the ransom and unlock the files. Ransomware has many variants, and has become so prevalent that novice hackers can purchase ransomware kits on a subscription basis to launch attacks. A victim's system is typically infected when a user clicks on a malicious link in a phishing email or on a bogus website, or attempts to download free files. After the initial infection, the ransomware spreads to other computers and servers throughout the system, locking up all data.

The attack on the city of Baltimore used malicious software known as "RobbinHood," and is reported to have contained a hacking tool developed by the National Security Agency, known as "EternalBlue." Since it was stolen from the NSA in 2016, EternalBlue has appeared in numerous

ransomware attacks, including WannaCry, launched by North Korea in 2017. WannaCry infections were reported in over 150 countries and hit hospitals and other public service companies worldwide. The NSA has come under intense criticism for creating these "back doors" to computer programs and systems, even if it was done for national security reasons, because they vastly increased the risk that criminal groups and other bad actors would also find these vulnerabilities.

Should a Victim Pay the Ransom?

In the first three months of 2019, the average ransom payment was $224,871, representing a 93% increase in the payment demand over the average demand in 2018. Hackers typically demand larger ransoms from larger organizations. The highest payment demand reported in 2018 was $8.5 million and the highest payment was $935,000. Payment is usually demanded in bitcoin or some other cryptocurrency, because such transactions are extremely difficult to trace. Money paid to hackers only serves to proliferate the ransomware activity, since it becomes so profitable to hackers. This is why the FBI, the Department of Health and Human Services and most cybersecurity leaders all stress that it's important not to pay ransoms to hackers.

Individual organizations make their own decisions whether to pay a ransom. After all, there's no guarantee that the hacker will honor his commitment and unlock the data after receiving the ransom. Factors that organizations consider include: whether there is a recent and uninfected backup of data that can be restored to a clean system; the harm expected to be caused by a prolonged shutdown; the amount of the demand; the likelihood that the hacker will unlock the data; whether insurance is available to cover the loss, and the company's policy of making a payout to criminals. One study has shown that less than one-third of those who pay the ransom receive their data back.

Steps to Reduce the Risk of a Ransomware Attack

The vast majority of ransomware attacks are almost entirely preventable. Here are some steps businesses can take to reduce risk:

- **Patching and Updating:** Update software and operating systems with the latest patches and upgrade to the latest version of systems on a regular basis. Outdated applications and operating systems are the target of most attacks.
- **Training:** Train employees never to click on suspicious links or open attachments in unsolicited emails.
- **Network Access:** Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- **Filtering:** Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- **Blocking:** Configure firewalls to block access to known malicious IP addresses.
- **Backups:** Back up data on a regular basis. Keep the backups on a separate device and store them offline.

Even after taking the best and most careful precautions, an organization can still find itself the victim of a ransomware attack. Preparation for responding to and recovering from such an event should include:

- **Incident Response Plan:** Make sure you have an incident response plan and practice it regularly. It should include the names and contact information for the incident response team and external resources that will be needed to assess and remediate the incident and assist with notice to stakeholders and public relations. Legal counsel should guide the process to minimize risk of third party claims and assure compliance with legal requirements.
- **Insurance Coverage:** Businesses should have insurance coverage that will respond to a ransomware event. Coverage should include the costs of paying a ransom, hiring a forensic investigator, hiring legal counsel to coordinate the response, remediation, lost revenues, defending against and paying to resolve third-party claims and other expenses resulting from an attack. ■

William Denny is a Partner and Head of Cybersecurity, Data Privacy and Information Governance Practice Group at Potter Anderson & Corroon LLP.