The Rise of Cyber-Extortion, and How to Fight Back

*John F. Stephens, Corporate Counsel*

Sensational headlines about major data breaches have become common. The most typical scenarios are those in which hackers access personal data about a company’s customers and use that data for identity theft. But another type of fast-growing hack, so-called cyberextortion, may be even more damaging. In this type of attack, hackers essentially kidnap data and hold it for ransom, or threaten to reveal it to others.

For both companies and their customers, the rise of cyberextortion is alarming. There are, however, steps that can be taken to help mitigate risk (I have suggested several below). Companies that are proactive both pre- and post-breach are generally better positioned when it comes to protecting their customers’ data.

**Typical Scenarios**

There are, unfortunately, many methods of attack employed by cyber-extorters. For example, these criminals can initiate an attack far outside a company’s network through a denial of service (DoS). Here, thousands of “zombie” computers, taken over by hackers without the knowledge of the computers’ owners, are used to simultaneously bombard a target website, knocking it offline. DoS attacks can be especially damaging to enterprises such as e-commerce companies that rely on user access to their websites to conduct business.

Apart from DoS attacks, cybercriminals may seek to break into company’s networks. Once inside, hackers can follow any number of avenues to obtain data to extort money from their victims.

Tactics may also include: encrypting data that exist in business systems to prevent its use by the company or individual; disabling critical business systems; or blocking access to corporate sites. In each case, victims are severely handcuffed by hackers until a “ransom” is paid.

Hackers may also redirect part or all of a corporate website by altering DNS settings and holding the original destination hostage. Or, they may steal intellectual property and threaten to sell it to competitors. Hackers even pose as cybersecurity specialists and offer to identify weaknesses and fix them for a fee. Instead, they find exploitable weaknesses in corporate networks and threaten to notify the press or competitors unless payment is made.

The same malware used on individuals can be adapted for corporate espionage. Criminals might commandeer a computer microphone or camera in a boardroom or executive office to film or record confidential meetings. Using that business intelligence, hackers could extort a company, sell its secrets to rivals or manipulate company stock with calibrated releases of privileged information.

Perpetrators of these and other forms of cyberextortion range from organized crime rings to disgruntled employees. Indeed, attacks are even more insidious when launched from the inside.

**Sony**

The hack of Sony Pictures Entertainment in late 2014, prior to its release of the film “The Interview,” drew more attention than any previous cyberextortion plot and could ultimately cost Sony millions in revenues and reputational damage. The facts surrounding this breach and its potentially long-reaching impact have been widely reported.
For the purpose of this article, it is important to note that the average company may think a lower public profile protects it from such a potentially damaging event. But while the Sony hack was unprecedented in its scope and the public interest it generated, the assistant director of the FBI's Cyber Division said it was likely that 90 percent of U.S. corporations — large, midsized and small — are equally vulnerable to such an attack.

Ashley Madison

More recently, some 37 million users of Ashley Madison are now reportedly at risk for extortion after hackers stole information - including nude pictures and credit card data - from the site on the night of July 19. Hackers claim to have completely compromised the user database and financial records of the site, which caters to customers seeking extramarital affairs while retaining their anonymity.

A statement from Avid Life Media, the parent company of Ashley Madison, confirmed the hack and stated that personal information posted online by hackers had been deleted. It is unknown, however, how many people accessed the leaked and highly sensitive personal information before it was taken down.

A second, even larger Ashley Madison data dump of 9.7 gigabytes occurred on August 20. The hackers provided data revealing user names, emails, physical addresses, credit card numbers and more. All of that was quickly made searchable online. Hackers also revealed internal documents, worker salary data, and what seemed to be passwords to the company's PayPal accounts. A week later Noel Biderman, Avid Life’s CEO, announced his resignation.

Why Companies Simply Pay Up

While breaches like Sony Pictures and Ashley Madison dominate headlines, midsize companies actually may be the most vulnerable. For a number of reasons, smaller organizations may fail to invest in adequate security measures to protect themselves, fearing that even minor changes to day-to-day operations might jeopardize profitability. These companies may also lack the personnel or resources to effectively respond to cyberextortion attempts. They are, however, viewed as having deep enough pockets to attract extortionists.

The vast majority of cyberextortion attempts go unreported. When it comes to insider attacks specifically, three-quarters of the time companies deal with the matter internally and do not disclose the incident to authorities, according to a 2014 cybercrime survey by Carnegie Mellon University. To many companies, it appears cheaper and less disruptive to pay the ransom than to hire a third-party, or even devote internal resources, to respond to the breach. Many businesses simply can’t afford the loss of revenues if their site goes down and stays down for any length of time.

Alternatives to Capitulation: How Companies Can Become Proactive

While it can be tempting for a company to try to buy itself out of a problem, capitulating to terrorist-like demands also carries risks. There is never a guarantee that the criminals will not come back for more, and customers and business partners may lose confidence in the company should they discover that it paid off extortionists.

Additionally, paying a ransom does not address the underlying vulnerability the criminals exploited in the first place. Only an investigation, in conjunction with law enforcement experienced in such crimes, can reveal the weaknesses that allowed the attack to occur. It can also help to identify remediation that will prevent similar attacks, and it may reveal other weaknesses that can also be fixed.

How to Deal With Cyberextortion: Before and After It Occurs
Once a company or individual becomes a victim of cyberextortion, the number of good options dwindles quickly. Rather than react after the fact, corporate leaders need to have a response plan in place so mitigating the risk of cyberextortion schemes can be the main focus.

A comprehensive plan should include:
- A list of stakeholders to be informed.
- Predetermined and defined lines of communication that will speed information sharing.
- Appropriately trained and informed leaders empowered to make decisions during an incident.
- A process for the continuous updating of information technology systems and security policies (at least quarterly) to keep pace with changes in business and technology.
- Established relationships with law enforcement (local, state and/or federal) to reduce the chance of a slow, confused response.

Companies can also take a number of steps to lessen the likelihood that they will fall victim to these tactics:
- Identify all potential internal and external threats by:
  - Monitoring social media.
  - Staying on top of public forums related to your business.
  - Identifying employees who may want to harm your company.

- Audit computer networks to identify and assess vulnerabilities. Questions should include:
  - Are software patches being applied in a timely fashion?
  - Does the network have segmentation so that an attack in one area won’t impact others?
  - Are there access controls in place for your data?
  - Are network logs collecting sufficient detail and maintained for a long enough period of time to allow for proper historical investigation?
  - Do you know where all your endpoints are, and are network topology maps up to date? This is especially important because networks are dynamic. Companies continually add and remove servers and distribute new devices to employees.

The Bottom Line

Cyber extortion crimes will only grow more complex over time. Criminals are always changing their patterns of attack. While no company can protect itself perfectly, it can make smart investments in due diligence, response plans and sensible security based on rigorous risk assessments of what they stand to lose in the event of such an attack.

John F. Stephens is a partner in the Los Angeles office of Sedgwick. He can be reached at john.stephens@sedgwicklaw.com, or via the firm’s website—http://www.sedgwicklaw.com.