FOLEY & LARDNER LLP

Practical Strategies to Combat Common Cybersecurity Threats and Mitigate Risk

Jennifer L. Urban, Aaron K. Tantleff, Avi B. Ginsberg
22 February 2022

Innovative Technology Insights

What would you do if you woke up tomorrow and your company was experiencing a cybersecurity incident? What if IT systems were completely locked down? What if you could not use phones, check emails, or receive orders? What if you could not operate machinery or pay payroll? What if the sensitive, personal, and proprietary information your company stores was suddenly unavailable and potentially for sale on the black market? What loss would your company sustain each hour it was offline? What would you do if your company was the subject of a regulatory investigation? What would you do if the media exposed that your company was shut down due to a cyberattack? What would you tell the board of directors or your shareholders? Unfortunately, this is the reality many companies suddenly face when they become the victim of a ransomware attack.

In addition to being the victim of an attack by a threat actor, these companies may become the target of lawsuits alleging a variety of harms, including failure to deliver on contractual promises, exposure of sensitive information, and violation of various laws due to the company's allegedly negligent cybersecurity practices. Many of these lawsuits result in large settlements for plaintiffs, as reasonable cybersecurity practices are now the standard of care expected of all businesses. Unfortunately, many companies are not adequately prepared. The practical strategies in this article can help ensure your business is on the path to preparing for and safeguarding against a ransomware attack and other cybersecurity risks.

Ransomware: A Substantial Threat to Supply Chains

Ransomware attacks frequently made headlines in 2021 and had a substantial impact on many U.S. companies. In the first six months of last year alone, ransomware attacks on U.S. companies were up 148% from 2020. These attacks were responsible for impacting the availability of gasoline up and down the East Coast, disrupting multiple meatpacking plants, and as the year came to a close, causing a cream cheese shortage (which frustrated bagel shops along with both home bakers and professional bakeries trying to make traditional holiday treats such as cheesecake and Christmas cookies). While numerous cybersecurity threats affect companies, such as phishing attacks and software vulnerabilities, these threats are now being utilized as a vector to infiltrate company systems and launch ransomware attacks.

Supply chains are a prime target for ransomware attacks. The cybercriminals that perpetrate these attacks (threat actors) are smart, organized, and creative. They frequently research their victims and target the

companies they believe will be most likely and able to pay a ransom. Increasingly, they are targeting industries and companies that they believe will be substantially affected by downtime. The just-in-time nature of many parts of supply chains makes them prime targets for these attacks, as threat actors know such companies cannot afford to be offline for several days or weeks and are more likely to pay a ransom to get back up and running as quickly as possible.

The U.S. Federal Government and many other governments are increasing efforts to combat ransomware, including issuing statements and guidance for the public and private sectors. For example, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) recently published guidance on 2021 global ransomware threat trends and mitigation tactics detailing ways in which ransomware tactics and techniques continued to evolve, and specific steps organizations can take to combat "ransomware threat actors' growing technological sophistication" and the increased ransomware threat to organizations globally. Unfortunately, due to rapidly evolving technologies, changing global payment systems, and countries that harbor cybercriminals, ransomware is a pervasive threat that is extremely difficult to eradicate. This means it is vitally important for all companies to understand how a ransomware attack could impact their operations, take steps to minimize the chances of an attack occurring, and make changes to minimize the potential damage should an attack occur.

Costs of a Ransomware Attack

Ransomware attacks can be devastating. Most companies cannot operate without computers — they control key machinery, keep track of production and orders, and operate safety systems, such as clean air systems, necessary for production. Yet ransomware can lock down computer systems in a matter of minutes, making them inoperable and rendering important information inaccessible. Further, confidential information may be stolen and, in some cases, published online or sold on digital black markets. Companies are then faced with a tough decision: pay a ransom to unlock their computer systems and prevent confidential information from being leaked or try to erase and restore systems from backups.

The obvious impacts of a ransomware attack are the costs and risks associated with production downtime and the cost of a ransom payment. Companies may be wholly or partially unable to operate while systems are locked down by ransomware. Ransom amounts typically range from several hundreds of thousands to millions of dollars, and even after payment, it can take days to fully restore computer systems. In addition to these costs and risks, there are many less-obvious costs:

- Restoring Computer Systems. Restoring computer systems can be costly. Even if the ransom is paid, trained professionals may need to be hired to properly use the specialized software provided by the attackers to restore systems to their pre-attack working state. In addition, companies that suffer a ransomware attack typically hire a computer forensics vendor to determine exactly how their systems were infiltrated and what actions the attackers took while inside so they can be remediated to prevent additional attacks in the future. (If you leave the back door open, you will likely be attacked again.)

- Legal Compliance. Depending on the systems and information impacted by ransomware, a company may be required to comply with various state data breach notification requirements, U.S. Department of Defense notification requirements, and other applicable laws. In addition, before paying or making a promise to pay a ransom, companies must conduct diligence to ensure payment is not prohibited by U.S. sanctions. The cost of legal compliance is highly fact-specific and can range from a few thousand dollars to hundreds of thousands, depending on the implicated laws and requirements.
- Subsequent Litigation. If personal information, such as certain information contained in a typical employee human resources file, is exfiltrated during a ransomware attack, lawsuits may be filed against the company. Resolving such suits can be costly.
- Contractual Violations. Production delays due to a ransomware attack frequently violate contractual requirements as companies are unable to meet obligations to their customers. Depending on the terms agreed upon, a company may be liable to its customers for the customer's lost profits due to the delays, a multiple of the cost of the product, or the cost for customers to temporarily find a new supplier if one is available. There may be additional liability if the unavailability of inputs or component parts causes a ripple effect resulting in delays downstream.
- Reputation Impact. Production delays can make a supplier appear unreliable, potentially resulting in customer distrust and loss of future business. In addition, after infecting a company with ransomware, threat actors may contact the company's customers or business partners to inform them of the ransomware attack to increase pressure and extort a larger ransom payment, resulting in additional reputational damage.

Practical Cybersecurity Strategies to Mitigate Ransomware and Other Risks

Ransomware is one of several common cybersecurity risks companies face today. Risks such as theft of intellectual property, insider threats, and business email compromises — in which a threat actor gains access to company email account(s) and uses that access to perform malicious actions such as misdirecting funds, changing order terms or recipients, or stealing sensitive information — are increasingly common. By employing these practical cybersecurity strategies, companies can mitigate risks associated with ransomware and many other types of cybersecurity risks.

1. Keep Computers and Hardware Patched and Up to Date. Attackers frequently use vulnerabilities in software to infiltrate company computer systems and launch ransomware attacks. Many of these attacks are avoidable by regularly installing updates and patches that fix security flaws. It is crucial to keep all network and internet-connected devices up to date, including computers, smartphones, tablets, routers, firewalls, and "smart" technology, including sensors, lightbulbs, and hubs. In addition, industry standard antivirus software should be used on all computers and kept up to date.

2. Plan Ahead. Your company should have an up-to-date incident response plan covering all types of

cybersecurity incidents. Due to the large uptick in ransomware, many companies also find it helpful to have a ransomware-specific policy in place. These documents help to ensure an orderly and efficient response to a cybersecurity incident, which can substantially reduce legal risk and other costs. Legal counsel can assist with drafting or revising these plans and policies to ensure they meet current industry standards and regulatory guidance.

3. Do Not Allow Personal Devices to Connect to Company Networks. If your company provides internet access to employees or customers, create an isolated guest WiFi network for them to use. Do not allow them to connect to the same network used by company computer systems.

4. Regularly Train Employees on Cybersecurity Risks. Ensure training covers topics such as ransomware, phishing, spear phishing, social engineering, and forged emails. Employees are frequently the "weakest link" in company security, and untrained employees are more likely to fall for targeted attacks.

5. Practice Responding to an Incident. One of the best ways to improve your company's response readiness is to regularly practice responding to an incident. Tabletop or mock incident response exercises help a company to identify weaknesses in its response plans and prepare incident response team members ahead of a ransomware attack or other cybersecurity incident. This way, if the company is affected by a ransomware attack, critical mistakes can be avoided and incident response team members will be prepared for their duties despite the chaos. Experienced cybersecurity counsel can assist with designing and conducting tabletop incident response exercises.

6. Require All Employees to use Multifactor Authentication. Employees should be required to use multifactor authentication on all accounts provided by the company, including computer, email, and VPN accounts.

7. Limit Employee Access. Each employee's computer account should be configured with the minimum amount of access required. Do not give employees administrator access unless they are trained IT professionals who require such access. Do not allow general employee accounts to install unapproved software or make changes to system settings. Do not allow employee accounts general access to file shares or servers unless such access is needed. Restrict file share access to specific folders where possible. Less access means more difficulty for an attacker if they obtain and try to use an employee's login credentials.

8. Allow Remote Login Only for Employees That Need It. Ensure only specific employees with a need for remote access can log into VPN or remote desktop services.

9. Regularly Backup Systems and Store Backups Separately. Backups should be kept on a different system (on a different network or offline), or stored with a secure cloud backup provider, to prevent

ransomware or other malicious code from impacting the availability of backups.

10. Segment Your Network. Consider moving critical systems to a separate network from the general network used for email, order processing, etc. This helps prevent ransomware and other malicious code from spreading to critical systems and may help avoid a total business shutdown in a ransomware attack.

11. Use Email Filtering Software. Software that filters out malicious links and phishing attacks is an excellent first line of defense and can make it more difficult for attackers to reach employees and infiltrate systems.

12. Ensure IT has an Adequate and Properly Utilized Budget. Upgrading software and hardware can be costly, but generally it is substantially cheaper than a ransomware attack. Ensure your company's IT team has an adequate budget for cybersecurity and that they proactively utilize it to improve your company's cybersecurity defenses. Ask them if your organization follows the IT guidance in this section and how they have prepared for a ransomware attack or other cybersecurity incident.

Industry-Specific Concerns

Ransomware and other cyber risks have the potential to impact virtually every industry. However, many industries have unique concerns. For example, if a health care provider suffers a ransomware attack, the incident may be a reportable breach under HIPAA regardless of whether sensitive data was exfiltrated, and the provider should consult the Office of Civil Rights Ransomware Guidance to help determine its legal obligations. Companies should consult experienced cybersecurity counsel and industry-specific guidance published by authoritative sources, such as regulatory bodies and trade associations, to help ensure they are aware of concerns specific to their industry.