DECEMBER 16, 2020

Legaltech news©

ONLINE

An ALM Publication

Ransomware as Reminder: Back to Basics of Cyber Readiness

Despite the unique threats posed by ransomware, basic cybersecurity measures and a strong cyber risk reduction strategy remain the most valuable tools to prevent an attack and shape a strong response if (or when) one happens. Here's five tips to get started.

BY MICHAEL F. BUCHANAN AND ALEJANDRO H. CRUZ, PATTERSON BELKNAP WEBB & TYLER

Credit: Khakimullin Aleksandr/Shutterstock.com

The growing threat from ransomware is forcing organizations to re-think their cyber risk mitigation strategy. As private organizations and governments look ahead to 2021 and the risks they face in an increasingly uncertain world, ransomware will no doubt rank high on any list. Ransomware attacks involve the use of malware that encrypts the victim's computing system, rendering files and data inaccessible until a demand for payment is met, and a decryption key is provided.

In a recent twist, certain ransomware attackers are increasingly threatening to release the victim's data publicly if demands are not met. The incidence of ransomware attacks increased 37% year over year between 2018 and 2019, with an associated increase in ransomware-related losses of 147%. And the threat has only grown in 2020 with a 20% increase in reported ransomware attacks globally and a 109% increase in the U.S. The so-called "professionalization" of ransomware criminal enterprises is also on the rise, including guaranteed turnaround times, real-time chat support for victims, and payment demands customized to a victim's financial profile.

Despite the unique threats posed by ransomware, however, basic cybersecurity measures and a strong cyber risk reduction strategy remain the most valuable tools to prevent an attack and shape a strong response if (or when) one happens.

Ransomware attacks are devastating for any organization, both operationally and financially. Indeed, recent attacks on hospitals have left no doubt that for certain organizations, lives can depend on a company's response. The effects of a successful ransomware attack, moreover, can ripple far and wide into potential breach notifications, regulatory reporting and investigations, and litigation against the victim company. Substantial regulatory concerns can further complicate the situation. For example, recently, the U.S. Department of the Treasury's Office of Foreign Assets Control and the Financial Crimes Enforcement Network notified ransomware victims and advisors that they may face investigations and penalties for paying or facilitating payments to individuals or entities on the Specially Designated Nationals and Blocked Persons List. Consequently, companies that have fallen prey to the global ransomware industry face months, and in some cases years, of business, legal, and reputational fallout.

To be sure, the proliferation of ransomware—and its zero-sum dilemma for victim companies—presents unique economic, operational, and philosophical questions for enterprises faced with a demand for money in return for a key to the lifeblood of their business. The decision to pay implicates fiduciary responsibilities of management and board members, a company's ability to pay, availability of insurance, the potential for release of data, exposure to potential regulatory violations, and, at bottom, whether the enterprise can reasonably trust a criminal counterparty to deliver on a bargain. Nonetheless, ransomware attacks share the core characteristics that shape the risk profile of any cyber event:

- Unauthorized access to a private digital environment;
- Potential for unauthorized manipulation and/or exfiltration of data;
- Potential loss of data and business disruption;
- High remediation costs;
- Lengthy life cycle, from initial breach to conclusion of related investigations and litigation;
- Legal and regulatory exposure; and
- Potential for severe financial and reputational harm.

These common threads are a reminder of the touchstones of a sound cyber risk strategy, and first principles may light the way to meeting the evolving threat of ransomware.

1. Provide the Right Tools

Information security teams need substantial resources to prepare and educate employees about cybersecurity risks and the internal policies necessary to maintain digital security. Policies and technical controls need to be audited periodically—and all audits and monitoring need to be documented—to ensure they remain reasonable and appropriate over time. Especially in the virtual environment brought on by the COVID-19 pandemic, companies need to be especially mindful to secure systems that enable remote access and ensure that VPNs and other remote access tools are up-to-date and fully patched.

Notably, improperly secured remote desktop protocols have long been the exploitation of choice for ransomware threat actors. The use of personal devices and email accounts should be centrally controlled and monitored through policies and technological solutions to minimize the risk of additional—and unknown—vulnerabilities. Indeed, an increasing number of states are passing laws requiring that companies implement reasonable security measures for their data (for example, New York's SHIELD Act).

2. Know Your Enemies

Criminals know that humans can easily (and unwittingly) be used to bypass the raft of technical controls in place to secure an organization's network. Continuing education and training at all levels of an organization is an opportunity to teach people to recognize phishing schemes, social engineering, and other insidious means of infiltration.

Cybercriminals, especially those seeking to deploy ransomware, are becoming increasingly sophisticated and flexible in their methods of attack; all members of an organization need to be vigilant to stop the enemy at the gate. Timely trainings that are fully and properly documented can also help to rebut allegations—following an attack—that the organization, including its officers and directors, did not take reasonable care in implementing an effective security plan.

3. Don't Trust Your Defenses

Technical and operational cyber defenses can be highly effective against ransomware and other threat vectors, but only until they are breached. The recent infiltration of cybersecurity firm FireEye is a prescient reminder of how quickly the tables can turn. Be prepared for an inevitable infiltration.

On top of an incident response plan, all enterprises should maintain robust and reliable back-ups of their critical network assets. Multiple copies of these back-ups, especially those containing sensitive or proprietary data, should be fully encrypted and maintained in a physically separate, secure location. Testing the integrity and restoring a network from back-ups can be time-consuming and resource-intensive, but secure, high-quality back-ups (and the ability to use them) can tip the calculus in negotiating a ransom. Businesses also need to inventory and map their data to facilitate determinations, in the case of a breach, as to what data was affected and whether those effects trigger notice obligations.

4. Have a Plan and Practice

The most important aspect of any cybersecurity response and legal strategy is intensive planning and preparation. Organizations need to be prepared for the worst with a robust incident response plan addressing a range of potential cyber events, with contingencies for, among other things, response leadership, lines of communication, and business continuity protocols.

These plans should be approved and implemented at every level of response, including the board and C-suite, information security staff, human resources, and public relations. And the plan must be regularly rehearsed to ensure smooth implementation should an event occur. Board and management involvement in creating the plan, moreover, will help when it comes time to defend against derivative suits arising from a ransomware incident or other negative cyber event.

5. Know Your Friends

The moment of infiltration is not the time to seek out the professionals who will guide the organization through the crisis and its aftermath. Company management and in-house counsel should engage experienced counsel, forensic investigators, and technical remediation experts as part of the advance planning process. Counsel will be critical in shaping decisions that will play out in public disclosures, investigations, and litigation down the road, as well as ensuring that all appropriate professional engagements and communications are properly protected by applicable privileges. Management will also need to coordinate with the organization's insurer on notice and any conditions of coverage, including the involvement of pre-approved experts and counsel. And finally, law enforcement contacts can be an important factor should the company decide to report an attack to government authorities. Early involvement of seasoned professionals to guide the organization through an incident can pay dividends in harm reduction, cost mitigation, and narrowing the field of long-term risk.

Ransomware takes its victims down a path riddled with risk and uncertainty. Re-thinking the essentials of a company's cyber risk strategy, both as to ransomware and digital security threats more broadly, will create an opportunity today to enhance the business and legal pathways available when the worst comes to pass.

Michael F. Buchanan *and* ***Alejandro H. Cruz*** *are partners in Patterson Belknap Webb & Tyler's Privacy and Data Security group. They represent clients in a wide range of cybersecurity and litigation matters, including responding to and investigating data breaches, complying with federal and state regulatory requirements and defending clients in class action matters resulting from cybersecurity incidents.*