The Computer & Internet Lawyer

Volume 38 ▲ Number 9 ▲ October 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Top 7 Issues All General Counsel Need to Know About Ransomware

By Kimberly Kiefer Peretti and Katherine Doty Hanniford

Ransomware has become a multibillion-dollar criminal industry that is projected to cause as much as $20 billion in global damages to companies in 2021. Ransomware attacks can result in disrupted or even crippled operations, as seen most recently in the ransomware attack against a major oil pipeline supply chain company. As companies continue to enhance their security and restoration capabilities to prevent or minimize the impact of a successful attack, ransomware actors likewise continue to escalate threats and adapt their tactics to overcome these measures.

1. Payment Will Not Result in Zero Impact

According to the Ponemon Institute, the cost of lost business is the largest cost factor in determining the total cost of a data breach, and irrespective of whether a ransom is paid or whether data is restored from backups or via a decryption tool, ransomware attacks typically involve significant downtime – and that downtime is increasing. A reputable third-party ransomware intermediary has reported that the average downtime following a ransomware attack increased from 19 days in the third quarter of 2020 to 21 days in the fourth quarter of 2020 regardless of whether the company paid for a decryption key. Is your company prepared to be "down" for over three weeks?

In addition, paying a ransom generally does not guarantee that a company will be able to restore all of its data immediately, or at all. Several factors – including the ransomware variant, the threat actor group, and the configuration of the company's systems – can contribute to whether a company will be able to partially or fully decrypt its data if it is not in a position to restore its system and data without paying for a decryption key.

The likelihood of downtime and the inherent uncertainty surrounding restoration following a ransomware incident have resulted in an increasing need for robust incident response and resilience planning. In particular, companies may be especially well-served by

Kimberly Kiefer Peretti, a partner at Alston & Bird LLP, is co-leader of the firm's Privacy, Cyber & Data Strategy team. **Katherine Doty Hanniford** is a senior associate on the firm's Technology and Privacy, Cyber & Data Strategy teams. The authors may be contacted at *kimberly.peretti@alston.com* and *kate.hanniford@alston.com*, respectively.

incorporating a ransomware playbook into their existing incident response plans and ensuring their incident response teams have practiced multiple ransomware scenarios in tabletop exercises, for example.

2. Check Your Cyber-Insurance Coverage . . . and Be Prepared for the Renewal Process

The increasing frequency of ransomware attacks and rising amounts of ransom payments have placed renewed focus on the particulars of cyber-insurance coverage. As the New York State Department of Financial Services ("NYDFS") identified in its recent guidance and cyber-risk framework for underwriting such insurance policies, the industry is facing both silent and systemic risk associated with the proliferation of ransomware incidents.

According to the NYDFS, some policies are unclear or ambiguous about their coverage of cybersecurity events (hence, silent risk); and other policies explicitly cover certain costs associated with cybersecurity events, but the unexpected severity of those events has contributed to industry-wide strain across insurers (systemic risk).

Because the increasing amount of ransom payments has placed strains on the insurance industry, insureds can expect that the underwriting and renewal processes may be more rigorous than in previous years. Indeed, as companies seek to acquire new cyber-insurance policies or renew existing ones, the insurers' enhanced diligence procedures may require additional disclosures or the implementation of new or more stringent cybersecurity procedures to meet the insurer's standards. Policies can often require a checklist of specific security controls to be in place and periodically tested for effectiveness, for example, which are designed to mitigate the risk of ransomware.

Other insurers are taking different approaches. Just recently, one European insurer announced that it will no longer issue cyber-insurance policies in France that reimburse insureds for ransom payments.

There is also the risk that an insured company may find that its policy's pre-approval process for the retention of outside counsel, forensic experts, ransom payment facilitators, and even the potential ransom payment itself is in tension with the company's interest in a swift and immediate response to a ransomware event. The extent to which the policy includes recovery costs can pose an additional challenge if a policy does not treat expenses related to the forensic investigation, ransom payment itself (if applicable), and rebuilding affected systems as covered recovery costs.

3. Double Extortion

As companies grapple with the challenges associated with improving security and recovery capabilities, organized criminal groups associated with ransomware attacks have undergone a period of reorganization and shifting of tactics that may frustrate response efforts.

For example, in the second half of 2019, threat actors began using a wider range of techniques to incentivize the payment of ransom, chiefly by exfiltrating data before execution of the ransomware and then threatening to post victims' identities and data through online "shaming" boards. This trend accelerated in 2020 and into 2021. According to a security firm, the percentage of ransomware attacks that involved the threat to release stolen data on the dark web increased from 50 percent in the third quarter of 2020 to 70 percent in the fourth quarter. Are you prepared to have your sensitive data leaked on a criminal site?

Forensic and threat intelligence firms also report that threat actor groups have shifted the type of information targeted for encryption or exfiltration in attacks. Whereas individuals' personal information has long been targeted, recent incidents such as the Accellion FTA breach highlight the extent to which sensitive corporate information and intellectual property are valuable targets.

4. Paying the Ransom Might Not Be an Option

Both U.S. financial regulators and insurance companies have recognized the proliferation of ransom demands and staggering amounts of cyber-extortion payments when viewed in the aggregate, and this recognition marks a watershed in the approach to ransom payments as a result of recent regulatory guidance and increased expectations for compliance.

More specifically, the October 2020 guidance from the Office of Foreign Assets Control ("OFAC") and Financial Crimes Enforcement Network ("FinCEN") alerted companies to the compliance risks of making or facilitating ransom payments that involve any individual or entity listed on OFAC's Specially Designated Nationals and Blocked Persons List ("SDN List") or a comprehensively embargoed jurisdiction and offered a total of 12 ransomware variants, threat actor groups, and blocked persons as examples of OFAC-designated malicious cyber-actors on the SDN List. Among those listed is Evil Corp, an active threat actor group that has continued to perpetrate ransomware attacks, most recently using different malicious code in an ultimately

unsuccessful attempt to evade OFAC sanctions. But for victim organizations, this example underscores that the impact of the SDN List and the corresponding need for enhanced compliance procedures is not a theoretical risk.

OFAC has affirmed that it will continue to impose sanctions on threat actors and those "who materially assist, sponsor, or provide financial, material, or other technological support for these activities" and noted the corresponding need for companies' compliance programs to consider and mitigate this risk when contemplating a ransom payment. Accordingly, there are circumstances where even if a company was inclined to pay the ransom to mitigate the risk to impacted data, it may not be able to lawfully do so.

As OFAC and FinCEN increase their scrutiny of such payments, insurers and some third-party payment facilitators have similarly bolstered their compliance procedures to insulate themselves from further risk. For example, some third-party payment facilitators now maintain a more stringent "no-fly" list than the OFAC SDN List.

Some insurance companies will now require more rigorous certifications of compliance with not only the OFAC SDN List but also other extraterritorial provisions, including anti-terrorism watch lists. Consequently, there are additional circumstances where even if a company may be able to lawfully pay the ransom, third-party payment facilitation or insurance reimbursement for the payment may be unavailable.

In sum, companies are well-served by preparing for circumstances where a company is precluded from payment – either as a matter of legal compliance or company policy or due to other practical or contractual considerations.

To further exacerbate the situation, because ransomware attacks are now frequently a two-step extortion process, in which payment is demanded in exchange for a decryption key and then to prevent data leakage of any exfiltrated data, the consequences of nonpayment can be significant. In instances where ransomware payment is not an option and data has been exfiltrated before encryption, the need for secure backups and a comprehensive incident response plan as a starting point for recovery is especially important.

5. U.S. Law Enforcement Is Shifting Its Approach

Recent government actions signal a recognition that the ransomware threat has become pervasive and is not one that can be solved through traditional criminal indictment alone. In April 2021, the Department of Justice ("DOJ") announced the formation of a ransomware task force designed to promote information sharing and coordination across the DOJ to respond more aggressively to the ransomware threat. Although in its nascency, the task force is intended to target the ransomware threat holistically, using all DOJ tools at its disposal, from prosecution to disruption of ongoing attacks and the services that facilitate and support them to information sharing. The task force is also intended to increase DOJ coordination with other federal agencies, including the Cybersecurity and Infrastructure Security Agency ("CISA") and Treasury, as well as with the private sector.

The creation of the task force and its focus on increasing opportunities between the public and private sectors to exchange threat intelligence build upon prior federal efforts to raise awareness and combat ransomware. For example, the FBI National Cyber Investigative Joint Task Force ("NCIJTF") released a ransomware fact sheet in February 2021 to share information in coordination with 15 other U.S. government agencies.

Similarly, CISA launched a Reduce the Risk of Ransomware Campaign in January 2021 to encourage public-private information sharing and cybersecurity best practices to mitigate risks associated with ransomware. Ostensibly, the new DOJ task force will be able to consolidate these efforts while also leveraging its existing legal authority to step up its efforts to disrupt and apprehend malicious actors.

The FBI operation in April 2021 that relied on credentialed, remote access techniques to access, copy, and remove malicious code from networks susceptible to Microsoft Exchange zero-day vulnerabilities via the execution of search warrants may be one such innovative use of existing legal authority that the DOJ is willing employ to thwart malicious cybersecurity threats going forward.

6. Expect Increased Obligations as a Result of the May 12, 2021, Executive Order

The Biden Administration released a lengthy executive order on May 12, 2021, designed at least in part to respond to the supply chain risks associated with ransomware incidents.[1] The executive order is broadly geared to address cybersecurity supply chain risk across the federal government and is likely to create a series of digital safety standards with which federal agencies and their contractors will need to comply. These standards may include certifications of the integrity of their software, information systems, and vulnerability management provisions, with additional reporting requirements and penalties for violations.

In addition, government contractors may be expected to share threat intelligence and report data breaches to CISA, which going forward will centrally collect and manage such information. As agencies work to enshrine the executive order's recommendations and the associated additional requirements take effect, organizations may see a ripple effect of enhanced procedures and standards – whether in the form of revised contractual language or direct federal regulation.

7. Proliferation of Guidance . . . It's Back to the Basics

Organizations have no shortage of guidance available to them from law enforcement and regulatory authorities regarding the ransomware threat and steps to mitigate it. Recent guidance spans the joint U.S. Secret Service and banking authorities' Ransomware Self-Assessment Tool ("R-SAT") to the Security and Exchange Commission's Ransomware Risk Alert to the joint FBI and U.S. interagency guidance to HHS's Ransomware Fact Sheet to CISA's MS-ISAC Ransomware Guide. A common thread that runs through ransomware guidance – irrespective of an organization's market sector, size, or nature – is the importance of certain security controls that fall squarely within basic cyber-hygiene and well-established principles of reasonable security.

Initial guidance on earlier ransomware variants focused on the need for reliable backups; however, the additional threats posed by data leakage, targeted attacks, and increased guidance (and therefore increased expectations for resiliency) have prompted a corresponding focus on basic cybersecurity controls that can be especially helpful in preventing or minimizing the impact of ransomware incidents.

Although maintaining proper backups continues to be a core measure to reduce the amount of downtime, additional measures include minimizing the potential success of phishing incidents, which can serve as a gateway incident to more serious ransomware attacks, by implementing email security measures such as multi-factor authentication and increased training, including simulated phishing emails, to ensure users are appropriately aware of the risks.

Organizations should consider disabling remote desktop protocol ("RDP") access because it permits attacks to circumvent endpoint detection tools and facilitates easier lateral movement within a network. In addition, patching vulnerabilities according to manufacturer's specifications and applying the latest updates may prevent vulnerability exploitation. Given the trend for zero-day vulnerabilities to be exploited, it may not be sufficient to rely on traditional patch management schedules.

Conclusion

Although the government's increased focus on information sharing and law enforcement may benefit companies as they bolster their cybersecurity preparedness, the evolving threat tactics associated with ransomware attacks continue to pose practical challenges for companies.

In situations where either the company's backup capabilities or ability to pay the ransom to prevent data leakage is suboptimal, a ransomware event's impact on the victim company now easily reaches "mega-breach" proportions. This is especially true when a company faces a costly recovery process that can include a ransom demand, technical restoration, a forensic investigation, dark web monitoring, and legal notifications – costs that may or may not be covered by a cyber-insurance policy.

And while certain aspects of the ransomware threat landscape are beyond a company's control – in particular the ransomware variants and threat actor group tactics – factors such as insurance coverage, the sufficiency of existing security controls in light of current threats, OFAC compliance, incident response planning, and information sharing arrangements can be addressed proactively by a company in the course of its incident response planning and preparation efforts.

Note

1. *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.*