Ransomware: Mitigating Risk and Avoiding Mistakes

Ransomware has come a long way since the 1989 "AIDS Trojan." Distributed by diskette, it encrypted the file names and directories of its victims. Ransom demands have also come a long way. The AIDS Trojan attack demanded $189 for the decryption key. In 2019 ransomware demands topped $12MM.

As the CrowdStrike 2020 Global Threat Report succinctly puts it: "Ransom demands grew larger. Tactics became more cutthroat." Particularly cutthroat has been the advent of encryption cum exfiltration.

More or Less Reason to Pay?

Historically, ransomware attacks were focused on the payoff, not acquiring information. This changed in late 2019.

Maze ransomware was observed by the FBI to hit its first US victims in November 2019 (BleepingComputer.com). These attacks not only looked to extort a ransom via encryption; the hackers also threatened to sell or publish the stolen data and name the victims if a ransom was not paid. In some Maze attacks proof of exfiltration was provided by showing the victim some stolen documents. Additionally, CrowdStrike notes in their report that they were able to detect a data exfiltration tool that included "the ability to search for keywords within files, including words related to sensitive information." These proofs of exfiltration raise an interesting point. What exactly are you buying if you pay the ransom? You cannot accept the promise that your data will be destroyed and not disclosed or sold. This is not a tenable position. Even if the data is not publicly disclosed, it must be assumed that the hackers will, or already have, monetized the information.

Furthermore, you may be contractually obligated to report the breach to clients and obligated by regulation to notify customers and regulating authorities. Coveware notes that not all of these attacks have been accompanied by exfiltration proofs, raising the possibility that this gambit is a bluff. Deciding to call this bluff, however, would no doubt require strong counsel and an assessment of the legal, business, and reputational risk.

Consequently, combining traditional ransomware with data theft may actually *decrease* the likelihood of a ransom being paid. Given reporting requirements, what is to be gained by paying? A quicker restoration of data to a thoroughly compromised environment?

> *"An alarming trend in targeted ransomware operations is the compromise of managed service providers." —CrowdStrike*

Ransom Payment: Value for Money?

Where exfiltration of data has occurred, a strong case can be made that payment of a ransom is disincentivized, if not altogether pointless. But what of traditional ransomware attacks that do not involve data exfiltration? Is there *value for money* in paying the ransom?

It is important to note that even traditional attacks focused on a ransom payoff and not acquiring information for extortion purposes still pose a real risk of data being stolen. Attackers will canvas your infrastructure looking for *targets of opportunity* such as password lists, bank account information, and other financial data, enabling the attacker to make fraudulent transfers.

It's Just the Tip of the Iceberg

The ransom is really just the tip of the iceberg of cost and pain associated with ransomware attacks. Ironically, it represents, on the one hand, *a minor cost* in terms of the expenses incurred in responding to the attack. Yet, on the other hand, it is *exorbitant* in terms of what it buys: presumably, quicker access to data but this is never guaranteed. One might argue that the only potential "value" to paying a ransom is as *hush money* in a dangerous gambit to avoid reputational damage.

Ultimately, whether you pay the ransom or not, remediation expenses and other hard and soft costs remain. These costs will likely dwarf even eight-figure ransom demands. Keep in mind that these large ransoms are demanded from organizations with extensive technology infrastructures and highly valuable reputations that are equally expensive to maintain, let alone remediate following a successful attack.

Legal Technology Services Firms Be Warned

The CrowdStrike 2020 Global Threat Report contains a missive that should reverberate within the legal technology services community and the clients they serve:

"An alarming trend in targeted ransomware operations is the compromise of managed service providers (MSPs) ... [which] can enable the spread of ransomware to many companies from a single point of entry ... [impacting] cloud service providers."

By way of example, suppose an eDiscovery company is hosting data that includes PII and that data is compromised in a ransomware attack. The company has to discover what data was involved and what sets of data constitute PII. Both the service provider (the data processor) and the company whose data is resident on their system (the data owner) are subject to the breach and must respond.

It is within this context that we can enumerate the *true cost* of a ransomware attack, the ultimate triviality of the ransom amount requested and, conversely, its exorbitance relative to value (or lack thereof). Consider the cost calculus:

1. Loss of revenue during downtime
2. Reputational damage and consequent loss of business
3. Fees to cyber security and forensic experts to trace the origin and propagation of the attack
4. Establishing a clean environment in which to restore your data
5. Establishing temporary employee systems in which to work
6. The cost of uncompensated rework
7. Paying for forensic analysis at the client's organization whose data was compromised at the service provider or accessed through an MSP
8. The cost of notifications and credit monitoring and ensuing cost of DSAR response management
9. Performing all necessary curative activities to impede future attacks
10. The likely fights with your insurance company which will audit your adherence to "acceptable" security protocols
11. Legal fees
12. The time senior management spends on this issue rather than running the company

In the final analysis it is not the ransom. Rather, it is the costs associated with the failure to prevent the attack and the consequent remediation that may prove to be a real company killer. And perhaps reputational damage is the *coup de grâce.*

To learn more and further understand how to mitigate risk, avoid extensive mistakes and have more predictable outcomes visit QuisLex's website today.

Michel Sahyoun has over 20 years of experience in risk management and designing, building, and deploying mission-critical applications for Fortune 500 companies. He is the CTO of QuisLex leading their technology, security, data

protection efforts and heads the technology innovation group. Prior to joining QuisLex, he was vice president and senior architect of risk management at JP Morgan Chase. Michel holds Master of Engineering degrees in both Computer Science and Operations Research from Columbia University.