ALSTON & BIRD

Privacy, Cyber & Data Strategy ADVISORY

FEBRUARY 23, 2024

Top 10 Issues General Counsel Need to Know About Ransomware in 2024

by: Kim Peretti, Kate Hanniford, Alysa Austin, and Lance Taubin

Ransomware continues to be a multibillion-dollar criminal industry, with a record-breaking $1 billion in ransom reported paid in 2023. Ransomware incidents have proven their potential to disrupt and even cripple operations across industries, including industrials and manufacturing, health care, financial services, and retail/hospitality market sectors. Indeed, as organizations continue to enhance their ability to detect and prevent ransomware from being deployed, and restore systems and data if ransomware is deployed, ransomware actors likewise continue to adapt their tactics and often forgo the ransomware deployment and focus instead entirely on data extortion. More recently, ransomware actors are deploying "timed wiper malware," allowing the threat actor to not only encrypt the data but also wipe it permanently. As the ransomware threat landscape continues to rapidly evolve, here are top 10 challenging dynamics that may need to be managed in a ransomware incident.

1. 2023 Was a Record Year for Payments

Ransomware incidents and their related extortion attempts will be a known risk for the foreseeable future and show little sign of abating. According to Chainalysis, ransom payments alone exceeded $1 billion in 2023. This amount does not include business impact costs; productivity losses; costs of the forensic investigation; individual, regulator, and contractual notifications; legal fees; and remediation. This is a significant uptick from 2022, when reported ransom payments totaled approximately $567 million, and a slight increase from 2021, when reported ransom payments totaled $984 million. Further, while reports vary, the average ransom payments are quite significant—Coveware, a reputable ransomware intermediary, reported that the average ransom payment for Q3 2023 was $568,705, whereas Sophos's "The State of Ransomware 2023" report found that the average ransom payment almost doubled from $812,380 in 2022 to $1,542,333 in 2023. On top of the ransom payment, IBM's "Cost of a Data Breach Report 2023" found that the average cost of a ransomware incident was $5.13 million, an increase of 13% from 2022.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

2. Execution with Precision and Speed

The rise in ransomware incidents and increase in ransom payments has been proportional to the increasing sophistication of threat actor techniques and their corresponding speed in executing the attack. Once the threat actor gains access to an organization's system or network, it is frequently able to identify confidential and sensitive data by way of an automated script, exfiltrate the data, and then deploy the ransomware to encrypt the systems and data, all within a day or a few days. Of course, the speed of the incident may vary, but the ransomware actor often operates with surgical precision to access and exfiltrate the data, and then deploy the ransomware.

According to Mandiant, the average "dwell time"—which is calculated as the number of days an attacker is present in a victim's environment before detection—for a ransomware incident in the U.S. is just five days, compared to the average global dwell time for all types of incidents, which is 16 days. The need for robust, comprehensive security tooling, along with 24/7 resources to help detect, investigate, and respond to any potential ransomware actors, is becoming increasingly essential. At the same time, the window for organizations to detect an intrusion before data theft and ransomware deployment occurs is narrowing.

3. More Affiliates = Less Predictability

In 2023, we witnessed the vast majority of major ransomware criminal actors pivoting their business models to a "ransomware-as-a-service" (RaaS) offering, which creates numerous affiliates of each ransomware gang. Zscaler reports that there was a 37% year-over-year increase in ransomware incidents in 2023, and this increase was largely driven by RaaS. Essentially, this model allows for the affiliate to leverage the ransomware gang's variant, tools, access to data leak sites, negotiation assistance, and other support to conduct the attack and receive in exchange a percentage of the ransom payment (up to 80%). This RaaS model has resulted in a lower cost of entry for aspiring cyber criminals and a corresponding less predictable cyber criminal behavior post-intrusion. Historically, ransomware gangs generally have guidelines on the "rules of the road," but the RaaS model inherently limits the ransomware gangs' ability to control the affiliates, resulting in less predictable outcomes and corresponding challenges in developing a negotiation strategy.

The 2023 attack on MGM Resorts illustrates the RaaS model in action. Scattered Spider, a sophisticated group that utilizes various social engineering tactics to gain access to organizations' networks and an affiliate of BlackCat/ALPHV, a well-known ransomware gang, allegedly gained access to certain MGM systems and was able to deploy BlackCat's ransomware. MGM reportedly declined to pay the ransom, but according to its SEC 8-K filing, lost approximately $100 million in revenue and paid an additional $10 million for one-time technology consulting services, legal fees, and expenses of other third-party advisors.

4. If You Pay, Expect to Justify It

Internal and external stakeholders, including boards of directors, insurance carriers, and regulators, are increasingly scrutinizing ransom payments. As a result, senior management should be prepared to justify any ransom payment both to internal and external stakeholders. During an incident, boards will often be asked to approve a ransom payment, which would be predicated on the board's relative level of comfort with management's considerations and rationale for payment. Insurance carriers may also question the value proposition if payment is made solely for data suppression (e.g., payment so that data will not be leaked) in contrast to payment for the decryptor tool.

Furthermore, certain regulators have added additional reporting requirements specifically related to ransom/extortion payments. The New York Department of Financial Services (NYDFS) amended its Cybersecurity Regulation (23 NYCRR Part 500) and, as of December 1, 2023, each covered entity is required to report any extortion payment to the NYDFS within 24 hours of the payment, and within 30 days of the extortion payment, provide "a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control." Similarly, the federal Cyber Incident Reporting and Critical Infrastructure Act directs the Cybersecurity and Infrastructure Security Agency to develop a proposed rule on reporting cyber incidents, including requiring covered entities to report ransom payments within 24 hours. The proposed rule is expected by March 2024, and a final rule by September 2025.

5. Forget the Malware, Just Steal the Data

Increasingly, ransomware gangs are turning primarily toward data theft and extortion—skipping the encryption stage altogether. By avoiding encryption, companies are less likely to immediately detect the incident and report it to law enforcement, but threat actors can nonetheless effectuate a compelling extortion demand related to the data exfiltration. In these incidents, threat actors claim to have stolen data from the company, provide screenshots or copies of exfiltrated files as limited proof of life, and threaten to leak the data on the dark web if they do not receive a payment in a specific timeframe. Absent detailed forensic evidence, identifying the potentially impacted data with specificity can become challenging if not impossible and can increase the likelihood of negotiation with the threat actor.

The 2023 exploitation of a "zero-day" vulnerability within the MOVEit Transfer client by CL0P, a Russian-backed ransomware gang, provides an extreme example of a mass extortion threat. CL0P leveraged a security flaw in the software that allowed it to access and steal the data of many organizations (and their customers, vendors, and other third parties) that used MOVEit Transfer software. Unlike typical data extortion incidents that impact one or only a few companies at a time, the scope of CL0P's attack broadly impacted thousands of companies and potentially millions of individuals. Given this volume, CL0P could not specifically extort each victim, so it resorted to mass extortion. CL0P posted a notice on its website that it had accessed the MOVEit Transfer databases and stolen data and threatened to leak data from companies that did not pay a ransom. It put the burden on companies to determine if they were impacted.

Consistent with their threats, CL0P leaked victim data. The full implications from this incident continue to unfold given the breadth and interconnectedness of service provider relationships and data impacted, though many victim organizations have been named in lawsuits.

6. Accelerated Communications Pace

In part due to the prevalence of ransomware incidents, there is increasing general awareness of the hallmarks of disruption associated with an incident, including network outages and the temporary unavailability of services. Any time an entity experiences a network outage or disruption, whether related to ransomware or not, there can be general suspicion of a ransomware incident that may prompt increased expectations for communications with internal and external stakeholders and requests for reassurance of the security of the system. In addition, because of the prospect of extortion threats that involve harassment and public shaming, there can be additional pressure to confidentially inform key external stakeholders of an incident to control the message and get ahead of potential disclosure by the threat actor.

The heightened awareness of the operational impact of ransomware and the interdependencies of information systems has translated in practice to a renewed emphasis on communications. Activating a cyber crisis communications plan that works in conjunction with the incident response process has become a typical component of responding to significant ransomware incidents. Although an entity may have extremely limited information available to share, the need for accurate and timely communications has only increased over the past few years. This in turn only highlights the importance of consistent messaging from the earliest reactive statements, through white glove talking points, status updates, legally required notifications, and technical assurances of containment and remediation.

7. Impact of New SEC Cyber Disclosure Rules

The recently effective SEC reporting requirements for material cybersecurity incidents have prompted a wave of review and revision to incident response plans to ensure the process for assessing and determining materiality is made in close coordination with the forensic investigation and that any Form 8-K filings are made in accordance with the company's disclosure controls process.

Separate from these process-related revisions, the threat actor group BlackCat/ALPHV has also leveraged the SEC Office of the Whistleblower's tips, complaints, and referrals (TCR) portal to disclose nonpublic ransomware events to the SEC it claims credit for. The TCR portal is intended to alert the SEC Office of the Whistleblower to potential violations of federal securities laws, in exchange for the possibility of a reward, should the TCR lead to a successful enforcement action. Although the new SEC rules require public companies to disclose material cybersecurity incidents, not all ransomware incidents necessarily rise to the level of materiality and therefore are not automatically disclosure events. Nevertheless, the prospect of a threat actor group (or disgruntled insider) reporting the incident to the SEC presents another dynamic to be managed as the entity works through the early days of containment, investigation, and remediation.

The extent to which the SEC will open inquiries based on threat actor reports via the TCR portal is not clear since it is hard to imagine that the SEC wants to encourage criminal exploitation of its online tools, and yet it may also be hard for the SEC to ignore claims of cyber incidents impacting its registrants. On balance, threat actor use of the TCR portal may increase the pressure for a company to file a Form 8-K to make the market (and the SEC) aware of the incident but avoid more formal scrutiny from the SEC.

8. Continue with Tabletops … And Bring in the Board

Annual tabletop exercises conducted at the direction of breach counsel continue to be a useful activity to further develop muscle memory and work through decision points that may arise in a cyber incident in a privileged and confidential setting. Technical tabletop exercises involving the organization's information security and information technology teams and executive tabletop exercises involving representatives from various departments, including not just information security and information technology but also legal, communications, marketing, finance, human resources, operations, and other potentially impacted stakeholders, may provide significant benefit due to the evolving threat landscape and corresponding defensive security enhancements. In addition, boards of directors are increasingly likely to participate in a tabletop exercise. Based on the recently updated "Director's Handbook on Cyber-Risk Oversight" by the National Association of Corporate Directors and Internet Security Alliance, "[i]t is also advisable for directors to participate with management in one or more cyberbreach simulations, or 'tabletop exercises.'"

Particularly in light of recent regulatory changes, boards of directors are increasingly expected to be informed and to actively exercise their oversight role in a cybersecurity incident. Over the past few years, the observed trend has been heightened engagement by boards of directors in cyber incidents, which is generally considered to be positive. However, this engagement can encroach on management-level functions if left unchecked or if directors are uncomfortable with incident response. Organizations may wish to reinforce appropriate roles, responsibilities, and lines of communication via executive tabletop exercises.

9. If You Don't Keep It, They Can't Steal It

Ransomware threat actors tend to move with speed, and large pools of unstructured data are easy targets for exfiltration that can provide the basis for later extortion demands. By reducing the amount of data available to threat actors, an entity can reduce the scope and potential severity of the incident. Securely disposing of data according to stated retention schedules and maintaining only the data needed for legitimate business purposes remain among the more effective means to minimize the potential damage of a ransomware event. As a consequence, regulators investigating an entity's response to a ransomware incident increasingly request copies of applicable data retention and disposal policies and procedures, as well as the date of the oldest data involved in a ransomware event to ascertain whether the entity is in compliance with reasonable security and other statutes.

In addition to these data governance measures, further securing sensitive data via widely accepted practices such as encryption, network segmentation, and privileged access may further complicate or thwart threat actor attempts to compromise data. Additional defensive measures such as honeypots or renamed files may also frustrate and lessen threat actor activity.

10. Law Enforcement Takedowns and Emboldened Criminals

In response to the proliferation of ransomware, law enforcement has escalated its activities designed to disrupt and dismantle the criminal networks that support and engage in ransomware, including multiple takedown operations and indictments. These takedown efforts can result in making decryption tools available to victims and disrupting the process of publishing exfiltrated data and prompting reorganizing and realignment of criminal gangs. At least one threat actor group, BlackCat/ALPHV, responded to law enforcement action by loosening restrictions on its affiliates to permit them to attack hospitals, critical infrastructure, and nuclear power plants "anything and anywhere" except for Russia and the states that formerly composed the USSR. BlackCat doubled down on its negotiation tactics, placing the affirmative obligation on the victim to reach out or it will publish data, threatening to notify the SEC and Department of Health and Human Services shortly after the incident, and eliminating any discounts to be applied to a ransom payment as a result of negotiation.

As the instances of law enforcement disruptions of ransomware gangs increases, such as the recent, impressive international law enforcement operation against the prolific ransomware actor LockBit, it remains to be seen whether such groups will adopt harsher tactics as BlackCat did; reorganize and reconstitute themselves with minimal changes to their tactics, techniques, and procedures; or be deterred from continuing and ultimately disband.