LAW360

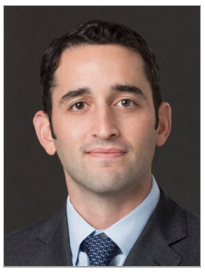
Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 Ransomware Issues GCs Should Have On Their Radar

By **Kim Peretti, Kate Hanniford and Lance Taubin** (April 1, 2024, 4:35 PM EDT)

Kim Peretti

Kate Hanniford



Lance Taubin

Ransomware continues to be a multibillion-dollar criminal industry, with a record-breaking $1 billion in ransom reported paid in 2023.

Ransomware is just one aspect of escalating cybersecurity concerns. Most recently, on March 11, the Biden administration **released** the 2025 fiscal budget proposal, which allocates $13 billion in cybersecurity funding for government and civilian agencies to combat increasing cyber threats.

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.

Looking ahead, ransomware actors may begin more widely deploying "timed wiper malware," which is designed to wipe data permanently.

To manage risk, general counsel should consider proactively evaluating their cybersecurity incident response protocols and stay abreast of emerging threats. As the ransomware threat landscape continues to rapidly evolve, here are the 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.[1] 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 reported that the average ransom payment for the fourth quarter of 2023 was $568,705,[2] and Sophos reported that the average ransom payment almost doubled from $812,380 in 2022 to $1,542,333 in 2023.[3]

On top of the ransom payment, IBM reported that the average cost of a ransomware incident was $5.13 million, an increase of 13% from 2022.[4]

2. Execution With Precision and Speed

The rise in ransomware incidents and ransom payments has been proportional to the increasing sophistication of threat actor techniques and their corresponding speed of execution.

Once the threat actor gains access to an organization's 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.

Although the speed of the incident may vary, 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.[5]

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, most major ransomware criminal actors pivoted their business models to a ransomware-as-a-service offering, which creates numerous affiliates per ransomware gang. Zscaler has attributed a 37% year-over-year increase in ransomware incidents in 2023 to ransomware as a service.[6]

Ransomware as a service permits the affiliate to leverage the ransomware gang's variant, tools, access to data leak sites, negotiation assistance and other support to conduct the attack in exchange for a percentage of the ransom payment.

This ransomware-as-a-service model has resulted in a lower cost of entry for aspiring criminals and less predictable criminal behavior post-intrusion. Historically, ransomware gangs generally followed the "rules of the road," but the model inherently limits the ransomware gangs' ability to control the affiliates, resulting in less predictable outcomes and corresponding challenges for victims to develop a negotiation strategy.

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 decryption tool.

Furthermore, certain regulators have added additional reporting requirements specifically related to ransom or extortion payments.

The New York Department of Financial Services now requires reporting of any extortion payment within 24 hours of the payment, and within 30 days of the extortion payment, "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."[7]

Similarly, the federal Cyber Incident Reporting for Critical Infrastructure Act directs the Cybersecurity and Infrastructure Security Agency to develop a proposed rule on reporting cyber incidents, which includes a requirement to report ransom payments within 24 hours.[8]

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 time frame.

Absent detailed forensic evidence, identifying the potentially affected data with specificity can become challenging if not impossible and can increase the likelihood of negotiation with the threat actor.

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.

When 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. Effect of New SEC Cyber Disclosure Rules

The recently effective U.S. Securities and Exchange Commission 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 portal to disclose nonpublic ransomware events to the SEC it claims credit for.

The 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 tips, complaints and referrals 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.

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.'"[9]

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.

10. Law Enforcement Takedowns and Emboldened Criminals

Law enforcement recently has escalated its activities designed to disrupt and dismantle the criminal networks that support and engage in ransomware, including multiple takedown operations and indictments, including with respect to the prolific Lockbit and BlackCat ransomware gangs.

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.

The threat actor group BlackCat/ALPHV responded to law enforcement action by loosening restrictions on its affiliates to permit them to attack "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, eliminating any discounts to be applied to a ransom payment as a result of negotiation, and in several cases, reviewing and disputing victims statements made in public disclosures.

Kim Peretti is a partner at Alston & Bird LLP and co-leads the firm's privacy, cyber and data strategy team, and its national security and digital crimes team. She is a former U.S. Department of Justice cybercrime prosecutor and former director of PwC's cyber forensics group.

Kate Hanniford is a partner at Alston & Bird.

Lance Taubin is a senior associate at the firm.

Alston & Bird senior associate Alysa Austin contributed to this article.

[1] Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, Chainalysis (Feb. 7, 2024) https://www.chainalysis.com/blog/ransomware-2024/.

[2] New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying, Coveware (Jan. 26, 2024), https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying.

[3] The State of Ransomware 2023, Sophos Ltd. (May 10, 2023), https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.

[4] Cost of a Data Breach 2023, IBM Security (Jul. 24, 2023) https://www.ibm.com/account/reg/us-en/signup?formid=urx-52258.

[5] Mandiant Unveils M-Trends 2023 Report, Delivering Critical Threat Intelligence Directly from the Frontlines, Mandiant, Inc. (Apr. 18, 2023), https://www.mandiant.com/company/press-releases/m-trends-2023.

[6] Zscaler ThreatLabz 2023 Ransomware Report, ZScaler (Jun. 28, 2023), https://info.zscaler.com/resources-industry-reports-2023-threatlabz-ransomware-report.

[7] N.Y. Comp. Codes R. & Regs. tit. 23, § 500.17 (2024).

[8] 6 U.S.C.S. § 681b (Feb. 9, 2024).

[9] Director's Handbook on Cyber-Risk Oversight, National Association for Corporate Directors (Mar. 24, 2023).