Ransomware Checklist

This checklist is intended to be a useful guide for cybersecurity incident response associated with a ransomware attack. This is not intended to constitute legal advice and should be used only for informal reference.

Initial Actions

- **Immediate Impacts and Scope.** Immediately following the discovery of a ransomware attack, it is important to quickly understand the scope of the attack, as well as the likely impacts to operations and the company's legal obligations. It is also important to understand whether the attack is still active and additional systems might be at risk.
- **Contain and Protect.** Can steps be taken immediately to stop or contain the attack? The company should also be looking at steps available to protect systems not (yet) impacted.
- **But Preserve Evidence.** Prompt action may be necessary to contain threats, but failure to preserve forensic evidence in doing so may limit subsequent investigation and create evidentiary challenges should litigation or regulatory inquiries materialize.
- **What Can Be Trusted?** It is important for companies to quickly get a sense of what parts of their systems and infrastructure can be trusted, what needs further review and where alternatives may be required.
- **Beware Multi-Stage Attacks and Multiple Attackers.** Ransomware attackers frequently exploit vulnerabilities that are also compromised by other threat actors, and sophisticated attacks often involve the use of multiple tools and stages.
- **Privileged Investigations.** Upon notice of an attack, consider initiating a counsel-led investigation to establish privilege.

Ransomware-Specific Actions

- **Establishing Contact.** Ransomware attackers frequently provide instructions for establishing contact with them. Companies need to not only decide whether to contact the attacker at all, but also determine if they have the means to establish contact (e.g., access to a Tor browser).
- **Whether to Pay.** As part of this decision, companies need to analyze their business and operational risks, as well as their legal risks with respect to payment decisions. For example, Treasury's Office of Foreign Assets Control (OFAC) has issued an advisory about potential sanctions risks and Financial Crimes Enforcement Network (FinCEN) published one about anti-money laundering (AML) concerns, both associated with making ransom payments. Companies also need to determine whether they have the ability to pay (e.g., access to cryptocurrency).
- **Ability to Restore.** A company's ability to restore, whether from back-ups or through other means (e.g., publicly available decryption keys) is critical to determining whether to pay ransom. Where back-ups are in place, the need to pay ransom to restore operations may be significantly reduced.
- **Was Data Lost?** Ransomware attackers are increasingly exfiltrating victim data as part of their attack, in many cases to establish the legitimacy of their attack but also to threaten leaks or otherwise put the data to malicious use.

Your Network

- **Hunt for IOCs and TTPs.** Potentially impacted companies should hunt for indicators of compromise (IOCs), as well as for evidence consistent with tactics, techniques and procedures (TTPs) identified as part of this attack. Additional information may be available from government entities, security vendors and other sources.
- **Update Security Tools.** Ensure that security tools are up-to-date, properly configured and running.

Contacts

Evan Wolff
Partner
Washington, DC
+1.202.624.2615
ewolff@crowell.com

Jeffrey Poston
Partner
Washington, DC
+1.202.624.2775
jposton@crowell.com

Paul Rosen
Partner
Los Angeles
+1.213.443.5577
prosen@crowell.com

Maida Lerner
Senior Counsel
Washington, DC
+1.202.624.2596
mlerner@crowell.com

Matthew Welling
Counsel
Washington, DC
+1.202.624.2588
mwelling@crowell.com

Michael Atkinson
Partner
Washington, DC
+1.202.624.2540
matkinson@crowell.com

Caroline Brown
Partner
Washington, DC
+1.202.624.2509
cbrown@crowell.com

Laura Foggan
Partner
Washington, DC
+1.202.624.2774
lfoggan@crowell.com

Michelle Gitlitz
Partner
New York
+1.212.895.4334
mgitlitz@crowell.com

Carlton Greene
Partner
Washington, DC
+1.202.624.2818
cgreene@crowell.com

Michelle Linderman
Partner
London
+44.20.7413.1353
mlinderman@crowell.com

David (Dj) Wolff
Partner
Washington, DC
+1.202.624.2548
djwolff@crowell.com

Preparedness

Companies may benefit by proactively referencing alerts and guidance from government agencies on preparing for and defending against ransomware attacks, as well as understanding potential legal and compliance risks, such as the following:

CISA Alert (AA21-131A), DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks

OFAC Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

FinCEN Advisory (FIN-2020-A006) on Ransomware and the Use of Financial Systems to Facilitate Ransom Payments

CISA Ransomware Guidance and Resources

FBI Common Scams and Crimes, Ransomware

U.S. Dept. of Justice, Ransomware: What It Is and What To Do About It

- **Determine Potential Exposure.** While the full nature and impacts of the attack may not be initially apparent, companies should determine the scope of risk exposure they may face as the investigation progresses.
- **Getting to Safe.** Eradication of sophisticated attackers and subsequent recovery often requires an iterative process and can involve varying levels of "safe." Working with professionals experienced at dealing with similar attackers can help benchmark this moving target.
- **Forensic Vendors.** If companies do not have significant ransomware experience in-house, 3rd party forensic vendors offer this expertise. For privileged investigations, engaging vendors through counsel helps ensure that appropriate privileges remain intact.

External Communications

- **Stay Consistent and Aligned.** Especially in situations with evolving information, external communications need to stay accurate and consistent, although level of detail may vary and evolve as circumstances warrant.
- **Centralize Decisions.** Companies should ensure that they have clear internal guidance on how incoming inquiries will be handled and how responses will be managed.
- **Statutory/Regulatory Obligations.** The company also needs to be aware of statutory and regulatory obligations. This includes whether the attack's impact on vendors triggers any reporting obligations for the company.
- **Contractual Obligations.** The company needs to be aware of its contractual obligations related to a potential compromise, which may include notifications to impacted customers, vendors or other counterparties.
- **Incoming Notifications.** Companies should have clear internal guidance to ensure efficient and timely intake and escalation where notifications are received regarding a potential attack (e.g., from vendors or law enforcement/government).
- **Engaging with Law Enforcement/Government.** Companies may opt to proactively engage with law enforcement or other government entities about an attack. Whether in response to a notification or proactive contact, all such communications should be coordinated with leadership and counsel.

Additional Considerations

- **Internal Processes and Procedures.** While these attacks can be high-profile, companies should still follow applicable internal processes and procedures, including for governance and documentation.
- **Intellectual Property Threats.** Ransomware attacks may involve compromising company IP and stealing proprietary information from victims.
- **Litigation Risk.** Companies need to track their potential litigation risk associated with a ransomware attack.
- **Stock Sale Blackout.** Companies should consult with counsel about whether to institute a blackout on stock sales for company insiders—including those involved in incident response.