Ransomware Payment: Legality, Logistics, and Proof of Life

Part Three: Notification, Remediation, and Insurance | by John Reed Stark

RANSOMWARE NOTIFICATION REQUIREMENTS

Although typically involving locking up data (rather than accessing, targeting or exfiltrating data), a ransomware attack could still be deemed the type of data security incident which can trigger legal notification/disclosure requirements, including notice to:

- State regulators (e.g. per state privacy statutes, rules and regulations, anyone whose data may have been compromised during a ransomware attack may require notification);
- Federal regulators (e.g. per the U.S. Securities and Exchange Commission (SEC) and the Financial Regulatory Authority (FINRA));
- Shareholders (e.g. per SEC disclosure obligations or shareholder agreements);
- Vendors, partners and other entities (e.g. if the ransomware victim company has cybersecurity-related notification requirements into their contracts, which can trigger when a victim company experiences a ransomware attack);
- Insurance carriers (e.g. if a victim company plans to make an insurance claim, relating to the ransomware attack);
- Customers and consumers (e.g. when the data of a customer, such as a hospital patient, is impacted by a ransomware attack, a victim company may have very specific legal obligations to notify that customer);
- Employees (e.g. when employee personal data is compromised); and
- Any other constituency who may have a vested interest in a victim-company.

Notification responsibilities relating to a ransomware attack can become complicated and may not precisely align with other cybersecurity-related notification obligations and triggers. Ransomware differs from most cyber-attacks in that the perpetrators of ransomware schemes do not typically abscond with sensitive customer data. Rather, ransomware attackers may merely prevent access to customer data or company systems, without any harm to any individual or theft of individual data. For instance, if company data is encrypted and never accessed, targeted or exfiltrated, and then the ransomware attackers decrypt the data after receiving a ransom payment, there arguably never occurred any actual or specific customer harm.

In addition, sometimes ransomware combines with other malware, such as when attackers plant a data-stealing Trojan virus in a system which can steal login credentials, and then use the credentials to encrypt data or systems or even just sell the credentials to other cyber attackers. Other times, attackers not only encrypt the victim's data, but threaten to post the data publicly online, causing even more havoc. Ransomware variants and iterations are infinite with each type creating thorny regulatory notification requirements.

First published on the Nasdaq Governance Clearinghouse

Meanwhile, disclosure of the ransomware attack can certainly harm a company's reputation and invite future attacks – or even prompt regulatory (or plaintiff's bar) scrutiny for weak cybersecurity, such as having inadequate patching practices or antiquated data protection systems. Thus, if not legally required, a victim company may remain reluctant to disclose the ransomware attack to anyone.

STATE VERSUS FEDERAL NOTIFICATION

There is no single national data breach notification law that governs all information the same way as state data breach laws do. Thus, ransomware victim companies must determine which state privacy laws apply to them and analyze their notification obligations within each state.

However, there are also federal laws that require disclosure of data breaches in certain instances, and usually these laws are "industry specific." Examples of federal laws that require data breach notification are two laws governing the health care industry – the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). Another example of a federal data breach notification requirement is found within the Gramm-Leach-Bliley Act (GLBA), which governs companies engaged in financial services.

STATE REGULATORS

In the United States, 52 jurisdictions (including 48 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) have enacted some version of a data breach notification law. Under these laws, notification may be required for any customer whose personally identifiable information (PII) was acquired or accessed, or reasonably likely to have been acquired or accessed.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/information brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, driver's license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information). While most states require some form of disclosure to their residents of a data breach, depending on applicable legal standards, some states also require notification to public agencies, such as the state attorney general.

With respect to ransomware in particular, the threshold issue is a technological one – best determined by a digital forensics expert and couched in legal terms. For instance, if the data is encrypted or otherwise "locked" through an automated process, companies could argue that the data was never accessed by an unauthorized party, which is the standard that typically triggers state data breach notification laws.

On the other hand, though the mere encryption of data may not trigger the notification rules, the viewing, copying, relocating and altering of information can. Digital forensics and malware reverse engineering can provide some clue with respect to the impact of a ransomware attack and help assess some of the lesser state thresholds (such as in states like Connecticut, Florida, Kansas, Louisiana and New Jersey) where the definition of a breach also includes accessing of protected health information.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) (E.G. HEALTHCARE ORGANIZATIONS LIKE HOSPITALS AND OTHER MEDICAL SERVICE FACILITIES)

One of the only regulators to have issued explicit guidance regarding ransomware notification issues is HHS. In July 2016, HHS issued informal guidance specifically addressing the notification obligations of healthcare providers and other businesses covered by the Health Information Portability and Accountability Act (HIPAA) in the event of a ransomware incident. The HHS Ransomware Guidance aims to provide healthcare organizations with information about ransomware attack prevention and recovery from a healthcare sector perspective, including how HIPAA breach notification processes should be managed in response to a ransomware attack.

Under HIPAA, covered entities are generally required to notify HHS in the event of any breach of unsecured protected health information (PHI). The HIPAA rules define a "breach" as the unauthorized "acquisition, access, use, or disclosure of PHI" that "compromises the security or privacy of the PHI."

For hospital organizations and others hit by ransomware attacks and covered under HIPPA, digital forensics analysis can provide critical information relating to disclosure requirements. For instance, HHS rules generally state that hospitals need only report attacks that result in the exposure of private medical or financial information, such as malware that steals data. The HHS Ransomware Guidance distinguishes ransomware from other malware, as "its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data … until a ransom is paid."

Overall, according to the HHS Ransomware Guidance, in order to demonstrate that there is a low probability that the PHI has been compromised because of a ransomware attack, healthcare organizations have to conduct a risk assessment considering at least four of the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Along those lines, HHS does not take the position that actual data exfiltration is necessary for a ransomware infection to qualify as a breach. Rather, the HHS Ransomware Guidance states that any ransomware attack affecting PHI can qualify as a breach because the encryption implies that the PHI has been "acquired" by attackers. On this view, the attacker's encryption of the data alone could qualify as an "acquisition" – even if the data is never viewed or stolen by the attacker. However, whether ransomware's data encryption clearly crosses that legal threshold can be challenging to determine, which is why ransomware attacks and other data security incidents at health care organizations often go unreported.

The HHS Ransomware Guidance also notes that even if the PHI is encrypted, additional analysis may still be required to ensure the encryption solution has rendered the affected PHI "unreadable, unusable and indecipherable to unauthorized persons."

In addition, HHS also recommends organizations consider the impact of the ransomware on the integrity of the patient data (PHI). The agency states that frequently ransomware, after encrypting the data it was seeking, deletes the original data and leaves only the data in encrypted form, which could be an issue. Per the HHS Ransomware Guidelines:

"An entity may be able to show mitigation of the impact of a ransomware attack affecting the integrity of the PHI through the implementation of robust contingency plans including disaster recovery and data backup plans."

GRAMM-LEACH BLILEY ACT (GLBA) (E.G. CONSUMER BANKS AND LOAN COMPANIES)

Passed in 1998, GLBA is a comprehensive package of banking and financial legislation, which includes significant data privacy and security requirements. Banks, brokers, mortgage companies, lenders, and financial advisers all fall under this law's data obligations. Specifically, GLBA requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

GLBA requires various federal agencies – including the Federal Trade Commission, the Federal Reserve, Treasury Department, and Securities and Exchange Commission – to write their own specific data security regulations, known as safeguards rules, for protecting customer data and to "establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of customer information."

Per the GLBA, when a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, such as a ransomware attack, the institution should conduct an investigation to determine the likelihood that the information has been or will be misused. If there is a determination that the misuse has occurred or is reasonably possible, the institution must notify the affected customer as soon as possible, unless there is a law enforcement determination that notification will interfere with a criminal investigation.

U.S. FEDERAL TRADE COMMISSION (FTC) GUIDANCE

Historically, the FTC has been the most active with respect to privacy protections arising from a cyber-attack, and its jurisdiction continues to expand. Previously the subject of some controversy and confusion, the FTC's jurisdiction was reinforced (in what some commentators cited as a sea change) when the Third Circuit Court of Appeals affirmed a federal district court's decision, *FTC v. Wyndham Worldwide Corp.*, holding that the FTC has authority to regulate a company's inadequate cybersecurity practices.

In addition, the FTC (and other federal agencies that regulate financial institutions, including the Federal Reserve Board, the National Credit Union Administration, the Office of the Comptroller of Currency and the SEC) has issued regulations to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which, together with the Fair Credit Reporting Act (FCRA), protects information used in credit, insurance and employment decisions. The FTC also, in 2002, finalized their GLBA-required Safeguards Rule (16 CFR 314), which covers financial companies offering consumer lending and consumer investment advice. These companies are required to have a program in place for "detecting, preventing and responding to attacks, intrusions, or other systems failures."

None of the FTC's regulations mandate disclosure/notification for ransomware attacks. However, the FTC's official publication, *Data Breach Response: A Guide for Business*, states that companies should report data security incidents (presumably including incidents involving ransomware) to law enforcement as follows:

"Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police aren't familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service."

In May 2015, the FTC published a blog post in which it explained how important it views reporting of cybersecurity incidents to law enforcement:

"We'll also consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion. In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated."

In short, the FTC requires companies such as financial firms that offer consumer lending and consumer investment advice to have a program in place for "detecting, preventing and responding to attacks, intrusions, or other systems failures." However, there is no explicit data breach notification requirement in the FTC's regulations.

U.S. SECURITIES AND EXCHANGE COMMISSION (SEC) (E.G. PUBLIC COMPANIES)

In 2000, the SEC issued its data safeguards interpretation of GLBA known as Regulation S-P (17 CFR 248.30) for brokers, dealers, investment companies and investment advisors. The SEC safeguards regulations have no requirement for data breach notification. Similar to the FTC's rules, companies falling under the SEC's GLBA related data regulations should have breach response as part of a security program, and should issue breach notifications to relevant authorities and individuals.

However, on Oct. 13, 2011, the SEC released its first ever staff guidance pertaining exclusively to the cybersecurity-related disclosure obligations of public companies, including data security incidents such as a ransomware attack. The SEC guidance covers a public company's reporting responsibilities both just after a cyberattack as a "material" event, and even before as a "risk factor." The SEC does not differentiate ransomware attacks from cyber-attacks but that does not seem relevant – because the type of attack is not necessarily relevant. What is relevant is whether the data security incident – be it cyber-attack or ransomware demand – is material.

From the SEC's perspective, the requirements outlined in its guidance introduce nothing new but, instead, merely clarify the SEC's long-standing requirement that public companies report "material" events to their shareholders, i.e., important developments or events that "a reasonable investor would consider important to an investment decision," such as a ransomware attack.

What precisely renders an event material has plagued securities lawyers for years and has been the subject of countless judicial decisions, SEC enforcement actions, law review articles, law firm guidance and the like. With the 2011 Guidance, the SEC officially (and quite noticeably) added cybersecurity into the mix of disclosure by putting every public company on notice that cyber-attacks (including ransomware attacks) and cybersecurity vulnerability fall squarely within a public company's reporting responsibilities.

Prior to the Guidance, publicly traded companies were not required to report in their SEC filings if a data security incident had occurred or if they had fixed the problem. Starting in 2012, however, publicly traded companies had to acknowledge the cyber-attacks to regulators and explain the measures they plan to take to close their cyber-security gaps. Before the Guidance, only certain sectors of the economy were required to report cyber-attacks.

Given the increasingly complex and tricky nature of recent ransomware attacks, the SEC staff has clearly allowed public companies some latitude and given companies a chance to get their arms around a situation before mandating the filing of any sort of disclosure. In fact, the SEC has yet to file an enforcement or administrative action alleging any data security incident disclosure failure, let alone a disclosure relating to ransomware.

THE FINANCIAL REGULATORY AUTHORITY (FINRA) (E.G. FINANCIAL FIRMS SUCH AS BROKERS AND DEALERS)

With respect to the 4,200 broker-dealer firms licensed by FINRA, notification of FINRA concerning a ransomware attacks is not always clear and there exists no specific rule or official FINRA *Notice to Members*. However, there are several references to the issue of cyber-attack disclosure on FINRA's website, including on its "Cybersecurity Topic Page" page (with similar guidance found on FINRA's Checklist for Compromised Accounts Page) stating:

"In case of a disruptive attack or a breach: Firms should get to know their local Federal Bureau of Investigation (FBI) and proactively plan for a cybersecurity attack or breach. In case your firm is the victim of a disruptive attack or breach, for instance your data has been accessed or your customers cannot do business, you should immediately report the incident to your local FBI field office, and FINRA Regulatory Coordinator (RC)."

Given that notification to FINRA of a ransomware attack could trigger for cause examinations from the SEC and from FINRA, victim companies will probably remain reluctant to notify them. In this light, a FINRA- regulated entity's concerns for establishing an unnecessary (and unduly burdensome) precedent and expectation also make sense, especially if the nature of their relationship with FINRA is solid and notification would be highly unusual.

Although the regulatory landscape is changing and FINRA expectations with respect to notification of cybersecurity incidents has become more acute, there exists no requirement or standard to apply – so there is certainly latitude in the least to pause. And while a ransomware victim's lack of disclosure could possibly draw the ire of FINRA (sparking enhanced regulatory oversight or investigation), that lesser risk might be preferable to the more likely and far greater risk of a for cause FINRA compliance exam. The key is to engage in a robust discussion about notification issues, and for a firm's internal compliance executives to contribute to a thoughtful and reasonable recommendation.

CANDOR WITH REGULATOR ABOUT A RANSOMWARE ATTACK

Given the lack of any specific FINRA rule, with respect to determining FINRA disclosure obligations after a ransomware attack, the most appropriate approach falls under the implicit disclosure rule of candor with one's regulator and the public service obligation of letting regulators and law enforcement know about a particular threat to financial markets. For example, typical disclosure along these lines could be as follows:

"Our firm has experienced a ransomware attack and the nature of the attack (not the impact) causes us concern for all financial firms, who may also be at risk. Our firm wanted to alert FINRA to the incident and make FINRA aware of the malware used; the IOC's we have discovered; the attack vector; and the modus operandi. This attack stands out among the many others our firm has investigated because of [X]. Our firm has a team of experts investigating and we will brief you about the details as soon as we know more."

WHEN A RANSOMWARE ATTACK MAY ALSO BE A REGULATORY FAILURE

If a ransomware attack brings to light significant regulatory failures, material weaknesses or possible securities regulation violations, or is of the type of conduct that was of concern as reflected in a prior SEC or FINRA deficiency letter, then the calculus for disclosure is much more strategic above all else.

Under such circumstances, the general approach should also be one of candid disclosure in hope of getting credit when an enforcement or administrative action is ultimately filed or ordered. Having said that, however, early disclosure is no guarantee that a company will receive any credit or good will – and in fact, the reluctance of FINRA staff to give "informal cooperation credit" is a common gripe of FINRA defense attorneys. The collective perception is that cooperation is not seriously considered and is too often given only short shrift – and unless done perfectly, done fully; and done early, are not always given adequate consideration.

Along those same lines, ransomware attack disclosure to FINRA might NOT be appropriate if the ransomware attack is:

- Not very different or unusual relative to other attacks a firm has investigated;
- Not anywhere near a cataclysmic or critical event for the global financial marketplace; the firm; its customers; its affiliates; etc.; and
- Being handled thoughtfully and professionally and in accordance with robust policies, practices and procedures; and "par for the course" among financial firms and all public companies.

If the above criteria are met, a firm can opt to alert FINRA when FINRA next visits for an inspection or examination -- in the same manner a firm would alert FINRA of significant customer complaints; employee misconduct; technological mishaps; or other similar routine incidents.

U.S. TREASURY DEPARTMENT AND FEDERAL RESERVE (E.G. BANKS AND BANK HOLDING COMPANIES)

The Federal Reserve and U.S. Treasury Department have been working out the details of their GLBA-required safeguards standards and in 2005, they jointly issued Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

Per the Interagency Guidelines, financial companies that are covered by these agencies-- including bank holding companies, private bankers and investment banks -- may have important notification/disclosure responsibilities relating to ransomware attacks. These regulated entities " have an 'affirmative duty' to protect their customer's data against unauthorized use or access, and notifying the customers is *a key part of that duty."* (emphasis added). The company, however, must first determine whether misuse of the information has occurred or is reasonably possible.

In the case of a ransomware attack, whether encryption alone is considered a misuse of data under Treasury or Federal Reserve guidelines is not clear. But if a financial firm does send a notification to customers about a ransomware incident, pursuant to the **Interagency Guidelines**, the notification must describe the incident, the data that was affected and measures that were being taken to protect against further unauthorized access.

While the disclosure/notification rules relating to financial data seem less strict than the rules for healthcare related data, that could easily change with new guidance or rule-making. Clearly, the spirit of the various GLBA safeguard rules would lean toward disclosure, but whether there exists a strict obligation to do so will always be a matter of interpretation and judgment.

U.S. DEPARTMENT OF JUSTICE (DOJ) GUIDANCE

DOJ's *Best Practices for Victim Response and Reporting of Cyber Incidents*, is an official government publication which encourages companies to engage with law enforcement when a data security incident occurs (including ransomware), stating:

"If an organization suspects at any point during its assessment or response that the incident constitutes criminal activity, it should contact law enforcement immediately. Historically, some companies have been reticent to contact law enforcement following a cyber incident fearing that a criminal investigation may result in disruption of its business or reputational harm. However, a company harboring such concerns should not hesitate to contact law enforcement. The FBI and U.S. Secret Service place a priority on conducting cyber investigations that cause as little disruption as possible to a victim organization's normal operations and recognize the need to work cooperatively and discreetly with victim companies. They will use investigative measures that avoid computer downtime or displacement of a company's employees. When using an indispensable investigative measure likely to inconvenience a victim organization, they will do so with the objective of minimizing the duration and scope of any disruption."

Interestingly, the DOJ's Guidance reminds companies of one of the benefits of federal law enforcement notification of a cyber-attack such as a ransomware attack: a possible temporary reprieve from state reporting obligations. The DOJ Guidance states:

" . . . [M]any [state] data breach reporting laws allow a covered organization to delay notification if law enforcement concludes that such notice would impede an investigation. State laws also may allow a victim company to forgo providing notice altogether if the victim company consults with law enforcement and thereafter determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed. Organizations should consult with counsel to determine their obligations under state data breach notification laws. It is also noteworthy that companies from regulated industries that cooperate with law enforcement may be viewed more favorably by regulators looking into a data breach."

Even if unsuccessful, notification to federal law enforcement of a ransomware attack is often expected by the regulators, shareholders, customers, partners and the many other constituencies potentially impacted by a ransomware attack. After all, a ransomware victim is being unlawfully extorted and needs federal help, protection and advice. Moreover, a ransomware victim will want to demonstrate that they are availing themselves of all available resources to protect against the potentially ongoing or future harm from the ransomware attackers.

However, notification to federal law enforcement can have costly and complicated ramifications. On one hand, the FBI, Secret Service, U.S. Air Force and other law enforcement agencies may be trying to identify and prosecute the intruders – and may even share with a ransomware victim the results of their investigation. On the other hand, myriad attorneys general and other regulatory agencies are issuing requests and demanding answers about the safety of the personal information of their respective citizenries. Managing this delicate balance can become challenging.

Law enforcement agencies may also: seek from the victim company forensic images of affected systems; request to attach a recording appliance to a victim company's network in hope of capturing traces of possible future attacker activity; ask to receive briefings of all findings from any incident response efforts; and want a range of other information, technological data and interviews. These requests raise a host of legal issues, including whether providing information to law enforcement could violate customer privacy or inadvertently waive the attorney-client privilege.

EUROPEAN UNION (EU) REGULATIONS

Under the Data Protection Directive (DPD), there is no data breach notification requirement. Some countries such as Germany, though, have added it in their national data protection laws. (Though ISPs and telecoms under the EU's e-Privacy Directive already have their own data breach reporting rule.)

However, pursuant to the new EU General Data Protection Regulation (GDPR), effective May 25, 2018, there is a requirement to notify the supervisory authority and affected data subjects when "personal data" is accessed, without undue delay (no later than 72 hours) after becoming aware of a data breach, unless it is unlikely to cause a risk to the affected individuals.

Of note is also that this harm-based threshold means that the ransomware attack would have to "result in a risk to the rights and freedoms" of consumers, which could create a significant exception. Specifically, per Article 34 (1) of the GDPR, notice is not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons," a phrase that will no doubt offer data protection officers and their outside counsel opportunities to debate the necessity of notification.

With respect to notification to "affected data subjects," there is also an explicit string of exceptions. The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances: (1) the controller has "implemented appropriate technical and organizational protection measures" that "render the data unintelligible to any person who is not authorized to access it, such as encryption"; (2) the controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialize; or (3) when notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.

Given that the GDPR is somewhat unclear about ransomware disclosure/notification responsibilities and has not yet become effective, the only notion for certain is that notification for a ransomware attack will be very dependent on specific circumstances.

As an aside, the fines for violating the EU Data Protection Regulation are significant -- an infringement of provisions related to the reporting of data breaches is subject to a fine of up to 10 million Euros or 2% of global group turnover, so any late notification will need to be justified.

A NOTE ON LEGAL, CONTRACTUAL AND INCIDENTAL DISCLOSURE OF RANSOMWARE ATTACKS

Whether a ransomware victim has a ***legal obligation*** to disclose a ransomware attack to regulators; partners; customers; operators; employees; vendors and a range of other constituencies will be driven by a robust, methodical and independent forensic investigation.

In other words, before a ransomware victim can make decisions about any legal responsibility for disclosure, the ransomware victim will need to conduct its own investigation and determine, among other things, the nature of the attacker's efforts; the scope of the attack vector; and whether credit card data, personal identifying information, personal health information, intellectual property or any other relevant data was targeted, accessed or exfiltrated.

Whether a ransomware victim has a ***contractual obligation*** to disclose a ransomware attack to partners; customers; operators; employees; vendors and a range of other constituencies, will turn upon the various agreements in place relating to those parties.

However, even though a ransomware victim might not have any ***legal*** or ***contractual*** obligations to disclose a ransomware attack, the ransomware victim company might still opt to disclose the attack to regulators; partners; customers; operators; employees; vendors; etc. Indeed, certain circumstances can arise where disclosure of the attack, though not legally or contractually required, nonetheless becomes necessary, prudent and/or practical.

Such so-called "incidental disclosures" can occur during certain events or because of certain relationships, such as:

- **PCI Audit**. If a ransomware victim accepts credit cards for payment and is about to undergo a Payment Card Industry (PCI) Compliance Assessment, the Qualified Security Assessor conducting the compliance review will undoubtedly ask questions about the ransomware victim company's overall cybersecurity, which could prompt or necessitate disclosure of the ransomware attack;
- **Cybersecurity Due Diligence**. Certain vendors, customers, partners, etc. may send a ransomware victim company a data security questionnaire, which is likely part of their due diligence concerning the cybersecurity strength of the relationship. In fact, cybersecurity-related inquiries, solicitations and

information demands have become increasingly common. Any one of these kinds of cybersecurity requests or queries directed at a ransomware victim company could prompt or necessitate disclosure of a ransomware attack;

- **Whistleblowers**. So-called bad leavers (those who leave a company badly) or disgruntled insiders with an axe to grind, could learn of the ransomware incident and disclose the details to the media; to regulators; to contracting parties; or to any other interested party. Any of this type of unwieldy disclosure could prompt or necessitate disclosure of the ransomware attack;
- **Law Enforcement Action**s. The sophistication and prevalence of ransomware threats seems to be growing and law enforcement seems committed not only to deterring the attacks but also to capturing the perpetrators. Given law enforcement's current focus on cyber-attacks generally, more law enforcement action concerning ransomware may occur in the future. Should the federal government bring a prosecution against a ransomware perpetrator or issue public warnings concerning a ransomware attacker, the ransomware attack could become public or could prompt or necessitate disclosure of the ransomware attack;
- **Contractual Negotiations**. If the ransomware victim company is a sophisticated corporation with many business relationships, contracts and agreements – and has any ongoing contractual negotiations or those contractual relationships are up for renewal, discussions of cybersecurity could arise, which, in turn, could trigger incidental disclosure. Moreover, if the ransomware victim company is pursuing any new corporate associations, affiliations, acquisitions or other relationships, discussions of cybersecurity could arise, which, in turn, could prompt or necessitate disclosure of the ransomware attack; and
- **Special Relationships**. Some contractual relationships carry with them a unique inherent/implied degree of trust and confidence or are of such extraordinary business importance, that, despite a ransomware victim company having no legal or contractual requirement to do so, the ransomware victim company may feel nonetheless inclined or obligated disclose the ransomware attack (such as during a status conference or other routine get-together).

RANSOMWARE REMEDIATION

There are a slew of basic steps companies should take as preemptive measures to avoid falling prey to ransomware, including backing up systems and employing the latest cybersecurity measures. Other measures include:

- Updating operating systems, software patching, antivirus programs and firewalls;
- Taking steps to detect and block ransomware through firewalls and intrusion detection monitoring, including setting alerts for anomalous behavior;
- Revisiting backup protocols to ensure that a crypto-attack is classified as a potential disaster with appropriate contingency plans;
- Enabling popup blockers;
- Employing IT professionals or consultants familiar with ransomware, who stay current with evolving iterations and variants; and
- Implementing a strong password policy requiring all users to regularly change passwords and require more complex passwords, i.e. mixture of lower and uppercase letters, numbers, and symbols;
- Reviewing and auditing all network permissions in your network while updating and deactivating all user accounts regularly, including departing employees;
- Rigorous employee education and outreach;
- Securing long and short-term backups, stored in a manner detached from a company's network;
- Intense screening of partners and vendors to ensure strong security procedures from associated third parties;
- Thoughtfully and securely segmenting sensitive user and corporate data within a corporate network; and
- Changing network and Wi-Fi passwords regularly.

Along the same lines, the FBI urges organizations to be vigilant keeping browsers, operating systems and third-party application patch levels up to date, and that antivirus protection is also current. The FBI also suggests companies back up often, lock down access granted to individuals and manage configuration of file systems, directories and network shares appropriately.

By setting snares and "honeypots" for would-be ransomware attackers, companies can go so far as to employ drastic and direct preemptive measures. For example, Deception Technology sets its trademarked HackTraps to misdirect the attacker and prevent them from going deeper into your network and reaching their intended target. These traps can be as simple as a document with a deceiving title that was created exclusively to lure in the cybercriminals.

A digital forensic expert can also help a victim company develop and implement a containment plan to isolate any additional infections and provide strategic recommendations to prevent further ransomware attacks and otherwise mitigate their impact.

It may be hard to believe, but when handled correctly, a customer data compromise or data security incident like a ransomware attack can actually become the kind of successful failure that not only prompts remediation that strengthens technological infrastructure, but also reinforces a firm's commitment and focus upon its customers, partners and other fiduciaries.

RANSOMWARE AND BUSINESS CONTINUITY PLANS

The critical importance of a business continuity plan in the event of a natural disaster is widely recognized and accepted. Yet, too often, such plans are not evaluated in the context of assessing cybersecurity risks such as ransomware.

Even when an organization's IT cybersecurity response fully aligns to IT best practices, there are benefits in utilizing or integrating IT's response into the existing business continuity structure, rather than having two separate response models. Speed and agility are key enablers in ransomware response, and business continuity enables nimble, rapid response limiting financial and reputational impact on the enterprise.

A powerful business continuity plan, which is properly integrated with an incident response plan, contemplates the threat of ransomware and plans for data recovery, such as with specialized back-up data systems that are routinely tested and updated as necessary.

RANSOMWARE AND CYBER INSURANCE

Like any other corporate risk, companies are beginning to realize that the financial, operational and even reputational risks of a ransomware attack can be addressed via a comprehensive and targeted cyber insurance policy. Over 60 insurance companies now offer cyber insurance, many containing specific provisions addressing ransomware. In 2015, ransomware accounted for just over 10% of cyber insurance claims, but in 2016 that figure grew to 25%.

Currently, most cyber insurance policies are modular, which means an organization chooses from a menu of coverage options, such as business interruption, third party liability for privacy breaches and first party coverage for an organization's own costs to detect, stop, investigate and remediate a network security incident.

Ransomware typically falls under "first party" liabilities as cyber extortion and network interruption. When making a cyber insurance claim for ransomware, a victim company should be prepared to demonstrate that: the ransom has been surrendered under duress; the incident is not a hoax; there was c-suite participation in the ransomware payment decision; the insurance company approved of the ransomware payment plan; and the ransomware attack was reported to law enforcement.

Making an insurance reimbursement claim for a Bitcoin payment is also tricky, even with respect to valuation and execution. Challenges include proving to an insurance company: that a Bitcoin payment was made; that a Bitcoin payment was for a particular amount of U.S. dollars; and that a Bitcoin transaction was documented in an acceptable and verifiable manner.

Thus, a ransomware victim company may have to engage a professional intermediary to pay the attackers, and then seek reimbursement for the fees paid to the digital intermediary. Otherwise, an insurer might have no way to audit a process involving Bitcoin and therefore refuse to recompense Bitcoin payments. Cyber insurance might also not cover the full amount of the ransomware or may have in place a high deductible amount (for large organizations the deductible could be $500,000 or as high as $5 million).

Without a specific ransomware cyber insurance policy, a victim company would have to look to the breadth of their professional liability and other insurance policies, which can give rise to ambiguities and disputes. For example, the presence of any sort of terrorism exclusion can become problematic. For instance, insurance policies may have “acts of foreign enemies” or “government acts” exclusions that can limit reimbursement if the ransomware was distributed by cyber-attackers tied to a foreign government.

In addition, whether a ransomware victim company must show "physical damage" can also become an issue. In the typical ransomware scenario, a victim company's data is not actually damaged but is rather, "locked." An insurance company may argue that like other cyber-attacks, where a victim's data was accessed, but not otherwise disturbed, altered or exfiltrated, then the victim has no insurance claim.

KIDNAPPING INSURANCE

Some companies, who do not have cyber insurance, may turn to their kidnap insurance for coverage relating to ransomware attacks. Kidnap policies, known as K&R coverage, are typically used by multinational companies looking to protect their staff in areas of danger, such as where violence related to oil and mining operations is common (like parts of Africa and Latin America).

K&R policies, which typically do not have deductibles, can cover the ransom payments as well as crisis response services, including getting in touch with criminal and regulatory authorities. Whether K&R coverage, which was not designed for ransomware, will cover ransomware costs and expenses will always be a matter of the specific policies involved.

To get the most out of cyber coverage for ransomware attacks, companies should work closely with their brokers, their insurers, their outside counsel and their own internal experts and executives to fully understand their particular ransomware risks. For now, the most effective cyber insurance policies are bespoke, and given the rapidly evolving nature of cyber-attacks, will continue to require custom-tailored fitting for quite some time.

Just like other kinds of insurance, ransomware coverage by itself will rarely be enough to make a company whole after a cyber-attack, but it can provide critical financial resources. Moreover, when coupled with a thoughtful and diligent incident response, a sound ransomware insurance policy can send a powerful message of strong business acumen; fierce customer dedication; and steadfast corporate governance, demonstrating profound expertise to the marketplace, shareholders, regulators and the many other interested corporate stakeholders.

FINAL THOUGHTS

Even under the best-case scenario, where a victim has maintained archives and can keep their business alive, ransomware victim companies will incur significant remedial costs, business disruptions and exhaustive management drag. Moreover, having a back-up storage solution in place is not always ideal; not only can outside storage of data create additional cybersecurity risks, but sometimes data archives are more like the proverbial *roach motels*, where data checks in but it can’t check out.

No doubt that the ease, anonymity and speed of crypto-currency payments such as Bitcoin has revolutionized the ransomware industry, prompting its extraordinary growth. Bitcoin not only makes it easier to remain anonymous, but also enables a nameless payment mechanism where the extorted funds can be immediately transferred into criminal hands.

Transactions in cryptocurrencies like Bitcoin lack a discernable audit trail and operate outside of regulated financial networks and are alarmingly unregulated. There is no central issuer of Bitcoins, nor a Federal Reserve of Bitcoins monitoring and tracking transactions or controlling their value. In short, government surveillance and regulation of cryptocurrency is virtually nonexistent (no pun intended) and so long as cryptocurrency payment schemes exist (and back-up systems fail), ransomware attacks and iterations will likely continue to thrive.

Though too early to tell, there may emerge some form of Bitcoin regulation via Executive Order No. 13,694 (April, 2015), which expands sanctions to include "blocking" the property of persons engaging in "Significant Malicious Cyber-Enabled Activities." The order declares a "national emergency" to deal with cyber-enabled threats and extends to the assets of those who "have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any [malicious cyber-enabled activities]."

Given that ransomware Bitcoin payments are made to cyber criminals, per Executive Order 13,694, the U.S. Secretary of the Treasury, the U.S. Attorney General and/or the U.S. Secretary of State could freeze or "block" assets of any participant in the Bitcoin financial chain. Such dramatic government intervention could discourage the purveyors of ransomware attacks, who depend on Bitcoin for receiving payments.

The government could also take additional steps to combat ransomware such as:

- Providing financial incentives for private investment in ransomware prevention and remediation technologies;
- Bringing more enforcement actions (as both criminal actions and FinCEN regulatory actions);
- Speaking more boldly to discourage ransomware payments that monetize crime, perhaps via the Financial Crimes Enforcement Network (FinCEN) or via a task force of state and federal law enforcement agencies. U.S. defense and intelligence agencies, FinCEN in particular, pride themselves on the U.S. government's ability to track and disrupt the illicit financial networks that work through traditional banks and finance channels and are more than up to the task of stepping up enforcement and regulatory efforts; or
- Creating new legal penalties for ransomware payments in a manner similar to the FCPA, rendering the option of paying ransom costlier, thus nudging firms toward choosing greater security.

But these government measures remain somewhat theoretical and even if implemented, might still fail to sojourn the dramatic growth of ransomware. The reality is that when it comes to ransomware attacks, the government seems idle and relatively powerless, which means ransomware victims are unfortunately on their own. So what should companies do to manage the increasing risk of the current ransomware crime wave?

As would probably be preached by Thomas Clayton (or Russell Crowe), companies struggling with ransomware threats should apply the same lessons to ransomware protection that Clayton uses for employee protection: Be prepared (e.g. deploy back-ups and the like); Be thoughtful (e.g. use professionals to implement preemptive measures and help handle the response); and Be vigilant (e.g. don't underestimate the impact of ransomware and don't take the threat lightly).

*John Reed Stark is President of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Mr. Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, the last 11 of which as Chief of its Office of Internet Enforcement. He also worked for 15 years as an Adjunct Professor of Law at the Georgetown University Law Center, where he taught several courses on the juxtaposition of law, technology and crime, and for five years as managing director of a global data breach response firm, including three years heading its Washington, D.C. office. Mr. Stark is the author of, "The Cybersecurity Due Diligence Handbook," available as an eBook on Amazon, iBooks and other booksellers.