Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Ransomware's Dirty Little Secret: Most Corporate Victims Pay

By **John Reed Stark** (February 6, 2019, 2:21 PM EST)

Ransomware attacks have reached epidemic proportions, but nobody is talking about it. Why? Because corporate ransomware victims are discreetly paying the ransoms and are (lawfully) sweeping the incidents under the rug.


John Reed Stark

Tendering ransomware payments has evolved into yet another dirty little secret of corporate operations — just like U.S. corporate foreign bribes prior to the enactment of the Foreign Corrupt Practices Act or U.S. business dealings with terrorists prior to the enactment of the Patriot Act. Except this time, there may not exist a statutory remedy for the current ransomware payment scourge — and this time one cannot help but sympathize with the excruciating suffering endured by ransomware victims.

In most cases of ransomware, the fact pattern is the same:

- Ransomware attackers break into a corporate system and encrypt, or lock-up, a corporate victim's data. Most ransomware infections come from phishing attacks, in which unwitting users are enticed to open a file or click on a link containing the ransomware malware;
- The ransomware attackers demand payment in cryptocurrency, typically bitcoin, for the encryption key to enable the victim corporation to unlock the now inaccessible data;
- The ransomware victim pays the cryptocurrency ransom to the attacker; and
- The ransomware attackers move on to their next victim.

What makes ransomware attacks so distinctive is that the corporate victim never loses possession of the data, merely access to it. In other words, whereas most other forms of cybercrime involve some type of pilfering such as exfiltrating credit card data or intellectual property that can be sold on the dark web, ransomware is different. In a ransomware scenario, the crime is more akin to extortion where the corporate victim's data is held hostage until the company pays the ransom.

What makes ransomware attacks so devastating is that many variants do not simply target individual endpoints, but rather establish a foothold on one device and then fan out across a corporate network, encrypting everything from shared drives and email servers to website platforms and backup servers. In this way, ransomware attackers can cripple significant portions, or even all, of a company's technologically facilitated operations.

Rarely is there ever even an arrest, let alone a successful prosecution, of a ransomware attacker. Law enforcement remains virtually paralyzed, while bitcoin continues to gain popularity as the outlaw's currency of choice. Ransomware attackers have become yet another class of cybercriminal who continue to enrich themselves while, for the most part, law enforcement can only watch from the sidelines.

While payment of a ransomware demand does not guarantee that the ransomware attacker will provide the right encryption keys with the proper decryption algorithms and may not stop the ransomware attacker from returning, the arguments for rendering a ransomware payment have nonetheless become increasingly compelling:

- Ransomware payment is often the least costly option. For instance, the city of Atlanta spent more than $2.6 million on emergency efforts to respond to a ransomware attack that destabilized[1] municipal operations last year. Attackers, who infected the city's systems with the pernicious SamSam malware, asked for a ransom of roughly $50,000 worth of bitcoin. Atlanta officials have not stated whether they paid the ransom, or even tried, but it seems that they may not have even had the chance;[2] the attackers (who were, in a rare instance, allegedly caught)[3] quickly took the payment portal offline, and left the city to fend for itself;
- Ransomware payment can be in the best interest of stakeholders. For example, consider hospital patients in desperate need of an immediate operation but whose records are locked up by a ransomware attack — quick payment may save their lives; and
- Ransomware payment may mean not going public with the data breach. Arguably, state, federal and international breach notification laws arguably do not apply to ransomware attacks because no corporate data is actually appropriated.

Indeed, it is not surprising that paying ransomware attackers has become as routine a cost of business as paying the electric bill — but what is surprising (and shocking) is that no one seems to care.

U.S. Law Enforcement is Virtually Powerless Against Ransomware

Historically, national law enforcement agencies such as the FBI have successfully tackled crime waves orchestrated by nationally organized mobsters, internationally organized terrorists, and other notorious, sophisticated and nefarious criminal enterprises. But sadly, with a few exceptions,[4] the FBI has apparently met their match when it comes to capturing (or even identifying) ransomware attackers.

Ironically, the FBI has itself even been used as a pawn in ransomware schemes, illustrating the hubris of ransomware purveyors and their overall sense of invincibility.

In general, seeking law enforcement help for a ransomware attack unfortunately remains a very limited option. First, law enforcement has become inundated with ransomware reports and lacks the resources and wherewithal to assist victims. Second, most of the ransomware attackers are overseas, where merely obtaining electronic evidence or interviewing a witness, let alone successful extradition and prosecution, are rarely possible. Finally, ransomware demands are often at monetary levels in the hundreds or thousands of dollars — too small to warrant federal law enforcement consideration and clearly beyond of the jurisdiction of local law enforcement.

Thus, it should come as no surprise that: when padlocked files are business-critical (e.g., an important intellectual property formula); when encryption cannot be defeated (no matter how good the code-breaker) or when time is of the essence (e.g., when patient data is needed for life-saving surgery), paying the ransom can become the proverbial best worst option.

Law Enforcement and Ransomware: The Official View

The official line from federal law enforcement with respect to ransomware is: Report the incident and don't pay. Specifically, the FBI warns:

> The FBI doesn't support paying a ransom in response to a ransomware attack ... Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. [B]y paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.[5]

Notwithstanding, the FBI's official ransomware guidance does not state, "Do not pay under any circumstances." Rather, the FBI's "Ransomware Prevention and Response for CISOs" document,[6] states:

> Whether to pay a ransom is a serious decision, requiring the evaluation of all options to protect shareholders, employees and customers. Victims will want to evaluate the technical feasibility, timeliness, and cost of restarting systems from backup.

The FBI also warns that paying ransomware does not guarantee that a victim company will obtain from the attacker a working key to rescue their data. The FBI is aware of cases[7] where either the attackers fail to hand over the correct decryption key or are unwilling to comply with the original ransomware demands after payment is received. According to Trend Micro research, nearly 33 percent of firms that pay the ransom when attacked by ransomware fail to get their data back.[8] The FBI also urges ransomware victims to report ransomware attacks immediately[9] and seek help from the FBI in handling the situation.

Along similar lines, during an emergency meeting to address the WannaCry ransomware attacks,[10] Tom Bossert, then-homeland security adviser to President Donald Trump, discussed the perils of ransomware payment, and warned that victims could still lose access to files even after making a payment:

> Well, the U.S. government doesn't make a recommendation on paying ransom, but I would provide a strong caution. You're dealing with people who are obviously not scrupulous, so making a payment does not mean you are going to get your data back.

Law Enforcement and Ransomware: The Unofficial View

In some public settings, the FBI has warned that, without paying a ransom, victim companies may not be able to unlock their kidnapped data from ransomware attackers who use Cryptolocker, Cryptowall and other potent malware[11] strains.

A few years ago, a Security Ledger article quoted Joseph Bonavolonta, assistant special agent in charge of the FBI's Cyber and Counterintelligence Program in its Boston office:[12] "The ransomware is that good. To be honest, we often advise people to just pay the ransom ... The amount of money made by these criminals is enormous and that's because the overwhelming majority of institutions just pay the ransom.[13]

Indeed, the Ponemon Institute reported in a 2016 study that 48 percent of businesses victimized by ransomware paid the ransom (average ransomware payment being $2,500),[14] while a similar IBM Security study found that 70 percent of business victims paid the ransom during that same period.[15]

Cottage Industry of Facilitators

While the FBI might be of little help when it comes to ransomware, the private sector has stepped up, becoming remarkably inventive. Hence the genesis of a new and cottage industry of so-called "ransomware payment facilitators," typically data recovery, digital forensics, or other incident response firms who, by negotiating and transacting with the ransomware attackers, will attempt to recover ransomware victim's files for a fee.

While the practice of ransomware payment facilitation can raise a slew of legal and regulatory questions,[16] it is also a practice that has become tacitly acknowledged as a necessity, and a genuine lifesaver for ransomware victims who would otherwise have nowhere else to turn.

Thus, in cases where a particular ransomware attack cannot be fully mitigated, which is the norm these days, an experienced digital forensics firm can broker and validate a solution that minimizes the cost of recovery and prevents further extortion from the attacker.

Paying off the ransomware attackers typically entails: (1) sending the secret ransomware key file now stored on the victim's computer; (2) uploading that file (or data string) to the attackers together with a bitcoin payment; and (3) awaiting a decryption key or a tool a victim can use to undo the encryption on the victim company files. This is a complex and challenging process.

First off, a digital forensics firm can help a ransomware victim navigate the maze of setting up an account to handle bitcoin, getting it funded, and figuring out how to pay others with it. A digital forensics examiner may even be able to construct a payment scheme where rendering ransomware payments is conditional.

By using cryptocurrency features[17] to ensure that ransomware attackers cannot receive their payment unless they deliver a key, there can exist some added level of security and reliability upon the transaction. Matthew Green, a ransomware response expert, notes:

> A ransomware developer could easily perform payment via a smart contract script (in a system like Ethereum) that guarantees the following property: This payment will be delivered to the ransomware operator if and only if the ransomware author unlocks it — by posting the ransomware decryption key to the same blockchain.

Ransomware attackers can transform the entire ransomware payment process into what seems like an ordinary business transaction than an international extortion scheme. In fact, some recent ransomware attackers purportedly even offer a victim company a discount if the victim company transmits the infection to other companies,[18] just like referral programs of Uber or Lyft.

Responsible ransomware facilitators can also orchestrate a payment process that will satisfy the due diligence of any reimbursing insurance companies, who may be supporting the victim corporation and recompensing them for any ransomware payments and expenses pursuant to a ransomware cyberinsurance policy.

However, while a ransomware payment process may seem straightforward and rudimentary, the reality is far more complicated and rife with challenges. No ransomware payment process can guarantee that the ransomware attacker will provide a decryption key. The ransomware scheme may be nothing more than a social engineering ruse,[19] more like an old-fashioned Nigerian internet scam[20] than a malware infection — and the payment could end up being all for naught.

Indeed, ransomware attackers may no longer have the encryption key or may just opt to take a ransom payment, infect a company's system, and flee the crime scene entirely. Not only is the system of paying in untraceable bitcoin risky, but the transaction in its entirety is so risky, it hardly seems palatable. Nonetheless, the number of victim companies that pay ransomware demands continues to grow at an alarming rate,[21] as high as 70 percent of the time,[22] perhaps even higher.

Ransomware Notification/Disclosure Requirements: Ambiguous at Best

No one knows the true magnitude of the current ransomware outbreak. This is because many ransomware victims do not report or disclose the ransomware incident to anyone — preferring instead to keep the unpleasantness to themselves and move on.

Given that ransomware attacks typically involve locking up data (rather than accessing or exfiltrating data), notification responsibilities relating to a ransomware attack do not neatly align with other cybersecurity-related notification obligations and triggers. Ransomware differs from most cyberattacks 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 doing any direct harm to any individual or theft of individual data.

For instance, if a ransomware attacker encrypts a company's data but never accesses or exfiltrates that data, and then the ransomware attackers decrypt the data after receiving a ransom payment, there arguably never occurred any actual or specific customer harm. The threshold issue is therefore a technological one, based on the educated guesswork of digital forensic and malware reverse-engineering experts, to determine the full scope of attacker activity. If the experts findings conclude that the data is encrypted or otherwise "locked" through an automated process (where there is no viewing, copying, relocating or altering data), companies could argue that no disclosure is required.

In other cases, 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 cyberattackers. Other times, attackers not only encrypt the victim's data, but threaten to post the data publicly online, causing even more havoc.

For example, RAA[23] and Betabot[24] are ransomware strains that also swipe usernames and passwords from logins on to financial institutions, e-commerce sites, online payment platforms, and social networks. The Betabot malware masks itself as the "User Account Control" message box, but when you click on this box, it will infect your computer (see "betabox" snapshot).

Ransomware variants and iterations are infinite with each type creating thorny regulatory notification requirements, replete with loopholes and vague incident definitions. Meanwhile, disclosure of the ransomware attack can certainly inflict damage upon a company's reputation and invite future attacks — or even prompt regulatory (or plaintiffs bar) scrutiny for weak cybersecurity, such as having inadequate patching practices or antiquated data protection systems. Thus, if not legally required, it is not surprising that a victim company would be reluctant to disclose the ransomware attack to anyone.

Even the European Union's new General Data Protection Regulation[25] contains similar flexibility with respect to ransomware attack disclosures, providing legal teams with plenty of wiggle room.

The GDPR

With respect to personal data of individuals residing in the EU, the GDPR requires notifying a GDPR 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. Thus, at first glance, with respect to a ransomware infection that occurs in a considerable number of workstations and servers that are central to processing personal data, the attack would constitute a breach under the GDPR.

However, there is a glitch: The GDPR applies a harm-based threshold to its criterion, which arguably creates a significant exception for ransomware. For example, per Article 34 (1) of the GDPR,[26] 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 undoubtedly offer data protection officers and their outside counsel opportunities to debate the necessity of notification and arguably avoid notification conditions altogether.

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:[27] (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.

Indeed, just like U.S. federal and state law enforcement and regulatory authorities, given that ransomware attacks typically do not involve the purloining of data, the GDPR offers flexibility of interpretation, and will be very dependent on specific circumstances. Moreover, given its overall opacity, some organizations may decide that the risk of being hit with a GDPR fine far outweighs the risk of not disclosing a ransomware attack.

A Matter of Contract

Failure to notify law enforcement or anyone else about a ransomware attack might not just be a matter of self-preservation for corporate ransomware victims, it may also be a matter of contract (albeit an illegal and unenforceable one).

Consider the recent rants of the notorious cyberattacker (or perhaps gang) known as the "Dark Lord," notorious for[28] targeting banks, health care insurance firms, plastic surgery clinic, media giants like Netflix, and Steve Harvey's "Funderdome" TV show.

Per recent reports,[29] the group has gone as far as leaking student data and sending death threats to an Iowa-based Johnston Community School District, forcing it to close some of its schools. Messages about physically harming kids and even killing them were sent to parents via text.

According to Motherboard,[30] in an announcement published on Pastebin, the Dark Overlord points to several different insurers and legal firms, claiming specifically that it hacked Hiscox Syndicates Ltd, Lloyds of London, and Silverstein Properties.

The stolen data, according to the group,[31] includes emails, nondisclosure agreements, liability analysis, retainer agreements, defense formations, litigation strategies, settlements, collection of expert witness testimonies, testimonies, communications with government officials in countries all over the world, voicemails, dealings with the FBI, U.S. Department of Justice and U.S. Department of Defense, and other confidential communication.

The stolen data apparently relates to the 9/11-related work of law firms representing a slew of different plaintiffs and defendants, including: first responders seeking compensation for exposure to contaminants at the site, the owner of the towers looking to collect from the airlines[32] that let the hijackers on board, victims looking to haul the government of Saudi Arabia into U.S. court,[33] and others.

According to the Dark Overlord's Pastebin post, Hiscox is well aware of the attack and paid the initial ransom but breached its agreement by involving law enforcement authorities. The Pastebin posting states:

> This involvement with law enforcement became clear to us months later through a source of ours disclosing details of the client to us that we never informed the source about. We were absolutely appalled by this transgression against our agreement. We decided to offer this company a second chance to repent, accept responsibility, and satisfy our penalty request. They declined to accept our offer, so we're here today ... If you're one of the dozens of solicitor firms who was involved in the litigation, a politician who was involved in the case, a law enforcement agency who was involved in the investigations, a property management firm, an investment bank, a client of a client, a reference of a reference, a global insurer, or whoever else, you're welcome to contact our e-mail below and make a request to formally have your documents and materials withdrawn from any eventual public release of the materials. However, you'll be paying us.

Looking Ahead

Ransomware attacks can trigger a litany of anticipated and unanticipated consequences for victim companies — including millions of dollars in related costs and expenses, unquantifiable potential liabilities, overwhelming management drag, and significant operational and reputational damage. Meanwhile the ransomware industry seems to be thriving, with ransomware payment demands growing in size and audacity and malware sophistication growing in intricacy and efficacy.

Given its ease, anonymity and speed, cryptocurrency such as bitcoin has set in motion the ransomware industry boom, facilitating its extraordinary growth. Bitcoin not only makes it easier to remain anonymous, but bitcoin also enables a pseudo-anonymous payment mechanism where the extorted funds can be immediately transferred into criminal hands.

Transactions in cryptocurrencies like bitcoin lack a discernable audit trail, 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 backup systems fail), ransomware attacks and iterations will likely continue to flourish.

Stopping the ransomware crime wave must therefore begin at the front end, depriving cybercriminals of access to financial channels, and financial penalties at the back end, particularly asset forfeiture, recovering the proceeds of criminal activity. 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 Financial Crimes Enforcement Network regulatory actions);
- Speaking more boldly to discourage ransomware payments that monetize crime, perhaps via 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
- Adding more ransom ware attackers to terrorist lists.[34] For example, the U.S. Department of the Treasury's Office of Foreign Assets Control imposed sanctions on two Russian individuals[35] for engaging in malicious cyber-enabled activities. One of the individuals was responsible for the development and use of Cryptolocker, a form of ransomware, which infected more than 120,000 U.S. victims. According to OFAC, he and his group are responsible for taking over $100 million from financial institutions and government agencies.
- 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.[36]

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 often on their own. Hence the trend toward tendering ransomware payment and keeping it all quiet — what other option is there?

The only guarantees during a ransomware attack are the feelings of fear, uncertainty, vulnerability and dread inevitably experienced by the corporate victim. Someone needs to stop the madness — or in the least, start talking about it. Right now, the silence is deafening.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

[2] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[3] https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public

[4] https://www.al.com/news/2018/11/samsam-ransomware-attack-arrests-iranian-men-charged-with-atlanta-cyber-attack-2-in-alabama.html

[5] https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

[6] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

[7] https://www.cyberscoop.com/paying-escape-ransomware-goes-wrong/

[8] http://www.theregister.co.uk/2016/09/07/uk_ransomware_victim_survey/

[9] https://www.ic3.gov/media/2016/160915.aspx

[10] http://consumersresearch.org/is-it-illegal-to-provide-bitcoin-used-to-pay-ransomware-demands/

[11] https://securityledger.com/tag/malware-2/

[12] https://www.welivesecurity.com/2016/05/09/fbi-ransomware-extortionists/

[13] https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/

[14] https://www.carbonite.com/globalassets/files-white-papers/ransomware-report.pdf?SID=cso&cm_mmc=affiliate-_-CJ-_-www.carbonite.com-_-8200811&c3ch=Affiliate&c3nid=8200811&pct-network-name=commission-junction&pct-network-pid=8200811&cj-publisher-id=4

[15] http://invenioit.com/security/ransomware-statistics-2016/

[16] https://www.johnreedstark.com/publications/ransomware-payment-legality-logistics-mitigation-insurance/

[17] https://blog.cryptographyengineering.com/2017/02/28/the-future-of-ransomware/

[18] https://www.theregister.co.uk/2016/12/11/ransomware_offer_pay_us_a_770_ransom_or_infect_two_friends/

[19] https://blog.watchpointdata.com/ransomware-variant-wont-decrypt-files-after-ransom-paid

[20] https://www.theregister.co.uk/2016/08/08/nigerian_scammer_busted_after_he_infected_himself/

[21] http://invenioit.com/security/ransomware-statistics-2016/

[22] http://invenioit.com/security/ransomware-statistics-2016/

[23] https://www.bleepingcomputer.com/news/security/the-new-raa-ransomware-is-created-entirely-using-javascript/

[24] https://blog.knowbe4.com/bid/336921/fbi-beta-bot-malware-kills-your-anti-virus-and-steals-data

[25] https://ec.europa.eu/info/law/law-topic/data-protection_en

[26] https://www.privacy-regulation.eu/en/34.htm

[27] https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/

[28] https://brica.de/alerts/alert/public/1242083/dark-overlord-hackers-vow-to-leak-911-related-data-stolen-from-law-firm/

[29] https://brica.de/alerts/alert/public/1242083/dark-overlord-hackers-vow-to-leak-911-related-data-stolen-from-law-firm/

[30] https://motherboard.vice.com/en_us/article/yw79k5/hacker-group-threatens-dump-911-insurance-files-dark-overlord

[31] https://brica.de/alerts/alert/public/1242083/dark-overlord-hackers-vow-to-leak-911-related-data-stolen-from-law-firm/

[32] https://www.law.com/newyorklawjournal/almID/1202611552817/silverstein-loses-bid-to-collect-35-billion-from-airlines-for-911/

[33] https://www.law.com/newyorklawjournal/sites/newyorklawjournal/2018/01/18/judge-mulls-if-new-law-allows-911-victims-claims-against-saudi-arabia/

[34] https://www.state.gov/j/ct/rls/crt/2015/257520.htm

[35] https://home.treasury.gov/news/press-releases/sm0338

[36] http://www.stites.com/uploads/learning-center/Ramsey_Ransoming-data_Jan2016.pdf

---