

---

4800 HAMPDEN LANE, SUITE 200, BETHESDA, MARYLAND 20814  
(301) 335-8387 WWW.JOHNREEDSTARK.COM

## ***Ransomware Payment: Legality, Logistics, Mitigation, Insurance and Proof of Life***

**By John Reed Stark\***

In the 2000 American thriller film *Proof of Life*, the title refers to a phrase commonly used to indicate proof that a kidnap victim is still alive. As an expert negotiator in kidnapping cases, Terry Thorne, played by Russell Crowe, is engaged to bargain for a corporate kidnap victim's safe return.

The film *Proof of Life* is not just a compelling narrative – its premise and main character also provide some useful insights into managing the emerging threat of ransomware. Ransomware, a special and more nascent type of malware, prevents or limits users from accessing their data, by locking system screens or user files, unless and until a ransom is paid.

*Proof of Life's* screenplay was partly inspired by Thomas Hargrove's book *The Long March to Freedom*, which recounts how the release of the once-kidnapped Hargrove was negotiated by Thomas Clayton, the founder of his eponymous kidnap-for-ransom consultancy Clayton Consultants (now part of risk management firm, Triple Canopy).

Just like Clayton Consultants, the team advising a ransomware victim company, whether a hospital or global corporate conglomerate, must employ a thoughtful, careful and methodical protocol to survive the ransomware crisis. Like any hostage situation, when a cyber-attacker locks up critical data files, the logistics and legalities of ransomware refusal, acquiescence or capitulation can be both elaborate and complicated.

To make matters worse, 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 an 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 while clearly outside of the jurisdiction of local law enforcement.

Thus, it should come as no surprise that a significant number of ransomware victims opt to pay the ransom. 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*. Moreover, the typically *de minimus* ransomware payment demands (on average, about \$679) are more akin to a financial nuisance than a material fiscal line-item, so from a cost-benefit perspective, payment can make the most sense.

Under any circumstance, ransomware has quickly become a novel, multifaceted and emerging risk to all corporate enterprises, and like any other material risk, should be addressed and mitigated in a reasonable, lawful, robust and effective manner.

This article provides guidance on the legal issues, logistical considerations and financial implications when managing ransomware threats, including an exposition of the unique issues which can arise when seeking *proof of life* and opting to meet the monetary demands of ransomware attacker.

### **What is Ransomware?**

Ransomware is a type of malicious software that infects a computer and restricts users' access to certain data, systems and/or files until a ransom is paid. Ransomware can come in many forms and iterations and like any other virus or infection, ransomware can evolve and transmogrify to counter cyber-defenses and remediation. Although only a fraction of ransomware attacks are actually reported to federal authorities, the U.S. Department of Justice reports over 4,000 ransomware attacks occur daily.

A ransomware victim company's files are rarely exfiltrated by a ransomware attacker, rather the attacker encrypts the files so a victim company cannot access them. Then the hacker offers to sell the encryption key to the victim, typically payable in an anonymizing online crypto-currency such as Bitcoin. The usual ransomware demand comes with a deadline -- after which time, the ransomware attacker threatens that the key will be destroyed or will expire, rendering the kidnapped files forever inaccessible. In many cases the ransom note that hijacks the victim's screen is accompanied by a digital clock ominously ticking down the minutes and seconds from 72 hours. When the timer expires, the ransom demand usually goes up or even doubles -- or the data is permanently locked and henceforth unrecoverable.

Bitcoin and other convertible crypto-currencies have become the keystone to current ransomware schemes, rendering the transactions practically untraceable and well suited for criminal transactions. Unlike the sequence of events during to a common kidnapping scenario, where the exchange of money arguably places criminals in their most vulnerable position, virtual kidnapping of ransomware actually facilitates anonymity throughout the Bitcoin transaction process.

### **Ransomware Growth**

According to a recent study by IBM, spam emails loaded with ransomware increased 6,000 percent in 2016 compared with 2015, comprising almost 40 percent of all spam messages in 2016. Another report, from cybersecurity firm Symantec, cited 460,000 ransomware attempts in

2016, up 36% from 2015, with the average payment demand ballooning from \$294 to \$1,077, a 266% increase. Ransomware attacks have grown almost exponentially for several reasons:

- The ransomware business model works, with the [FBI stating that ransomware is on pace to become a one billion dollar source of income for cybercriminals in 2017](#);
- Ransomware start-up costs are cheap. Ransomware software is readily and easily available – and is extraordinarily inexpensive. Ransomware is available for rent; for purchase or even in kits for building. Indeed, [60 percent of the Internet’s top sites sell ransomware](#); and
- Ransomware schemes are typically successful. [One recent study](#) found that 70 percent of business victims paid the hackers to get their data back. Of those who paid, 50 percent paid more than \$10,000 and 20 percent paid more than \$40,000.

Ransomware attacks target the most vulnerable part of a company’s computer networks: people. The primary attack vector for ransomware is an employee who has clicked on a file or a linked he or she should not have clicked. That employee may be:

- An accidental insider (e.g. an inattentive employee infiltrated due to inadvertent behaviors or broken business processes);
- A compromised insider (e.g. a targeted employee via social engineering and infiltrated due to malware infections or stolen credentials); or
- A malicious insider (e.g. a so-called [bad leaver](#) or criminal insider who infiltrate via corporate espionage and sabotage).

[Ransomware is sometimes embedded in seemingly legitimate downloads such as software updates or resume files](#). Fake Adobe Flash updates are a notorious Trojan horse for delivering ransomware because Flash is such a ubiquitous add-on to most Internet browsers. Once inside a network, some ransomware [can seed itself to additional computers](#) or other devices via SMS messages or a user’s contact list.

What makes ransomware countermeasures challenging is the evolution of ransomware variants. There has been a tremendous increase in ransomware strains – reaching almost epidemic proportions. Indeed, [new ransomware strains are now being created](#) to tap into the mobile user base, which can impact both personal and business information, already dramatically expanding the ransomware threat landscape, [diversifying and expanding their platforms](#), capabilities and techniques in order to accrue more targets.

[Per recent reports](#), in the third quarter of 2011, about 60,000 new variants of ransomware were detected. That number doubled to over 200,000 in 2012; quadrupling to over 700,000 variants from 2014, to the first quarter of 2015. In the first quarter of 2016, security firm Kaspersky Lab revealed 2,900 new “modifications” of existing ransomware, a 14% increase from the last quarter, and a 30% increase from the previous quarter.

As the *Internet of Things* begins to establish a foothold in daily life, ransomware growth seems poised to become more severe and more widespread. [Market forecaster Gartner expects 6.4 billion connected devices](#) will surround us in the home and workplace this year, a \$30 billion market by the year 2020. This growing network of Internet-connected household devices, from Samsung refrigerators to Nest thermostats, will undoubtedly render individuals and corporations increasingly vulnerable to ransomware attacks.

## Recent Ransomware Attacks

While ransomware has beleaguered victim companies for much of the last decade, a recent global spate of ransomware attacks has prompted intense media coverage and worldwide apprehension and concern.

For instance, in April 2017, a ransomware group known as *Shadow Brokers* coopted a ransomware exploit (nicknamed [Eternal Blue](#)) from the U.S. National Security Agency, and took advantage of a Windows vulnerability, targeting a wave of hospitals. The ransomware extortion demands impacted more than just corporate operations and secrets; suddenly, a cyber-attack impacted the lives of sick hospital patients, prompting an [almost international hysteria](#).

The vulnerability, patchable for new Microsoft systems but not necessarily for older systems upon which many hospitals were running, was dubbed “WannaCry” or “WannaCrypt” ransomware, and [according to Europol](#), claimed over 200,000 victims in over 150 countries.

Similarly, in late June 2017, another strain of ransomware hit at least six countries, including and primarily Ukraine, where it was blamed for a large and coordinated attack on key parts of the nation's infrastructure, from government agencies and electric grids to stores and banks. [According to Microsoft](#), this outbreak, referred to as NotPetya - aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya and Diskcoder.C - resulted in "a less widespread attack" than WannaCry, aka WannaCrypt.

As a result of NotPetya ransomware, A.T.M.'s in the Ukraine apparently stopped working; workers were forced to manually monitor radiation at the old Chernobyl nuclear plant when their computers failed; and data security personnel at companies around the world — from Maersk, the Danish shipping conglomerate, to Merck, the drug giant in the United States — [were reportedly scrambling to respond](#). Even an Australian factory for the chocolate giant Cadbury [was affected](#).

Though more sophisticated than WannaCry and employing the same Eternal Blue server message block exploit, NotPetya's global impact was [reportedly blunted](#) by its own limited attack capabilities (e.g. by a default setting, the infected system reboots after 60 minutes, and the malware does not persist after the reboot). "This means that the threat can only do lateral movement and exploitation of other machines during this limited time," [Microsoft says](#). "This reduced the reach of the attack."

## 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.”*

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 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. The FBI also urges ransomware victims to report ransomware attacks immediately and seek help from the FBI in handling the situation.

Along similar lines, during an emergency meeting to address the WannaCry ransomware attacks, Tom Bossert, Homeland Security Advisor 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 strains.

“The ransomware is that good,” said Joseph Bonavolonta, the Assistant Special Agent in Charge of the FBI’s CYBER and Counterintelligence Program in its Boston office. “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.”

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

Even some law enforcement officials themselves have decided to cut their losses by paying off the purveyors of ransomware. For instance, in the Massachusetts townships of Tewksbury and Swansea, ransomware attackers made off with \$500 and \$750 bounties, respectively. Elsewhere, police departments in the Chicago suburbs of Midlothian and Dickson County, Tenn., also paid ransom amounts to ransomware attackers. That even law enforcement officials have opted to cut their losses by succumbing to, and paying off, ransomware attackers demonstrates how oddly commonplace ransomware payments have become.

### **Counsel as Quarterback for Ransomware Response**

Ransomware is a crime, has significant regulatory implications and can involve important legal responsibilities and liabilities. At a minimum, ransomware schemes run afoul of the federal computer crime statute, 18 U.S.C. § 1030, and particularly subsection (a)(7), which forbids hacking intended to extort something of value from the victim.

Above all else, the legal ramifications of any ransomware incident or failure can be calamitous for any public or private company. Even the most traditional realms of IT dominion such as exfiltration analysis, malware reverse engineering, digital forensics, logging review and most technological remediation measures **are rife with legal and compliance issues and a myriad of potential conflicts.**

For instance, after a cybersecurity incident such as a ransomware attack, law enforcement, regulators, vendors, partners, insurers, customers and others may:

- Request forensic images of impacted systems;
- Demand copies of *indicators of compromise*;
- Mandate that their own auditors or examiners visit sites of infiltration and conduct their own audit and investigation;
- Want to participate in remediation planning;
- Seek interviews and interactions with IT personnel;
- Require briefings from a victim company's forensic experts and data security engineers; or
- Ask to attach a recording appliance to a victim company's network in hope of capturing traces of attacker activity, should an attacker return.

These requests raise a host of legal issues, including how exactly to respond to each request and whether any response would violate the privacy of customers; be at odds with commercial agreements; result in a waiver of the attorney-client or work product privileges; or have any other legal/compliance consequences.

Because so many incident response issues are critical to the very survival of a company, who else but the GC can oversee and direct investigative workflow, commanding the investigation and remediation for the C-suite, sharing with senior management the ultimate responsibility for key decisions, while having the responsibility and duty of reporting to the company's board.

### **Ransomware and the Attorney-Client Privilege**

Attorney involvement, awareness, leadership, and direction are not the only essentials for managing the quagmire of legal issues arising during a ransomware response. GC involvement also triggers the protections afforded by the attorney-client and work product privileges, a critical component in the response to data security incidents.

The involvement and direction of counsel in the context of any investigation will presumably apply to the work product produced not only directly by the legal team members but also by the outside advisors, including the digital forensic investigators engaged by internal or outside counsel.

This is standard practice in the context of any other type of investigation – a cyber incident is no different. There is nothing nefarious or extraordinary about this approach, it is a time-honored and tested standard operating procedure. The involvement of counsel establishes a single point of coordination and a designated information collection point.

Counsel as quarterback of ransomware response also enhances visibility into the facts, improves the ability to pursue appropriate leads and, most importantly, ensures the accuracy and completeness of information before it is communicated to external audiences. Otherwise, incomplete and/or inaccurate information could be released, only to have to later be corrected or even retracted.

### **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 triggers a legal notification requirement, including notice to:

State regulators (per state privacy statutes, rules and regulations);

- Shareholders (per SEC disclosure obligations);
- Vendors, partners and other entities (Many companies now incorporate rigorous cybersecurity notification requirements into their contracts, which can trigger when a victim company experiences a ransomware attack.);
- Insurance carriers (especially if a victim company plans to make an insurance claim, relating to the ransomware attack);
- Customers (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); and
- Any other constituency who may have a vested interest in a victim-company.

With respect to state regulatory notifications there is some grey area worthy of mention. 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](#). While most states require some form of notice 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.

The threshold issue is a technological one – probably 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 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](#).

With respect to some of the more onerous and specific federal notification rules, such as under the Health Insurance Portability and Accountability Act of 1996 ([HIPAA](#)), digital forensics analysis can also 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. Whether ransomware’s data encryption 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.

In addition, under the new EU General Data Protection Regulation, effective May 25, 2018, there is a requirement to notify the supervisory authorities 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. The [fines for violating this regulation](#) are significant—up to 4% of global annual turnover or €20 million (whichever is the higher), so any late notification will need to be justified.

### **Ransomware Investigative Tactics**

While determining the bona fides of a ransomware strain is always challenging, an experienced digital forensic examiner can find some answers by searching for some of the more typical cyber-indicators. Ransomware malware is characteristically a type of tool, which is not only known to most professionals, but may even be readily available for purchase online. If the name and modus operandi of the ransomware is new or otherwise unknown, rather than a victim firm being “[patient zero](#),” the ransomware may turn out to be bogus.

Digital forensic experts can also research the Bitcoin payment address; the malware message; any [relevant phishing emails](#); and any other of the ransomware’s characteristics in data security research forums and internal archives, to analyze recent commentary about the ransomware and test its efficacy and validity.

There are also a range of digital forensics tests to initiate upon an infected file to assess a ransomware strain’s actual efficacy. For instance, one simple test is to return the file name to its original form. Real ransomware changes the file extension of encrypted files. The Ransomware files may not be encrypted but just renamed to provide the illusion of encryption to cajole a ransom payment. A digital forensics expert can also investigate the severity of the attack;

reverse-engineer the malware that has taken control of victim data; and attempt a full-fledged data recovery.

## **Ransomware Payment**

In cases where a particular ransomware attack cannot be fully mitigated, 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 other people 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](#) 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. [One 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 may portray the entire ransomware payment process as more akin to 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](#), just like referral programs of Uber or Lyft.

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](#), more like an old fashioned [Nigerian Internet scam](#) 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](#).

## **The Legalities of Ransomware Payment**

Though the FBI has [hinted at the possible illegality of paying a ransomware demand](#), the FBI has never specifically stated that the payer could actually be charged with a crime. It would seem

rather obvious that with respect to any criminal statute, [actions taken under duress do not ordinarily constitute a crime](#). Moreover, the ransomware attacker possesses the criminal intent, not the victim who agrees to pay. However, there is little specific legal authority on the subject of payment and negotiation with ransomware attackers, so the legalities of payment are worthy of some analysis.

In general, legal commentary and case law regarding ransom payments is limited. However, in a germane 2011 British case, [Masefield AG v Amlin Corporate Member Ltd \(The Bunga Melati Dua\)](#), relating to maritime piracy and ransom demands for safe return of the vessel and crew, the court faced a somewhat analogous scenario. Specifically, the British Court of Appeal held that there was no general public policy argument against paying ransoms, stating that:

*“...there is no universal morality against the payment of ransom, the act not of the aggressor but of the victim of piratical threats, performed in order to save property and the liberty or life of hostages. There is no evidence before the court of such payments being illegal anywhere in the world. This is despite the realization that the payment of ransom, whatever it might achieve in terms of the rescue of hostages and property, itself encourages the incidence of piracy for the purposes of exacting more ransoms. (Perhaps it should be said that the pirates are not classified as terrorists. It may be that the position with regard to terrorists is different).”*

Though addressing hostage ransoms, and not ransomware, former President Barak Obama provided a similar message in his [Statement by the President on the U.S. Government’s Hostage Policy Review \(June 24, 2015\)](#):

*“I firmly believe that the United States government paying ransom to terrorists’ risks endangering more Americans and funding the very terrorism that we’re trying to stop. And so I firmly believe that our policy ultimately puts fewer Americans at risk. At the same time, we are clarifying that our policy does not prevent communication with hostage-takers -- by our government, the families of hostages, or third parties who help these families . . . In particular, I want to point out that no family of an American hostage has ever been prosecuted for paying a ransom for the return of their loved ones. The last thing that we should ever do is to add to a family’s pain with threats like that.”*

## **Ransomware and the FCPA**

The Foreign Corrupt Practices Act of 1977 (FCPA) prohibits payments to foreign government officials to assist in obtaining or retaining business or directing business to any person. Laws such as the FCPA reflect an alternative approach to deterring bribes, by penalizing those on the payment side of the transaction.

Specifically, the [FCPA prohibits giving something of value for the purpose of](#): "(i) influencing any act or decision of [a] foreign official in his official capacity, (ii) inducing such foreign official to do or omit any act in violation of the lawful duty of such official, or (iii) securing any improper advantage ... to obtain or retain business for or with ... any person." The law provides an affirmative defense for payments that are "lawful under the written laws and regulations" of the country.

Given the FCPA threshold requirement that a payment must be made to assist in obtaining or retaining business for the individual or company or directing that business to another person, a ransomware scenario [does not appear to trigger the FCPA](#).

However, FCPA's enforcement can provide a useful analogy when considering the legalities of paying a ransomware demand. [U.S. companies often face extortionate demands from foreign police, bureaucrats, and regulators, who threaten to hold, expel, or even harm employees if ransoms are not paid](#). And there have always been [questions whether](#) those involuntary payments can violate the FCPA. The [DOJ-SEC Guidance on FCPA](#) addresses this issue, stating:

*“Does the FCPA Apply to Cases of Extortion or Duress? Situations involving extortion or duress will not give rise to FCPA liability because a payment made in response to true extortionate demands under imminent threat of physical harm cannot be said to have been made with corrupt intent or for the purpose of obtaining or retaining business.”*

This notion, that under FCPA an individual is not guilty of a criminal offense when forced to do so by duress or extortion, is confirmed in [United States v. Kozeny, 582 F.Supp.2d 535, 540 \(S.D.N.Y. 2008\)](#). Specifically, in the [Kozeny](#) decision, the United States District Court for the Southern District of New York ruled that extortion or duress under the threat of imminent physical harm would excuse the conduct (essentially negating a corrupt intent), stating:

*“ . . . while the FCPA would apply to a situation in which a "payment [is] demanded on the part of a government official as a price for gaining entry into a market or to obtain a contract," it would not apply to one in which payment is made to an official "to keep an oil rig from being dynamited," an example of "true extortion." The reason is that in the former situation, the bribe payer cannot argue that he lacked the intent to bribe the official because he made the "conscious decision" to pay the official. In other words, in the first example, the payer could have turned his back and walked away—in the latter example, he could not.”*

Whether the “economic duress” of a typical ransomware attack would rise to the level of “true extortion” as described in the [Kozeny](#) decision remains untested, and might be viewed as insufficient to excuse conduct from sanctions under the FCPA.

The FCPA could also potentially apply in ransomware scenarios where the cyber-criminal has a known connection to a foreign government. While the concealed identity of cyber-criminals involved in ransomware attacks likely prevents a payer from knowing that a payment violates the FCPA, the issue could still arise when a digital forensic expert identifies a ransomware attacker's modus operandi to be that of a state sponsored organization (e.g. from Russia, North Korea or Iran).

## **Foreign Sanctions and Ransomware**

Like the FCPA, international sanctions regimes are also designed to prevent payments to certain designated payees, institutions, and countries who are enemies of the U.S, such as terrorists and terrorist organizations. In the United States, the [Treasury's Office of Foreign Asset Controls](#) (OFAC) supervises these programs, such as the [Trading with the Enemy Act](#) and the [International Emergency Economic Powers Act](#) (IEEPA).

Under these Acts, ransom payments (whether directly or indirectly through an intermediary) to [Foreign Terrorist Organizations \(FTOs\)](#) or [Specially Designated Global Terrorists \(SDGTs\)](#) identified by OFAC, are illegal under U.S. law. Monetary contributions to FTOs are considered material support under 18 U.S.C. 2339B, while transfers to SDGTs are violations of economic sanctions imposed pursuant to the IEEPA.

For example, in a February 2017 [cyber-attack](#) against the British National Health System, the attackers appeared to be ISIS and in particular, the [Tunisian Falange Team](#), which posted graphics and pictures decrying at the war in Syria. Whether a similar attack against a U.S. hospital, with a similar evidentiary trail indicating terrorist attribution, would trigger the limitations imposed OFAC is unclear and untested. However, any digital forensic findings of a ransomware attack indicating terrorist attribution or involvement is certainly worthy of consideration when contemplating a ransomware payment.

### **Ransomware and Conspiracy**

Whether a payer of a ransomware demand can be held to have entered into a conspiracy with the ransomware attacker seems unlikely and contrary to the public interest. A conspiracy is an *agreement* with another that a criminal course of conduct is to be pursued. Ransomware payments do not appear to be the kind of *agreements* contemplated by conspiracy statutes, but instead are forced arrangements dictated by a ransomware attacker.

However, other profiting and culpable participants in the Bitcoin payment scheme to pay a ransomware attacker might find themselves facing criminal penalties. [Anthony Murgio, who recently pled guilty to operating as a money transmitter without a license in 2015, was also charged with violating Title 18 U.S.C., Section 1030\(a\)\(7\)](#) and sentenced to 5 ½ years in prison. Federal prosecutors alleged that Murgio and his co-conspirators benefitted from transactions providing victims with Bitcoin to pay off ransomware demands. The Murgio indictment states:

*“As part of the unlawful Coin.mx scheme, Anthony P. Murgio, the defendant, and his co-conspirators knowingly processed and profited from numerous Bitcoin transactions conducted on behalf of victims of ransomware schemes...By knowingly permitting ransomware victims to exchange currency for Bitcoins through Coin.mx, Murgio and his co-conspirators facilitated the transfer of ransom proceeds to the malware operators while generating revenue for Coin.mx.”*

Unlike a ransomware payer, Murgio was a part of the payment process and clearly facilitated the ransomware transactions with *unclean hands* – possessing the kind of felonious intent required for money laundering criminal liability. Crypto-currency sellers or exchange operators may be caught up in legal trouble if: they have avoided or neglected reporting requirements or have not registered as a money transmission business (like Murgio), or, if they were criminally complicit with the ransomware attackers.

The distinction seems clear: if a Bitcoin seller actively aided and abetted a ransomware attacker, knowingly profiting from the scheme, the Bitcoin seller could be criminally liable. However, if a digital forensics firm made Bitcoin available to a client and provided technical advice as to how

to pay in Bitcoin, then, like Thomas Clayton in *Proof of Life*, criminal liability seems wholly inappropriate.

### **Ransomware: To Pay or Not To Pay**

For now, it seems that paying ransomware, while obviously risky and empowering/encouraging ransomware attackers, does not appear to break any laws – and even if payment is arguably unlawful, seems unlikely to be prosecuted. Thus, the decision whether to pay or ignore a ransomware demand, seems less of a legal, and more of a practical, determination -- almost like a cost-benefit analysis.

The arguments for rendering a ransomware payment include:

- Payment is the least costly option;
- Payment is in the best interest of stakeholders (e.g. a hospital patient in desperate need of an immediate operation whose records are locked up);
- Payment can avoid being fined for losing important data;
- Payment means not losing highly confidential information; and
- Payment may mean not going public with the data breach.

The arguments against rendering a ransomware payment include:

- Payment does not guarantee that the right encryption keys with the proper decryption algorithms will be provided;
- Payment further funds additional criminal pursuits of the attacker, enabling a cycle of ransomware crime;
- Payment can do damage to a corporate brand;
- Payment may not stop the ransomware attacker from returning;
- If victims stopped making ransomware payments, the ransomware revenue stream would stop and ransomware attackers would have to move on to perpetrating another scheme; and
- Using Bitcoin to pay a ransomware attacker can put organizations at risk. Most victims must buy Bitcoin on entirely unregulated and free-wheeling exchanges that can also be hacked, leaving buyers' bank account information stored on these exchanges vulnerable.

### **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 stays 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 ransomware attackers and prevent them from going deeper into a corporate 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; and

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**

When confronted with a ransomware attack, the options all seem bleak. Pay the hackers – and the victim may not only prompt future attacks, but there is also no guarantee that the hackers will restore a victim’s dataset. Ignore the hackers - and the victim may incur significant financial

damage or even find themselves out of business. The only guarantees during a ransomware attack are the fear, uncertainty and dread inevitably experienced by the victim.

Even under the best-case scenario, where a victim has maintained archives and can keep their business alive, the 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 motel*, 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 simpler to remain anonymous, but also enables a nameless payment mechanism where the extorted funds can be immediately transferred into criminal hands.

Transactions in crypto-currencies 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 crypto-currency payment schemes exist, 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 upon 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;
- Speaking more boldly discouraging 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; 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 are theoretical and even if implemented, might still not 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. never underestimate the impact of ransomware and never 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.

