Ransomware: Often, there *might be* honor among thieves

Ransomware is a business and as such, it has rules, requirements, customer support, and a driving need for customer loyalty and trust. Trust your attacker? Evan Schuman explains.

Looking for insights in modern literature to address the challenges facing CISOs might seem farfetched, but there is some logic to this. Lewis Carroll's *Alice's Adventures in Wonderland* and *Through the Looking Glass* illustrates the challenges posed by ransomware. While this might seem contradictory on the surface, the options and twisted logic Alice faced are eerily similar to those posed by this pernicious malware.

Yet fight ransomware CISOs must do, so be prepared to abandon logic and enter the looking glass that is modern-day cybersecurity.

The good news is that there are ways to tilt those ransomware calculations in the company's favor so you are less likely to have to pay the ransom. Fighting ransomware in 2019 forces CISOs to embrace quite a few contradictions that are most vexing. Here are some to consider:

- In a logical world, it is only the ransom-demander who is the criminal with the enterprise target merely a victim. But in the contrarian world of ransomware, there is an excellent chance that a company — or a company employee — paying a ransom might be violating federal law by sending money if the attacker is associated with terrorists or is in a country that doesn't play nice with the U.S. Ultimately, you could be prosecuted for it. If you do not pay, you can lose your data. If you do pay, you might go to jail. Tough choice.
- There is potentially more legal trouble for the ransomware victim: Compliance and breach disclosure issues could be expensive and damage the company image. There could be related costs, such as states that require purchasing identity theft insurance for all impacted consumers. But were the consumers impacted? This raises a question that is difficult to answer: How far can a CISO trust the representations of the attacker? The company's decision here can have expensive repercussions.

By all indications, an attack merely seemed to encrypt sensitive data. But given that the bad guys needed to first access it to encrypt it, might they have copied the data first so they could double-dip and sell the data on the black market even if the company pays the ransom? If the attacker has not yet done so, does that exfiltration still trigger compliance-related costs and efforts? Are companies required to assume that the attackers did more than they claimed? Will regulators make that assumption? Questions like these can send even the most grizzled CISO down the proverbial rabbit hole looking for answers.

- As is the case when anyone is dealing with a kidnapper who demands a ransom, it seems foolish to trust such a thief. What would stop them from taking your ransom and then opting to renege and not

OUR EXPERTS: Ransomware

Dante Disparte, CEO, Risk Cooperative

Bryan Kissinger, CISO, Banner Health

Scott Laliberte, managing director and global leader of cybersecurity and privacy, Protiviti

Tatiana Melnik, private practice attorney

Joshua Motta, CEO, Coalition

Mark Rasch, former federal prosecutor, private practice cybersecurity attorney

Sean Tierney, director of cyber intelligence, Infoblox

50%

Percentage of companies that report that they are not adequately prepared for a ransomware attack.

– healthitsecurity.com

release your data? And yet, ransomware experts say that ransomware in 2019 is a highly professional business and that these ransomware businesses, which will often have customer service and free tech support, can be trusted to do what they say. If they do not, their highly lucrative business model would quickly implode. Is there a CISO or CEO willing to take that chance?

Dante Disparte, CEO, Risk Cooperative

• The official policy of just about every Fortune 1000 company is to never pay a ransom. And yet, just about all of those same companies routinely will pay that ransom when the ROI calculation of fighting versus paying makes it clear that paying is better. That said, the calculation sometimes tells companies to not pay, depending on the situation and the nature of the attack. Was the City of Atlanta correct in saying no to a $51,000 ransom (the exchange rate for six bitcoin at the time of the attack) when experts say the costs to restore the data might well reach an estimated $17 million?

• If the situation is dire enough, CISOs always retain the option of surrendering

> "Unlike previous forms of ransomware, including SamSam and Dharma, Ryuk is extraordinarily difficult to remove. It is also very difficult to recover from."
>
> *– Joshua Motta, CEO, Coalition*

and simply paying the ransom. And yet, many companies then discover that the nature of buying cryptocurrency — the ransom of choice these days — is next-to-impossible to do in volume given the limits the system imposes on cryptocurrency brokers, especially if the company does not have existing relationships with multiple cryptocurrency brokers. Buying a lot of cryptocurrency to hold in reserve for a future ransomware attack also does not work, both because of the potential loss of value due to the dramatic shifts in cryptocurrency exchange rates and because there is no way to know which cryptocurrency will be demanded.

• The limits as to how much bitcoin a single broker can sell changes from broker to broker, as do the precise procedures. Regardless, it is critical to start establishing those relationships before an attack hits so that your team can get as much of the paperwork wrapped before you need the virtual currency, experts agree. A second option is to get ransomware insurance and let the insurance company do all of that paperwork and logistics.

• Senior executives often assert that when the time comes to deal with ransomware, they will be the ones to decide, often in concert with the board. And yet, some ransomware attacks are now designed for mid-level or entry-level employees to be able to pay on their own — with demands as low as $100 or a few hundred dollars, in cryptocurrency — so the lower-level employee can, in theory, avoid the embarrassment and potential punishment of admitting to management that they clicked on the attachment and caused the problem.

Unraveling the contradictions

A typical first line of defense includes aggressive backups, but attackers plan for that. Attackers often plant malware that goes silent for weeks or more before sending a ransom demand. This is designed to not

$34

A criminal phishing business can be run for as little as $34 per month and generate $25,000; a $3,800 monthly investment could return $1 million monthly.

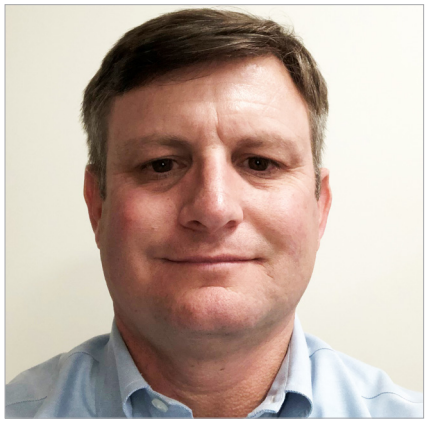
– Deloitte Black Market Ecosystem: Estimating the cost of ownership report

merely infect backups with the malware, but to make it difficult to determine exactly when the infection began. Also, even if the security team identifies the exact date of infection, it might mean restoring a backup from a month or longer ago, losing considerable critical data.

> "We don't allow our workforce to have administrative privileges on end-user devices."
>
> – Bryan Kissinger, CISO, Banner Health

This is all part of the ransomware return on investment (ROI) strategy. Attackers want the enterprise's ROI calculation to make it worthwhile to pay the ransom.

The most obvious way to combat this strategy is to separate data backups from executables backups. In theory, this would allow protection of all data, as a database of raw data should not be able to house a malware executable. But homegrown legacy applications, along with legacy apps made from companies that are no longer in business or at least no longer selling that application, make that executable backup essential. This would suggest keeping secure backups of all legacy code on disks that are entirely off-network, ideally with multiple copies in multiple air-conditioned and air-gapped vaults.



Bryan Kissinger, CISO, Banner Health

Bryan Kissinger is the CISO for Banner Health, an $8.5 billion chain of 28 hospitals along with physician groups, long-term care centers and outpatient surgery centers in six states. Kissinger argues that his security team has done everything it can think of to thwart a ransomware attack.

"We're preparing ourselves as best as we can," Kissinger says. "We don't allow our workforce to have administrative privileges on end-user devices."

That restriction on administrative privileges is a key part of Banner's defense strategy. Given that the typical ransomware attack involves attachment malware intended to compromise administrative credentials, "we attempt to head that part off. Our remedy would be to flush the system and reload it from a clean backup."

Given that Banner performs backups on everything in the network — applications, data and operating system — there is always a risk of the malware infecting the backup so "we try and go back to a good time." But by sharply limiting who has administrative privileges, Kissinger is hoping an attack would not ever touch any of the backups.

When asked about whether his firm, if indeed caught in a ransomware web, would ever pay ransom, he says he would recommend such a payment in only a few circumstances, such as if the system was "hopelessly locked and if the ransom is lower than our operating costs to repair the damage."

Kissinger adds that it is hardly practical to have an ironclad policy against ever paying such a ransom. "I think anyone who says flat out 'no' is not being realistic."

But if it ever happened, Kissinger says, his top priority would be identifying how the attacker got in and patching that hole. "We would try and close the threat vector so they can't just attack again" after the ransom is paid, he says.

The question of whether paying encourages more ransomware is a difficult one to answer, which is why most companies that pay do everything they can to keep the payments secret.

$1,200

The dark web index price for a person's full US online identify is roughly $1200. In the UK it's approximately £800.

– Top10VPN

"Broadly, I would advise 'don't pay' because I do think it encourages the problem," says Sean Tierney, director of cyber intelligence for security consulting firm Infoblox of Santa Clara, Calif. "But (CISOs) have to be aware of what the business reality is and what the impact of not paying will be. This does require the decision-makers to decide in advance what their decision will likely be."

Sean Tierney, director of cyber intelligence, Infoblox

When an enterprise is trying to craft strategies and policies to counter today's ransomware threats, it must look closely at its abilities to pay a ransom if it chose to do so. Many companies have tried and quickly discovered that the logistics of paying a large ransom in blockchain currency can be overwhelming if arrangements have not been put in place months earlier, says Mark Rasch, a former federal prosecutor who today serves as a private practice cybersecurity lawyer in Bethesda, Md.

Can I? May I? Should I?

"With ransomware, the first questions a company must address are 'Can I? May I? Should I?,'" Rasch says.

The "Can I?" part addresses the tricky nature of cryptocurrency. "Do I have access to cryptocurrency — in multiple denominations and multiple types? Anywhere from (a value of) $300 to $3 million?" Rasch asks rhetorically. "If you have a need to deploy cryptocurrency, who in the organization will be responsible for making that decision? And how do you get that information to that person?"

When an attack hits, the extortionist typically gives a very short window for paying, often 24-48 hours. That means that every minute is critical. When some employee receives an extortion demand, does that employee know where to send it? Does that employee's supervisor know? And what if the designated recipient is on vacation, traveling or otherwise unavailable? Is there a backup assigned to handle it and is that backup's contact information widely known among employees? If designated contacts and/or their backups leave the company, is there an immediate trigger for someone to select a replacement? Are such plans routinely rehearsed to learn of holes?

"Who makes that decision? Is somebody is going to own that decision?" Rasch queries. Sometimes staffers have different spending approval limits, so it becomes a question of determining which person has the authority to approve the ransom spend.

> "Broadly, I would advise 'don't pay' because I do think it encourages the problem."
>
> *– Sean Tierney, director of cyber intelligence, Infoblox*

The "May I?" part refers to the tricky legal environment surrounding ransomware. There are various regulatory rules — the most prominent coming from a unit in the U.S. Treasury called the Office of Foreign Asset and Control (OFAC) — that restricts where money can go (prohibited countries) and people/organizations where it can go (entities on suspected terrorist or terrorism organization lists).

This is where the nature of ransomware makes payments complicated. Communications between the victim company and attacker

7%

In the first quarter of 2018, the top identified malware group was Trojan-PSW. Win32. Fareit representing 7.01% of reported attacks.

– Kaspersky Lab

are anonymized through multiple layers of obfuscation software. In short, CISOs do not really know who they are about to pay ransom to and where that person is really based.

Hence, a ransom payment could easily violate OFAC rules without the CISO even realizing it. The enterprise might be making a prohibited payment unintentionally. This raises the question: Does the enterprise have any reason to suspect that this payment is going to a prohibited individual or geography? It also brings us back to the basic contradiction of pay and potentially go to jail or don't pay and lose your data.

Mark Rasch, private practice cybersecurity lawyer and former federal prosecutor

There are also U.S. Securities and Exchange Commission (SEC) implications when paying a ransom. Those are not limited to whether the amount is material, Rasch says, which is a relatively easy calculation based on the size of the company's revenue and the size of the ransom demand. A large enough ransom would demand SEC notification on its own.

> "They want to be known as a trustworthy thief. They want four stars on www.hostages-r-us.com."
>
> *– Mark Rasch, private practice cybersecurity lawyer and former federal prosecutor*

The question is whether the ransom attack means that there is a key security hole and "material" in the eyes of the SEC. Material means: "Do shareholders have a right to know this? Is it reasonably likely to move the stock price if it is disclosed?" The security hole alone might require an SEC disclosure.

Rasch also says that a company's security typically improves after a ransomware attack, which is at least a microdot of a silver lining. "You're never more secure than you are two weeks after having been attacked. It's a motivating event, at least temporarily. You're going to be doing some locking down," Rasch says. "The idea that paying ransomware invites more ransomware is probably not true. But being vulnerable to ransomware probably does invite more attacks."

Rasch argues that there really is a professionalism among many of the larger ransomware groups and punishing a paying customer is rarely seen. "In the incidents where I have dealt with ransomware, we haven't had the experience that they immediately get hit again," Rasch says, adding that not delivering a paid-for decryption tool is something else that rarely if ever happens.

"They don't make money if you can't unlock it," Rasch says. "They want to be known as a trustworthy thief. They want four stars on www.hostages-r-us.com."

The final consideration, the "Should I," essentially addresses the aforementioned discussion on comparing the ROI of paying the ransom versus not paying it. The CISO calculates what it will cost the company to try and repair the damage itself—factoring in down-time, status of backups, how long ago the system was impacted—versus paying the ransom. It may be galling, but a hard calculation will inform the "Should I?" decision. It also overlaps with the May I factor when it comes to the legality of paying, plus addresses a host of business and ethical considerations unique to each company.

Legal beagles

On other legal matters, there are the compliance issues dealing with states and

2019

The Android platform is expected to reach #2 ranking behind Windows as the most popular attack platform in 2019.

– DuoCircle

other rules requiring disclosures, and possibly consumer insurance purchases, when Social Security numbers or other specified personally identifiable information (PII) is stolen. Given that even a forensic examination does not always deliver a complete and definitive picture of what attackers did (especially given the ever-present possibility that the bad guys manipulated security logs to hide their true tracks), it is hard to know if data was stolen (copied and exfiltrated) before it was encrypted.

> "If you can, see what the malicious code was intended to do."
>
> – Tatiana Melnik, attorney

As with almost everything in compliance, each rule depends on its definitions and phrasing. "One of the triggers is unauthorized access," says Tatiana Melnik, a Tampa-based attorney who specializes in cyber issues. "At the same time, there is a requirement under HIPAA (Health Insurance Portability and Accountability Act) that requires integrity of the data remains in place. If someone has encrypted the data, does integrity of the data remain in place?"

Tatiana Melnik, attorney

The answer is to do everything your company can to determine what happened. "If you can, see what the malicious code was intended to do. If it was merely designed to find information and encrypt it, arguably, it may not be a breach," Melnik says—and then make that argument to regulators and hope for the best.

Dante Disparte, CEO at the Washington, DC-based security consulting firm Risk Cooperative and a member of the national advisory council for the Federal Emergency Management Agency, says the prevailing view is that if the company investigates and "if there's no determination of exfiltration," then no reporting is necessary. He also argues that this approach is "what makes sense from a public policy point of view. [If every ransomware required full reporting] what it would produce is just to create a lot more noise. Everyone would get a notice every five seconds from every provider they work with."

As far as HIPAA is concerned, the U.S. Department of Health and Human Services (HHS) has issued guidelines on ransomware and HIPAA and, not surprisingly, it leans toward reporting.

"Unless the covered entity or business associate can demonstrate that there is a 'low probability that the PHI (personal health information) has been compromised,' based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred," the HHS guideline says. "The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media for breaches affecting over 500 individuals, in accordance with HIPAA breach notification requirements."

But how well do professional ransomware extortionists cover their tracks? According to consulting firm Deloitte, quite well.

"Many of the most popular BPH (bullet-proof host) services offer dedicated 'fast-flux' capabilities where nameservers and proxy front-end exit nodes are rapidly changed. These setups are extraordinarily resilient and may include load balancers and proxies as well," Deloitte wrote in a December 2018

>4000

More than 4000 ransomware attacks occur daily with an average demand of $1,077.

– DuoCircle

report entitled *Black Market Ecosystem: Estimating the cost of ownership*. "If either a nameserver or front-end is blocked or taken offline, a new one is automatically created in its place, allowing the back-end server hosting the criminal customers' content to remain online."

Deloitte noted that companies are quite open, on the dark web, at least, about the software suites they sell specifically for ransomware attacks, including whether fees are flat or involve a percentage of ransom acquired.

There is an advantage that the larger ransomware companies are so well known. That means that their tactics are well known. Companies, such as cyber insurance firms, often can identify the company attacking by looking at the code used. "Is it a variant of some known code? Has it been used before?" Rasch says.

Sometimes, attackers reuse their decryption tools and even decryption keys, which creates the slight possibility that victims can find the decryption items online from a recent victim of the attack rather than from the attacker.

Another concern is about the attacker-provided decryption tool. Not whether it will work necessarily, but how well it will work.

"In the last three months we've seen the Ryuk strain of ransomware become very active. It is the fast growing ransomware strain we see," says Joshua Motta, CEO of San Francisco-based Coalition, a cyber insurance company. "More worrisome is that the ransoms for Ryuk are much larger than other strains of ransomware, totaling between $200K to $700K."

Model	**Affiliate Programs**				**Builds & Source Code**		
Actor	**GrandCrab**	**Spora**	**Shark Atom Satan**	**Rapid**	**Philadelphia**	**Trojans**	**InTheMood Cryptolocker**
Pricing	60/40 profit share. Major partners get an opportunity to increase their share up to 70 percent.	Fixed rate 70/30	Percentage of ransom (20-30%)	75/25 profit share	Lifetime license + fee updates and full support! Introductory price: $389 Discounted price of US $320 Stampado Ransom-ware — Cheapest - only $39 lifetime license	Price: US $650 per copy	Price: $1500 USD
Average license cost (est.)	N/A — Restricted Affiliate Program with profit sharing model	N/A — Restricted Affiliate Program with profit sharing model	N/A — Open Affiliate Program with profit sharing model	N/A — Restricted Affiliate Program with profit sharing model	$21	$54	$125

Source: Deloitte Black-market ecosystem | Malware and tools

This graphic illustrates a dark web page with ransomware for sale. Ransomware become a commodity, often sold the same way as packaged software with support and a license. According to Deloitte, "This enables [ransomware sellers] to provide a malicious 'suite' of services in conjunction with ransomware, known as Ransomware as a Service (RaaS)." *note - monthly costs for ransomware builds distributed over 12 months

14 sec

In 2019 a new organization will fall victim to a ransomware attack every 14 seconds, increasing to every 11 seconds by 2021

– Cybersecurity Ventures

He adds that "Unlike previous forms of ransomware, including SamSam and Dharma, Ryuk is extraordinarily difficult to remove. It is also very difficult to recover from. Even if you pay the ransom, the decryptor provided by the threat actor doesn't work well. It does decrypt files, but it frequently fails making recovering extraordinarily time consuming for the victim."

Scott Laliberte, managing director and global leader of cybersecurity and privacy for consulting firm Protiviti of Menlo Park, Calif., argues that ransomware is likely to get a lot worse before it, actually, it will just continue to get worse.

"My thoughts are that we are going to see escalation in ransomware over the next few years. I think the payload will start moving beyond just denying access to data to other types of actions that could threaten harm. For example, attacking healthcare providers to put patient lives in danger unless ransom is paid, distribution companies' logistics systems to prevent them from making shipments, chemical plants, threatening catastrophic accidents, etc.," Laliberte says.

Cybercriminals will "look for ways to monetize their attacks [given that] credit report monitoring and credit card tokenization [is making] identity theft and credit card fraud less profitable. Consequently, I believe [cyberthieves] will be upping the stakes. We need to start preparing now for these types of attacks and expanding our view of risk assessment beyond loss of confidential data."

Laliberte says he expects IoT and mobile will be ransomware's new focus in the near term. ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

53%

More than half of all reported malicious emails were tied to credential phishing.

– Cofense