

To pay or not to pay

Confronting cyber extortionists



Table of contents

Rapidly changing threats to the enterprise	2
Ransomware: A game of chess	2
“Don’t pay!”	2
Growing threat	3
The ransomware choice	4
Customizing the amount	5
Payment conundrum	6
Decryption uncertainties	7
Recurring attacks	8
Refusing to pay	9
Data theft	11
Ransomware: Not insurmountable	13

Rapidly changing threats to the enterprise

Today’s enterprise is more vulnerable than ever before. The traditional boundaries of the enterprise are changing, with technologies such as cloud, analytics and mobility now widely integrated across operations and partner and supplier networks. Attacks come more frequently, driven by increasingly agile, well-funded, collaborative groups of cyber criminals who are constantly changing their mode of attack to stay ahead of security specialists. To operate in this rapidly changing environment, organizations must proactively secure every facet of the enterprise and look beyond the horizon for emerging threats — such as ransomware attacks.

Ransomware: A game of chess

Ransomware is serious, damaging business. It is also like a game of chess: Enterprises must plan their strategy and make the best moves. Because there is no “right” answer, this paper outlines steps enterprises can take and what trade-offs they should assess when deciding whether or not to pay a ransomware demand.

“Don’t pay!”

You’ve heard this many times.

Industry bodies and law enforcement scream the party line at the top of their lungs: “We do not negotiate with kidnappers; it invites endless abductions.”

But while the question of whether to pay extortionists or not sounds binary, nuances exist.

Because they are determined to adhere to a hard-line position of nonpayment, industry bodies have not provided comprehensive advice to enterprises about what to expect when dealing with extortionists. Thus, executives have no guidance to prepare them for a crisis situation, where often only hours separate their organization from catastrophic business and brand damage.

DXC Technology can help you understand the full spectrum of options, how interactions with extortionists may evolve and how to position your enterprise to withstand such attacks.

Growing threat

Ransomware is a pernicious and endemic threat to enterprises.

In 2016, ransomware attacks increased by orders of magnitude, and there is little expectation that the current level of activity will diminish in the near future.¹ Half of the UK companies surveyed in a 2016 study had suffered ransomware attacks.² Analysts estimate that more than a billion dollars were paid in ransoms in 2016.³ In 2017, one organization alone estimated that the Petya ransomware attack resulted in \$200 million to \$300 million in losses for the company.⁴

Ransomware is the harbinger of a wider extortion threat, the embers of which are spread by the criminal fraternity.

Medical companies have suffered extortion attempts under threat of their stolen patient records being dumped online.⁵ Netflix was subjected to an extortion attempt after unreleased episodes of its series “Orange Is the New Black” were stolen from an associated postproduction studio and leaked online; the studio itself had already been extorted for \$50,000.⁶ Cybercriminals also attempted to extort media company HBO for a reported \$6 million;⁷ as a result of nonpayment, the attackers posted online the data they stole and an unreleased episode of “Game of Thrones.”

Cybercriminals attempted to extort Disney, claiming to have a copy of its unreleased movie, “Pirates of the Caribbean.” Despite the fact that Disney did not pay the ransom, the film was never leaked. It seems the attackers were bluffing. That said, fear is making organizations susceptible to extortion, and ransomware attacks are trending up.

In one survey, 70 percent of executives confessed to paying ransoms.⁸ Criminals are using their ransom proceeds to innovate, introducing new virility into their business models.

In the following pages, we outline steps that enterprises (and extortionists) can take at each stage of the extortion process. These steps inform executives about what they should assess in order to decide whether to pay or not pay.

-
- 1 2017 SonicWall Annual Threat Report, <https://www.sonicwall.com/en-us/lp/2017-sonicwall-annual-threat-report>
 - 2 “The Rise of Ransomware,” Ponemon Institute study sponsored by Carbonite, January 2017. <http://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf>
 - 3 “Ransomware took in \$1 billion in 2016 — improved defenses may not be enough to stem the tide,” CSO, January 5, 2017. <http://www.csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html>
 - 4 “Interim Report Q2 2017,” Maersk, August 16, 2017, <http://investor.maersk.com/releasedetail.cfm?ReleaseID=1037421>. “Global Shipping Giant Maersk Is Reeling from the Ransomware Fallout,” *Fortune*, June 29, 2017, <http://fortune.com/2017/06/29/petya-goldeneye-maersk-ransomware-effects/>.
 - 5 “How The Dark Overlord is costing U.S. clinics big time with ransom demands,” McClatchy DC Bureau, May 15, 2017. <http://www.mcclatchydc.com/news/nation-world/national/national-security/article150678617.html>
 - 6 “How Hollywood Got Hacked: Studio at Center of Netflix Leak Breaks Silence,” *Variety*, June 20, 2017. <http://variety.com/2017/digital/features/netflix-orange-is-the-new-black-leak-dark-overlord-larson-studios-1202471400/>
 - 7 “HBO offered \$250,000 to hackers in bid to delay data release,” *Reuters*, August 11, 2017. <https://www.reuters.com/article/us-cyber-hbo-idUSKBN1AR16M>
 - 8 IBM Infographic, “If the price is right, ransomware wins,” 2016. https://www.flickr.com/photos/ibm_media/30819897523/

The ransomware choice

When the extortion demand arrives, you have a choice. You will probably have only hours to make it.


The decision you make will have repercussions for your enterprise, which could suffer significant financial and reputational damage, and your clients, who may face a range of negative consequences.

Say you are a medical director whose backups and original files have been encrypted by extortionists. Without that data, patient care could be compromised. Lives could be threatened.

Or you could be a struggling manufacturer whose entire factory floor is dependent on industrial equipment that is now incapacitated because ransomware is affecting the control computers. It may be that the equipment is so old that no one knows how to rebuild the controllers. Without them, the production line grinds to a halt. The business goes under, with hundreds of jobs lost.

To pay or not to pay is a genuine dilemma. There is no “right” answer in such a predicament.

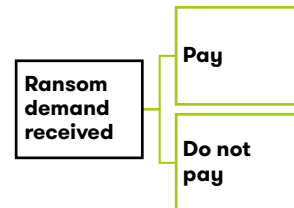
While the executive is confronted with what looks like a binary choice — to pay or not to pay — there are many variables involved in each choice.



This is chess rather than checkers, played out on a semiobscured board against a hidden adversary.

Customizing the amount

The ransom demand itself is often reasonable relative to the victim's means.



In most global extortion campaigns, such as Locky, the ransom is typically around \$300. However, in roughly 40 percent of cases, ransomware affects more than one machine;⁹ should several thousand endpoints be compromised, it can become an expensive proposition to capitulate.

Cybercriminals are increasingly customizing their ransom demands based on the assessed resources of the victim. For example, the Fatboy Ransomware-as-a-Service calculates the amount it extorts based on *The Economist's* Big Mac index,¹⁰ a model used to calculate global exchange rates. The intent is to align the extortion amount with the victim's means, resulting in an improved chance of payment.

Higher ransoms are being targeted at large enterprises, as they can afford more than individuals and often hold valuable and sensitive information. In June 2017, online hosting firm Nayana Communications was subjected to a \$1 million extortion after its systems and backups, containing its clients' websites and customer databases, were encrypted by cybercriminals.¹¹ We are likely to see many more of these tailored ransom demands in the future.

Negotiating

History shows that often, cybercriminals negotiate with their victims. For instance, the Nayana CEO was able to achieve a reduction from an initial demand of \$1.6 million to the eventual \$1 million paid.¹²

In another example, discounts and deadline extensions were granted by four separate cybercriminals when a researcher contacted them posing as a victim.¹³

If you do decide to pay, haggling is an option.

⁹ "Understanding the Depth of the Global Ransomware Problem," Osterman Research sponsored by Malwarebytes, August 2016. <https://www.malwarebytes.com/surveys/ransomware/?allid=13242065>

¹⁰ "The Big Mac index," *The Economist*, July 13, 2017. <http://www.economist.com/content/big-mac-index/>

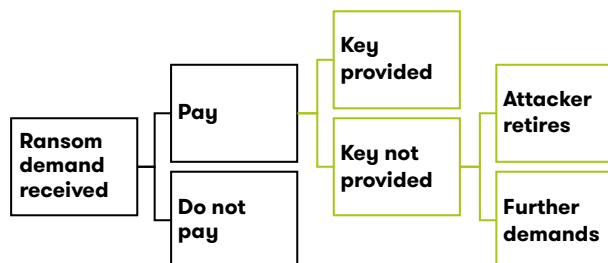
¹¹ Nayana Customer Center. http://www.nayana.com/bbs/set_view.php?b_name=notice&w_no=969

¹² Ibid.

¹³ "Evaluating the Customer Journey of Crypto-Ransomware and the Paradox Behind It," F-Secure, 2016. https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf

Payment conundrum

If you do decide to pay, there is no guarantee that you will get your data back.



The ransomware business model is underwritten by a sense of trust between the victim and extortionist. If the ransom is significantly lower than the business cost of recovering without paying the attackers, and the victim is confident that acquiescing will result in file restoration, there is an economic argument to pay.

At a global level, it is in the interest of the attackers to decrypt their victim's files. If trust in the model is eroded, the calculation for the victim will change and payments will cease, as the victim deduces that its capitulation is not likely to result in data restoration.

For most large ransomware campaigns such as Locky, which are likely operated by organized criminals or "professional adversaries," as they have sometimes called themselves, a reasonable chance exists that the attackers will honor the model by providing the decryption keys, thereby preserving the trust that will encourage future victims to pay. A recent study found that 55 percent of attackers provided functioning decryption keys after being paid.¹⁴

However, it is also possible that the attackers will not honor this model. It could be that they are not committed to sustaining the trust, as they are focused on quick wins rather than sustainable profits.

An additional consideration is that ransomware attacks can act as plausible cover for destructive "wiper" attacks. In such attacks, it is not possible to recover files even if the ransom is paid.

Further demands

It is also possible, once the extortionists know a company is willing to pay, that they may decide to find out just how much they can extort from that company by issuing continuing and escalating demands.

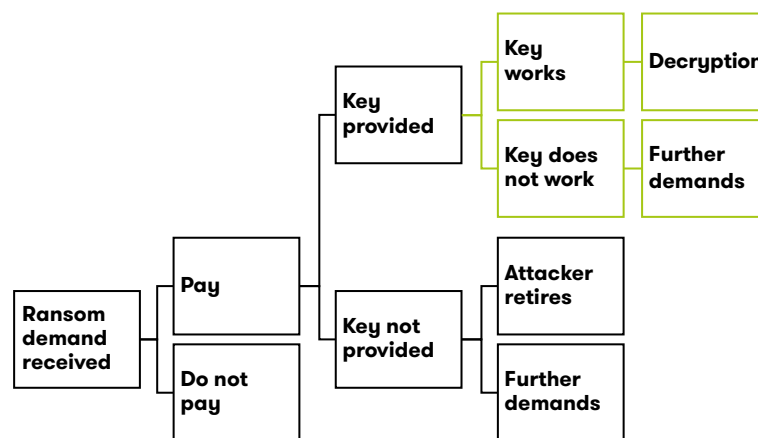
Kansas City Hospital faced such a scenario in mid-2016 when it paid a ransom, only to be contacted with an increased demand in order for the attackers to decrypt the files; the hospital chose not to pay a second time.¹⁵

¹⁴ "The Rise of Ransomware," Ponemon Institute study sponsored by Carbonite, January 2017.
<http://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf>

¹⁵ Hospital pays ransomware, but doesn't get files decrypted," ExtremeTech, May 25, 2016.
<https://www.extremetech.com/extreme/229162-hospital-pays-ransomware-but-doesnt-get-files-decrypted>

Decryption uncertainties

Even if you reach an agreement with the attackers and they send you a decryption key, there is no guarantee the key will work. Writing cryptographic procedures is complicated. Even when drawing on standard programming libraries, implementation is a challenge, with myriad errors possible. If this were a drug operation, the ransomware author would be the equivalent of a highly trained chemist. But sometimes the narcotics are “cooked” incorrectly, often proving fatal for the addict; the same can be said of ransomware, with the victim’s data being the casualty.



Typically, more time is dedicated to creating the encryption — rather than the decryption — algorithms, as there is no profit in the latter. The ransom will have already been paid (although one could argue that to preserve the trust model, there is long-term profit).

Another scenario is when further components of the payment infrastructure do not work correctly. This was the case with UltraCrypter. Despite payment having been made, the decryption keys were never issued, as the attacker had not configured the infrastructure correctly to recognize payment and automatically provide the keys.¹⁶ External factors, such as law enforcement actions, could also shut down the attacker’s command-and-control infrastructure, meaning that payment would not result in decryption of the victim’s files.

Knowing that their business is threatened by ransomware decryption keys that do not work, criminals have emulated the commercial sector by offering a “try before you buy” feature.

For example, the Spora ransomware offers the option of decrypting two files at no charge.¹⁷ This allows the attacker to build trust with the victim and, the attacker hopes, with evidence of decryption capabilities, galvanize payment of the ransom.

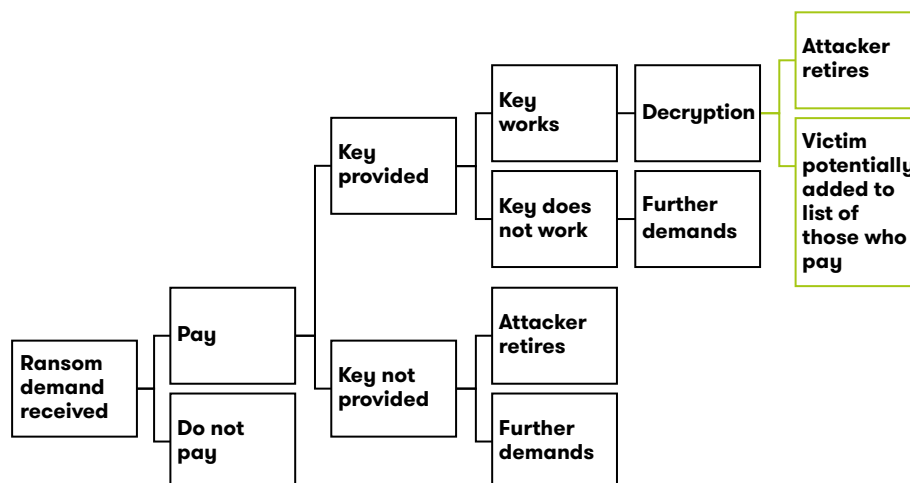
¹⁶ “UltraCrypter not providing Decryption Keys after payment. Launches Help Desk,” BleepingComputer, June 6, 2016. <https://www.bleepingcomputer.com/news/security/ultracrypter-not-providing-decryption-keys-after-payment-launches-help-desk/>

¹⁷ “Spora ransomware goes freemium with four different payment options,” Naked Security, January 16, 2017. <https://nakedsecurity.sophos.com/2017/01/16/spora-ransomware-goes-freemium-with-four-different-payment-options/>

Recurring attacks

Even when attackers cease their activities following payment and decryption, that may not be the end of the problem.

Following a successful extortion, some criminals may retire; however, the victim's payment may instigate further consequences. Your enterprise will have declared that you are willing to pay ransoms. As in kidnapping, once the attackers know you will pay, they are incited to take further hostages.



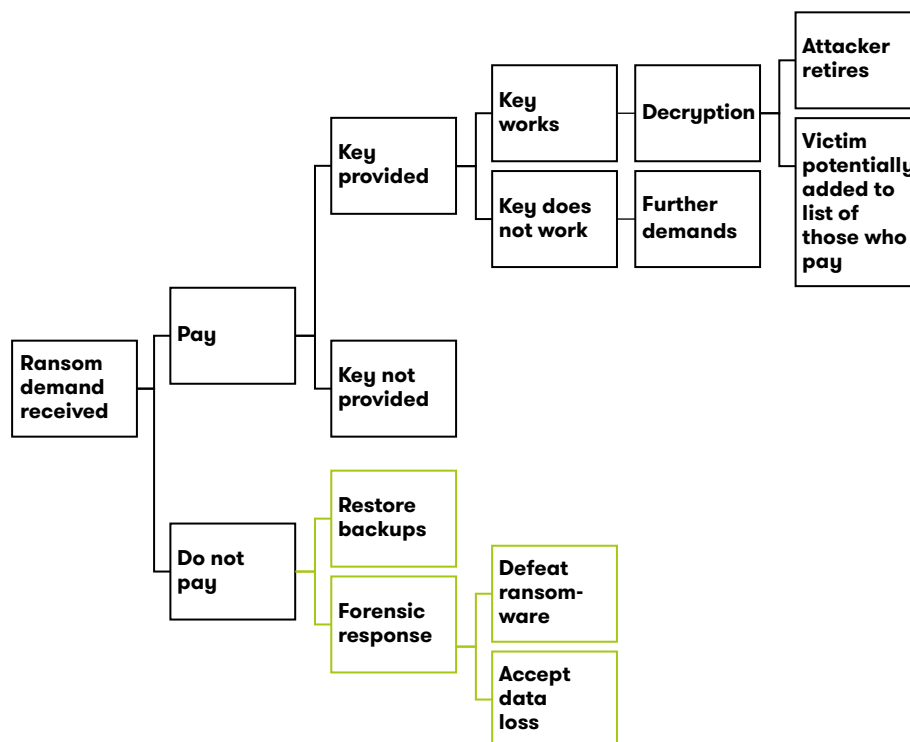
Insight into the criminal underworld is limited; however, it is likely that if attackers are able to monetize their knowledge of who will pay by selling such information on the dark web, they will sell it.

Or they may just attack the victim again themselves. It may not happen immediately, but there is a good chance the enterprise will be targeted again, and with the payment precedent set, the extortion may be much higher.

It is also possible that you can get lucky. You might have found one of the few criminals who keeps his or her word; however, do not count on it.

Refusing to pay

Not paying leaves two options: restoring backups or conducting a forensic response.



In an ideal world, your enterprise will have a robust backup process that is continually generating fresh copies of your data, providing business continuity against physical and cyberdisasters. In the event of an attack, the hope is that these backups will be only hours old — one day at most — and will have been continually tested. If the option is available, restoring from backups is the optimum solution (after not being compromised at all, of course).

However, DXC's incident response teams have been called in to help organizations recover from ransomware only to find backups that are out of date or not functional. *It is absolutely vital to ensure rigorous and regular testing of backups.*

A forensic response entails analyzing a compromised machine and, if available, the ransomware itself. The primary objective is to identify a way of either recovering the data from the machine, in hopes that the encryption has not been correctly executed, or identifying a flaw in the implementation of the encryption algorithm in the malware itself, allowing a reversal of the procedure.

This can be a lengthy exercise, though. If you have only hours, or at best days, to decide between paying the ransom or forever losing your data, a forensic response is highly unlikely to yield success if a robust encryption process has been implemented by the attacker.

The No More Ransom project is a group of experts from academia, law enforcement and industry who have come together to try to reduce the scourge of ransomware. The alliance's website hosts the best collection of decryption capabilities available and is a resource you should employ in any forensic response.

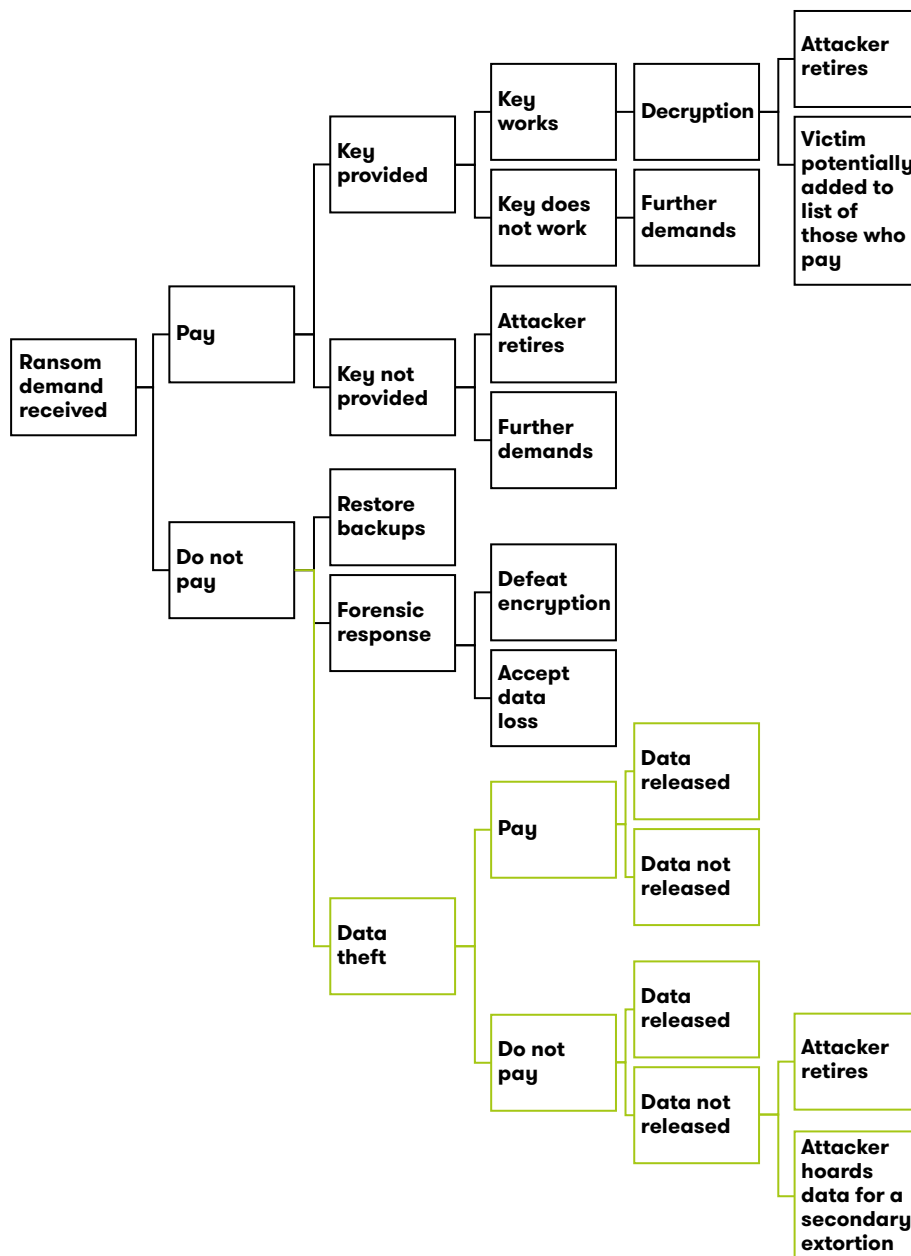
Without a decryption capability, it is unlikely that a forensic practitioner could develop one within the attacker's response window.

Your last option is to accept the data loss and implement preventive measures to significantly reduce the probability of a successful future attack on your enterprise.

Without a decryption capability, it is unlikely that a forensic practitioner could develop one within the attacker's response window.

Data theft

Anticipating that restoring backups is the standard ransomware countermeasure, attackers are innovating.



Before encrypting data, extortionists have started to exfiltrate data located on their victims' machines. Ransomware such as DynA-Crypt steals files from Skype, Firefox and Chrome,¹⁸ likely enabling further monetization of each victim compromised.

¹⁸ "DynA-Crypt Not Only Encrypts Your Files, But Also Steals Your Info," BleepingComputer, February 9, 2017. <https://www.bleepingcomputer.com/news/security/dyna-crypt-not-only-encrypts-your-files-but-also-steals-your-info/>

A recent study found that in 55 percent of cases, victims were either certain, or judged it likely, that data had been stolen before the ransomware encrypted their files.¹⁹ This trend will increase as criminals refine their business models to ensure continuing growth even as enterprises modernize and secure their backup and restore processes. Stolen data is used as a secondary mechanism to extort victims with the threat of data release. Even if paid, there is no guarantee that the attackers will refrain from releasing the data or from attempting subsequent extortions.

The media as a weapon

Attackers are also starting to use the media as a weapon in the extortion attack model.

One hacking entity known as “The Dark Overlord” has stolen data absent any form of ransomware. The attacker first tries to extort the victim in private with the threat of data release. If the victim does not pay, the attacker leaks a sample of the stolen data online and develops a narrative aimed at the media and the victim’s clients, saying that the victim does not care about the clients’ data being exposed. This leaves the victim in an even more precarious situation. If the victim capitulates to extortionists, this invites more attacks. If the victim does not capitulate, the company could suffer substantial brand damage.

¹⁹ “The Rise of Ransomware,” Ponemon Institute study sponsored by Carbonite, January 2017.
<http://www.ponemon.org/local/upload/file/Ransomware%20Report%20Final%201.pdf>

Your trusted security partner

DXC Technology, one of the world's leading IT and security services providers, has more than 4,000 security specialists who advise, transform and manage leading-edge security capabilities.

Our network of global, intelligent Security Operations Centers (SOCs) enables us to deliver end-to-end security management and monitoring capabilities, 24x7x365, anywhere in the world. Sharing threat intelligence across multiple technology bases increases our ability to defend enterprises against risk.

We correlate billions of security events and manage more than 1.8 million security-specific devices globally, along with another 8 million end user and server devices worldwide.

**Learn more at
[www.dxc.technology/
ransomwarediagnostic](http://www.dxc.technology/ransomwarediagnostic)**

Ransomware: Not insurmountable

The decision to pay or not pay a ransomware demand — and the resulting risk from that decision — sits squarely with individual enterprises. Executives must make a decision based on individual variables such as the criticality and sensitivity of their data, and the consequences of loss of such data, which could include financial and brand damage, job losses and, in some cases, a potential compromise of safety.

If executives decide to pay, it should be remembered that payment will not necessarily result in decryption of the data; capitulating holds its own risks. Executives should also consider the ethical dimension; it is unknown what criminal activities may be fueled by a ransom payment.

If executives do pay, their enterprises must also embark on an immediate and urgent security improvement plan. The improvement plan must prepare the enterprise to repel future attacks that the payment may have induced, as well as other cyber incidents the enterprise may be a target for in the contemporary threat arena.

Enterprises need to be able to not only withstand ransomware attacks, but also assess whether any data has been stolen from their organization by attackers who may seek to extort the enterprise with threats of data dumps. It is vital to be able to assess whether the criminals are bluffing in order to make a decision on payment.

Ultimately, ransomware is not an insurmountable problem. For example, WannaCry could have been mitigated with an optimized patching cycle. User education can drastically limit the attack surface. Basic hygiene such as antiphishing education — often not prioritized or audited, unfortunately — could reduce much of the risk.

However, doing the basics well solves only part of the challenge. Enterprises need defense-in-depth to combat ransomware and the full threat spectrum. This requires a long-term strategy complemented with highly specialized practitioners for implementation.

DXC is an expert in protecting businesses from the most advanced threats, enabling you to thrive in the digital era. We stand ready to assist you in accelerating your security transformation journey.

About DXC Technology

DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner network combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.