Conversational
Ransomware Defense and Survival

A ConversationalGeek® Book

Sponsored by VEEAM

Learn about:

- Scoping the impact and intricacies of ransomware
- Effectively fighting ransomware with resilience and Hyper-Availability
- Quickly responding to, and recovering from, ransomware attacks

2nd Edition updated for 2018

By Orlando Scott-Cowley (Cybersecurity Consultant. CISSP, CCSP, CCSK)

Sponsored by Veeam

Veeam is the leader in Intelligent Data Management for the Hyper-Available enterprise. Veeam Hyper-Availability Platform is the most complete solution to help customers on the journey to Intelligent Data Management in a world that demands the Hyper-Availability of data.

Veeam supports more than 282,000 customers worldwide, including 74% of the Fortune 500 and 57% of the Global 2000. Their customer satisfaction scores, at 2.5X the industry average, are the highest in the industry. Their global ecosystem includes 55,000 channel partners; Cisco, HPE, and NetApp as exclusive resellers; and nearly 18,000 cloud and service providers. Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries.

To learn more, visit

https://www.veeam.com

or follow Veeam on Twitter

@veeam

Conversational
Ransomware Defense and Survival

by Orlando Scott-Cowley

ConversationalGeek

Conversational Ransomware Defense and Survival

Published by Conversational Geek Inc.
www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Orlando Scott-Cowley
Project/Copy Editor:	Steven Zimmerman
Content Reviewer(s):	J. Peter Bruzzese

Note from the Author

I've called ransomware the "threat-du-jour" before now; unfortunately, ransomware still proves to be a useful tool for earning money. There are hints that malicious cryptocurrency mining is slowly taking over but, for the foreseeable future, ransomware is here to stay. IT departments, CISOs, and CIOs feel like they're stuck in a giant revolving door that rotates between states of secure and insecure within their environments. Ransomware threatens organizations as it comes rolling down their internet connection, causing that door to spin so fast everything becomes a sickening blur.

In this updated edition of Conversational Ransomware Defense and Survival, I'll examine some of the new tactics cybercriminals are using, as well as the better ways of protecting yourself, your business, and your users.

It's hardly surprising that ransomware has become so ubiquitous and successful because of its impressive ability to evolve. It sneaks past existing defenses like secure email gateways and desktop anti-virus with ease. Then, through the clever use of social engineering, tricks users into running its viral payload. All of this compounded by end users facing other threats such as phishing, vishing, whaling (or business email compromise), plain old spam, malware, and internet-villainy. Just when we thought we'd escaped the latest in that long list of threats, along comes ransomware to test our preparedness, to the max.

If this sounds familiar, you're not alone. There are lots of euphemisms the security industry uses to describe this process. The most common is "arms race," but you'll also hear "red queen effect," "hamster wheel," or just a lot of muttering, swearing, and cursing. The frustration of those affected by these problems is palpable. Most are now looking at a broader

cross section of technologies to protect themselves and, importantly, to recover after an attack, rather than rely on pure-play security solutions alone.

I've been helping organizations protect themselves from a variety of security threats for many years now, and have seen these tactical pivots by hackers and cybercriminals over and over again. Sadly, all we can do is learn to adapt our protections, stay agile and make sure we don't just sit back and hope for the best.

This book gives you a little insight into the ransomware threat, without being too complicated and technical. It'll help you understand ransomware and what to do to protect yourself and your organization.

Stay safe out there.

Orlando Scott-Cowley
CISSP, CCSP, CCSK

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

The Rise of Malware for Extortion

Ransomware is common enough now that you can't help but to have heard of it. As far as enterprise IT goes, it is probably one of the top three things they worry about, and could well be the cause of "that phone call" that changes everything in an instant – *you know the one that I mean*.

Ransomware resilience, recovery, and availability has become a key part of IT contingency planning. You have planned for it haven't you? If not, you have my condolences and I hope your backup regime was thorough enough that you're able to recover from the attack.

For those who have yet to be affected by ransomware but are keen to learn more about the threat, how to protect yourself from it, and to recover once attacked, this book is for you.

Where did the threat originate?

Ransomware is said to be "invented" by the mysterious-sounding Dr. J.L. Popp back in 1989. Dr. Popp was in fact an evolutionary biologist who thought he would increase his notoriety at the World Health Organization Aids conference in that year, by distributing malware infected diskettes to delegates in the hope they'd stump up $189 to have their computer repaired.

You may have heard ransomware described in different ways too. Locker or crypto-malware are also common names for the same threat.

Ransomware is a type of malware, or computer virus, and is designed to extort money from its victims by either locking their computer to make it inaccessible or, more commonly, encrypting some or all of the files. The perpetrating cybercriminals and hackers send the ransomware in hopes that victims will pay the ransom in order to get their data back. *More on that later.* You will usually be infected by ransomware through a malicious email attachment, though attackers may use other tricks like malvertising and social engineering.

Today, ransomware is mostly driven through ransomware-as-a-service platforms run by organized cyber criminals. They have become so skilled at extorting money from victims that they even set up legitimate-sounding "customer service centers" to make it easier for victims to pay the ransom. The average ransomware attack campaign can net criminals millions of dollars at little expense or with little risk of being caught.

Over the past few years, we've seen a gradual decline in the volume of attacks, indicating a slight move away from the "mass mailer" attacks of 2014-2017 using Cerber and Locky variants. The bad news, however, is that ransomware is become much more targeted, and cybercriminals are tailoring their attacks to specific industries and organizations with custom malware.

Ransomware Is a Clever Little Beastie

So how does it work?

Ransomware has become the poster child for successful malware everywhere, not only because it's so effective at what it does, but also because it's the model of agile, rapid development by the cybercriminals who write it.

To give you an example, a popular piece of ransomware from 2015 called CryptoWall 2.0 was redeveloped from a completely new code base to CryptoWall 3.0 in as little as 48 hours after the former was effectively hobbled by the security community. The same malware was said to have earned its owners around $350 Million, as reported by Dark Reading. Ask yourself how many enterprises you know with that sort of budget and R&D capability and you'll quickly see how significant this threat is to the majority of us.

Ransomware has always been about extortion. Even the earliest versions were designed to trick you into paying money for some sort of fix to your computer. Early ransomware used a "locker" technology to simply deny you access to your computer, often pretending to be delivered from a law enforcement agency such as the FBI. Again, payment was demanded to allow the victim access to their computer. At this stage, ransomware didn't encrypt files like is does today.

Early versions of file-encrypting ransomware used relatively simple encryption compared to today's standards. Sometimes the private keys for decryption were easily discovered or weaker symmetric encryption was used, making reverse

engineering easier. CryptoTorLocker (2015) for example was a variant that hid its decryption key in the malware executable.

In other cases, the security community has managed to develop decryption tools due to poor implementations of file encryption. By 2013, encryption standards had moved on to the much meatier 256 bit AES with 2048 bit RSA keys.

The key to the success of ransomware is its reliance on the human element of computing, by which I mean the fallibility of the person between the chair and the keyboard (PBCAK if you will). Take, for example, many of the ransomware attacks delivered by email:

The email encourages the reader to open the file. Usually, as soon as it happens, the ransomware is working away in the background quietly encrypting all the data in the victim's computer. Alarmingly, this often happens once the email has been cleared by the usual gateway and desktop anti-virus applications.

Once the malware has been activated, it's often too late.

How does this happen?

Well, the avoidance of classic anti-virus technology is such an important note, that I've dedicated a whole section to it later.

Victims will only realize they've been infected when the warning pops up on their screen. These warnings vary depending on the ransomware used, but will generally tell you all your files have been encrypted and you must pay to get them back.

Ransomware doesn't just spread by email though. Social media is an important hunting ground for the threat too; the

direct messaging systems are abused by attackers who will rely on link shortening services to hide their malware-laden website from unsuspecting victims.

Malvertising has also been used to deliver ransomware attacks. Attackers compromise a legitimate online ad network and use it to trick browsers into downloading their malicious payload—usually an exploit kit which then deploys ransomware to the victim. These are commonly known as drive-by and watering hole attacks.

In an enterprise's networked environment, ransomware can be even more insidious as it will use the Windows networking SMB shares to propagate around the network, infecting other computers as it goes. This is why we see entire networks taken offline during ransomware attacks, as the threat loves the inherent trust built into our LAN infrastructure.

Some variants will even encrypt mapped and unmapped network drives as well as connected cloud services like Dropbox, OneDrive, and Box.

Scoping the Impact of Ransomware

The blast radius of a ransomware attack can be significant if the initial outbreak is not well contained. The media is full of war stories about ransomware, two great examples stand out of late. Not because of how bad the impact was (and it was bad), but how much we've learned from the attacks themselves and how much analysis there has been on them.

You can't help but to have noticed the WannaCry attack in the spring of 2017. The WannaCry ransomware is said to have affected 200,000 computers across 150 countries, with the worst affected in Russia, Ukraine, India, and Taiwan. In the UK, the National Health Service (NHS) was severely impacted, with

hospitals having to revert to paper records and cancel all but non-essential services. Nissan UK and Renault stopped their production lines temporarily to try and thwart the attack. Telefonica, FedEx, and Deutsche Bahn were among other organizations to be affected. The global losses as a result of WannaCry are estimated at $4 Billion.

More recently, the City of Atlanta was hit by the SamSam ransomware. The ransom was ‘‘only” around $50,000 worth of bitcoin, but the impact on the city’s finances has been shown to be much more. Their emergency preparedness expenditure in the period after the attack was close to $2.7 Million, which covered the incident response, forensic analysis, additional staffing, and vendor support. To date, we still don’t know if the city paid the ransom demand.

The City of Atlanta’s remediation bill is a great example of how the cost to fix and recover from these types of attacks can easily run into seven figures and two commas, even for a relatively small ransom demand. Taking these sorts of numbers to your own IT teams, executives, and board members is an excellent idea since they’re real examples of what this problem can cost you.

Ignoring serious examples should only be done if you’ve updated your résumé recently.

Hit by Ransomware? Get out Your Checkbook

Ransomware can affect you in many ways, but all are likely to cost you money unless your preparedness efforts are top notch.

It’s likely the attackers will want a payment of cryptocurrency, like Bitcoin. Note, the attackers aren’t greedy here. They’re

reliant on the volume of successful ransomware attacks to generate an income rather than individual attacks. Their price point reflects a price which people will be prepared, or convinced, to pay to get their data back.

ZDnet asserts that about 20% of enterprises succumb to these demands. Make the ransom too expensive and people will simply find a cheaper way of recovering data. Anonymous cryptocurrencies have been cited as a contributor to the success of ransomware, allowing for the effective collection of money with no paper trail; sending a check or PayPal credit isn't something cybercriminals are too keen on, for obvious reasons.

Should you pay? No.
I'll tell you why shortly.

It's also not just the cost of recovering from the individual ransomware infections you need to consider. If there's a wider network outage due to an outbreak, your business could be losing revenue from lost productivity. There could also be costs associated with a damaged reputation, loss of customer confidence, regulatory penalties, and the sheer cost of cleanup.

Your Inbox and the Enemy Within

Infected email attachments are probably the easiest and most popular way of delivering ransomware attacks, especially in an enterprise environment. The inherent trust that most end users put in the contents of their inbox means it's simple for cybercriminals and hackers to persuade the average business user to click on a link or run at attachment which, in turn, infects their computer with ransomware.

The truth is, the cybercriminals are relying on this level of apathy to ensure they can sneak their malicious payload past your quickly out-of-date gateway or desktop security systems.

To trick users into opening file attachments, attackers use all sorts of tactics. You'll see emails containing notices of court appearances, courier delivery notes, booking requests, speeding tickets, complaint letters, sales notices, invoices, travel itineraries, and more. Social engineering plays a heavy part in persuading end users to open the email, but also to trick them into running any code inside the file. This code, of course, is the dreaded macro.

Macros: The Gift that Keeps on Giving

Aside from the finance team, and perhaps State Excel Champions, there are very few people who would, in normal daily life, use an Office document macro. *So why are our users are tricked into running malicious macros all the time?* Cybercriminals have become adept at using booby-trapped Word, Excel, and even PowerPoint documents as a dropper for their malware; and our end users are falling for their tricks again and again.

Later, i.e. post-Office 2010, versions of Microsoft Office have macros disabled by default. Unless, of course, your IT team have re-enabled them for the sake of productivity. But that doesn't stop attackers trying to persuade end users into the clicking the "enable macro" button that appears at the top of the document. Often, a popup will claim the content of the file is obscured or even encrypted and that you'll need to "enable content" to read the message. It's not uncommon for cybercriminals to target stressed finance users at the end of a quarter or fiscal year to elicit a hurried decision for action.

The trick here, as demonstrated well by Locky, is to send a "clean" file to a victim; there is no signature-able content in the file, so it won't get picked up by classic anti-virus tools. Most botnet and malware code generators can create

polymorphic malware code, so every piece of malware they send is unique to a specific email. This is done in an attempt to avoid signature and content scanning engines. Once the clean-looking, yet malicious, file is delivered, the victim may be tricked into opening said file and either auto-executing the macro or manually enabling it. Quietly, in the background, Microsoft Office is running the macro code which, in this case, is downloading the actual malware from a remote site.

We're Ok, We're a Small Business… Right?

Wrong. Ransomware attacks can strike any type of business. In fact, smaller organizations are usually less protected (or have fewer IT resources) than their larger counterparts. The impact is often greater in smaller businesses too, as the IT infrastructure plays a vital role in daily operations.

Small businesses are often reluctant to appreciate their risk. I've had many business owners tell me, "we're safe, why would anyone want to hack us?"

This always fills me with fear, as it indicates an underlying level of general security apathy.

What we all need to realize is that there are cybercriminals out there who will target every type of business, large or small. In fact, sometimes, the smaller the better. Of course there's the usual fire-and-forget or scatter-gun tactic, where hackers will send millions of emails to prospective victims in the hope that some of it is successful. I call this general malicious internet noise. But, there's also the type of hacker who will research a particular vertical or type of business and tailor their attack specifically to the target. Often, we'll see hospitals become the target of choice here because of the sensitivity of information

they contain (high-value) and their commonly below-average security preparedness (easy target).

So please don't think it won't happen to you. You don't want to find out the hard way that you're not prepared for the aftermath of the attack.

Is there a Silver Lining?

We could be on the verge of seeing ransomware attacks decline. Some reports, like the Verizon Data Breach Investigations Report, tell us that occurrences of ransomware attacks doubled compared to the previous twelve months. Even then, ransomware accounted for 39% of all malware-specific security breaches. At the same time, some of the technology used by cybercriminals to deliver ransomware is evolving as well.

I mentioned earlier that we're seeing a rise in the rate of malicious cryptocurrency mining. This may soon surpass ransomware's popularity in the coming years. You see, ransomware has often relied upon malicious software packages called exploit kits; you may have heard of Angler, Neutrino, Nuclear, and RIG. Exploit kits, or EKs, are designed to run on watering-hole websites or be delivered by compromised advertising networks.

Usually EKs are part of an underground malware market, which rises and falls as they gain notoriety. As one EK dies, another pops up. However, towards the end of 2017, that started not to be the case and as larger EKs like RIG, Angler, Neutrino, and Sundown disappeared, they simply weren't replaced. There are lots of reason for this decline, but the net effect is that there are fewer ways to deploy ransomware to a target. So attackers had to rely on the old tried and true mechanisms like phishing, which are often less successful because we're doing a good job educating our users to be wary of such attacks.

EKs that do survive, like RIG for example, now concentrate on delivering cryptocurrency miners computers instead of

ransomware. Cryptocurrency mining could be “the new black” in the malware world, as it is certainly more profitable than even the most successful ransomware. And, as enterprises get better at protecting themselves against ransomware, they leave a door open to this new threat. The arms race continues, but understand that ransomware is not dead yet.

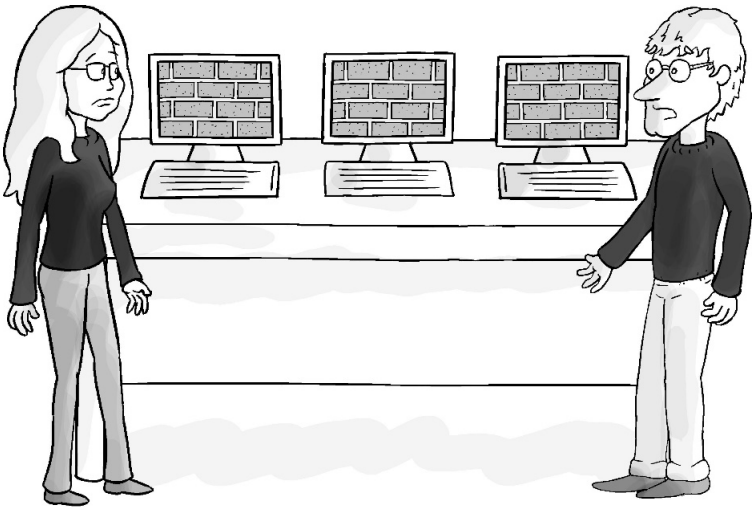
Paying the Ransom. Yes, or No?

Do not pay, just don’t. There are several reasons why. You’re perpetuating the problem and negotiating with terrorists. You need to realize that the money paid goes toward the nastiest, darkest parts of humanity such as the people smuggling, sex trafficking, drug dealing, gun running, and organized crime that is the criminal underworld. But perhaps more directly, there is no guarantee your files will be returned to their normal state, nor that you won’t be re-infected later.

Just to be clear, I’m going to say it again.
Do not pay the ransom.

Of course, I do appreciate there will be times when you have absolutely no choice but to pay, but these ought to only be related to personal computing losses, rather than enterprise IT, and incredibly rare by now. But you should only really pay if you can come to terms with funding the list of activities I mentioned above. In an enterprise IT environment, restoring from a good and recent backup should be the only answer to your ransomware problems.

Resilience, Hyper-Availability, and Recovery



"We paid the ransom but the computers are bricked."

We know now that ransomware is clever, it adapts and overcomes, and it specializes in sneaking past traditional security solutions like secure email gateways (SEG) and desktop anti-virus (AV). *So when it comes to solving a problem like ransomware where do you start?*

Well, I'm not suggesting you're wasting money on your SEG or desktop AV, just make sure they're modern. For example, use an SEG vendor who can apply additional checks to inbound attachments, like sandboxing, and make sure your desktop AV solution has similar and specific anti-ransomware protections; some will even prevent the spontaneous encryption of data and allow you to roll back if the worst happens.

But, in my view, those are just the basics; get those right and you're half way to being protected. There are many other types of protection you should deploy.

Patch Everything, and Patch Often

Looking back over most of the exploits from the last few years, you'll see they all rely on a vulnerability in an operating systems, application, browser, or plugin. These vulnerabilities are a fact of life when it comes to writing code, hence why vendors and software makers push patches and fixes out to their user base all the time.

There really isn't any excuse for not making sure your IT infrastructure is patched these days.

So, patching everything, patching it often, and making sure you stick to this regime is an important first line of defense against ransomware. Most exploits are successful because they rely on the end user's computer being unpatched and, therefore, still vulnerable, so patching is a vital step you must take to help reduce your threat window.

But We Have Desktop Anti-virus

This is a lament I hear all the time. *"We have desktop anti-virus, we'll be ok, right?"* Sorry folks, but just relying on desktop AV isn't going to protect you.

And, for the Mac users out there, the old *"we use Macs we don't get viruses,"* line won't cut it either.

Of course there are many desktop or endpoint protection solutions that can offer some degree of protection, but those should really only be your last line of defense. If the attack gets as far as the OS on the desktop, then it's right inside your environment and has circumvented all of your other layers of security. Remember, we talk about defense in depth when it comes to cyber security.

CryptoWall 3.0 is a great example of what we're up against here. This ransomware variant is said to have made its owners nearly $350 million, and the turnaround time from version 3.0 to 4.0 was a mere 48 hours. Imagine the resources the cybercriminals must have to be able to develop code that quickly; and with that kind of budget. I'd argue this is not the agility that most AV vendors can work with, sadly.

Modern AV systems rely on signatures and fingerprints to identify code or behaviors in malware. Cybercriminals and malware writers know this too, and write code to try and avoid detection. Polymorphism in malware is a great example of this cat and mouse game. Cybercriminals know that they need to stay ahead in the race against AV vendors, but they also rely on the lag that exists between the vendor releasing a new signature and the time it takes to get that rolled out to all your desktops or endpoints. By the time the roll out is complete, the malware writers are releasing new code, and the whole process starts again.

Better Safe than Sorry – Backups Are Important

By now you may be thinking that all is potentially lost when it comes to ransomware. But that doesn't need to be the case. With proper preparation, the impact of a ransomware attack can be easily mitigated. Backing up data and key infrastructure is the first step to ensuring you can continue operating and recover from a ransomware attack, and this has been proven by several high-profile victims already. But, there's a catch here too. I'm not just talking about taking a shadow copy of your files and storing them on the network somewhere. As you know there are some ransomware variants that will actively hunt down and encrypt mapped an unmapped network drives, as well as cloud storage. We've also seen a few instances of backups being encrypted by ransomware as well.

Why are backups so important? Well, consider the impact of a ransomware attack. You're basically going to suffer an outage of your IT infrastructure as everything is taken offline by the

malware. Remember, ransomware can spread throughout a corporate network once a single computer is infected, so you'll have to act fast to prevent this from happening, or rely on your backup regime to recover.

The following tips should help you keep your backups out of reach of the malware.

Apply the 3-2-1 Rule for Protection

There's a handy and timeless rule you can use to think about best-practice backups, it's the 3-2-1 rule. Sadly, it's not something I invented, and the credit must go to the photographer Peter Krogh. The rule will mean you always have an available and useable backup of your data and systems and, in a world where ransomware can instantly take you offline, that's a vital precaution.

For many, a straight copy of the data to another drive is about as complex as their backup gets.

So how does the 3-2-1 rule work? It's likely you're already following a similar process if you're serious about backups.

Three: Ensure you have at least three copies of your data; a primary and two backups. Why? Well, think about trying to verify a backup, or individual file—you might use something like a hash or checksum to validate a file. If you only have one copy, you have no idea if it's corrupt. Having two copies means you can only compare one checksum to the other, and have no idea which is corrupt and which isn't. Having three copies means that you have a deciding vote and the third checksum can be used to validate one of the

others and ensure you overwrite a corrupt file with a known good copy.

Two: Use at least two different media types to store the backups. Why? All media degrades, from tapes, to DVDs, to flash media, and it's all vulnerable to environmental factors as well as technical obsolescence. Two different types of regular media are enough to protect you here.

One: Keep at least one copy of your backup offsite and offline. Why? To protect your backups from environmental issues like fire, flood, theft, and electromagnetic problems. This is likely to be the best practice you follow today, but make sure offsite is actually "offsite in a secure location." In the back of your car or at home in a cupboard isn't classed as a secure environment for offsite data. The cloud can be used for offsite backups, but at least make sure these are offline until you need them—remember how some ransomware will encrypt mapped network drives too.

Consider How You Perform Your Backups

There are other useful and incredibly simple considerations for backups when it comes to ransomware that could help.

It's important here not to fall for the convenience bias; making your life easier in exchange for weaker security.

Think about the accounts that control and store your backups. Don't backup data with a network administrator account. Use a dedicated service account that is only there for running backup processes and doesn't have wider network access.

Disable or remove local administrator rights from normal end users. You'll protect them from 90% of the threats that face the endpoint just by doing this alone, making it much harder for malware and ransomware to infect a computer.

Keep your backups 'air-gapped' as much as possible. By this I mean offsite and offline, and disconnected when not in use. Backing up to an attached storage device, such as a removable hard drive is a sensible idea, but once the job is complete, remove the device so it can't be overwritten by any malware that might affect that computer. If possible, it's always a sensible idea to auto-eject any removable backup media and tapes once a backup is completed. I've yet to meet a ransomware that can physically pop media back in again.

Using the cloud as a storage location for backups, or even using a dedicated cloud backup agent is a sensible idea too, especially for ndividual computers that can't store their file data centrally in an enterprise environment. And always make sure you can set the backup to offline somehow, as offsite and offline is an essential protection here.

Similarly, easy re-imaging of devices and computers is necessary if you're not able to fully restore bare-metal backups to end user computers. Bare-metal recovery is largely reserved for production servers, whereas end user computers are generally only backed up to a file level. So being able to restore a vanilla OS to end user devices is as vital as restoring the file data. Imaging platforms allow devices to be recovered to their "as new" state in the event of an attack, and serve a useful purpose as a deployment tool for everyday infrastructure management. Do ensure, however, you keep your images up to date—image OS, apps, and patch level should be reviewed on a regular basis.

Think About the Endpoint Too

The endpoint, in this case, is anywhere data is processed. Ransomware will hunt down every connected device and drive

and work to encrypt that data, so make sure you think about the connectedness within your network.

I always advise organizations to think about the original endpoint first, i.e. the end user. Their training, awareness and understanding is vital; I'll come back to user awareness training later. It is vital you think about all the places the end user can access data and Internet resources, email etc. If you make the mistake of just focusing on gateway protection or desktop AV protection, you're missing the bigger picture.

Remember users can process data not just on laptops and desktops, but also smartphones, and even workloads in the cloud, or cloud-connected storage. Applying the same protection across all these endpoints means your ransomware resilience, recovery, and availability will be better planned and executed than if you're just thinking about a single endpoint or device.

Foster User Understanding, Not Just Awareness

Human nature has become the weakest link in most enterprise cybersecurity strategies. Social engineering is an easy way for any attacker to trick an employee into carrying out a number of tasks for them; it doesn't require any particular expertise or knowledge and, due to the inherent trust of human nature, it generally succeeds. The bad news is the attackers, hackers, and cybercriminals are getting better at it all the time. It's far easier for them to send an exploit bought from a cybercrime network in a cleverly worded email than it is to learn the code required to compromise a device or network.

Simply asking for the crown jewels is often all that's required.

The security community has woken up to this threat over the last few years, and talks a lot about the human firewall, end user awareness, and end user security training. Sadly, even with all this focus on the end users, attacks still get through and are successful. There are even a few brave organizations that don't train their staff, as they believe it doesn't provide value for money, given how many successful attacks occur despite the training. I don't condone this. I simply warrant that it's always better to provide some training than none at all.

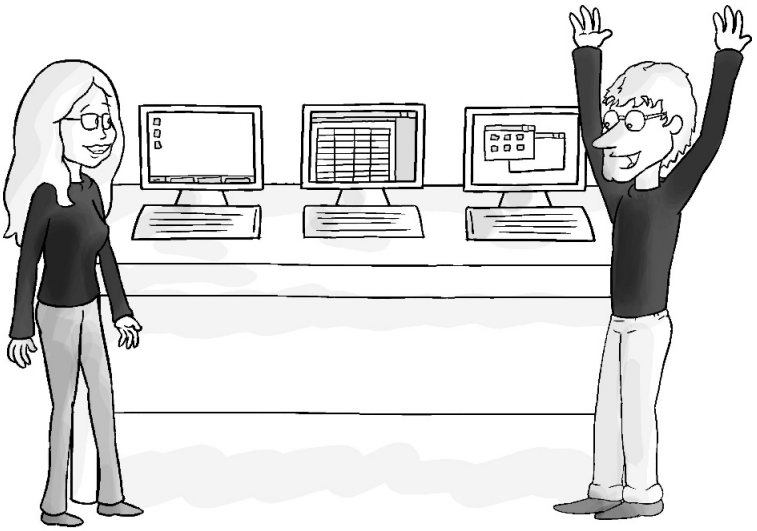
I'd be much happier if we thought about end user understanding, rather than awareness. Awareness lends itself to a shrug of the shoulders and the "it'll never happen to me" apathy that causes organizations to have security lapses.

I'd advocate that it's far better to talk about end user understanding instead.

So ensure your end users actually understand the threat of the day and how it'll impact them personally as well as the business. Try to find new and interesting ways to keep them informed, don't just re-run the same old dry security training every month.

The threat moves on at such a pace that we need to keep our end users up-to-date with the latest developments, and by virtue of better this better engagement they'll feel more empowered to help protect the business.

Recovering from Ransomware Attacks



"They weren't bricked. The systems are recoverable and we were prepared!"

Recovery capabilities from ransomware and other cyberattacks should now be a staple part of any enterprise IT strategy. In fact, you ought to consider the recovery from these types of attacks in the same way you do an outage since, in most cases, an outage is the most likely outcome with infrastructure taken offline or service is denied. So get into the habit of extending your BCP activity to include cyberattacks. These simple standard operating procedures (SOPs) and immediate actions (IAs) should help you plan how to recover from a ransomware or other cyberattacks.

SOPs for Responding to Ransomware Attacks

1. Panic. Yes, panic. It's only natural under the circumstances, so get it finished and out the way. Go somewhere out of sight, have a small panic, then take some deep breaths, as you'll need a clear head.

2. Don't panic. Time to calm down, stop, and think. *What's happening, what's being affected and do you have any clear idea of the impact yet?* Try to control the adrenaline that'll be pumping around your system so you can make sensible, level-headed decisions; the first of which is to make sure what's happening is actually real, by which I mean it's not a panic from someone who's not sure what's affecting them. Get your incident response team together. If you don't have one, this will be a representative or two from IT, security, PR, legal, and management. You may want to implement your business continuity plan since it'll take time to isolate and remove the ransomware threat.
3. Pull the power. The easiest way to forensically preserve the state of a disk that's being attacked by something is to simply pull the power cord. Shutting down takes time and alters timestamps, as does a reboot. By then, the ransomware might be resident enough to cause a lot of damage. Pulling the power will, at least, allow you to recover unaltered files from the disk and support forensic analysis.
4. Contain and limit damage. If you can identify ground zero quickly, then great. Isolate the device from the network as per point 3 above. If you can limit network access between VLANs or segments temporarily, do that too in order to prevent further propagation. The key here is to make sure you know the scope of the attack right now and where you think it could spread to.

You may want to preserve the ground zero infection point for forensic analysis and law enforcement action.

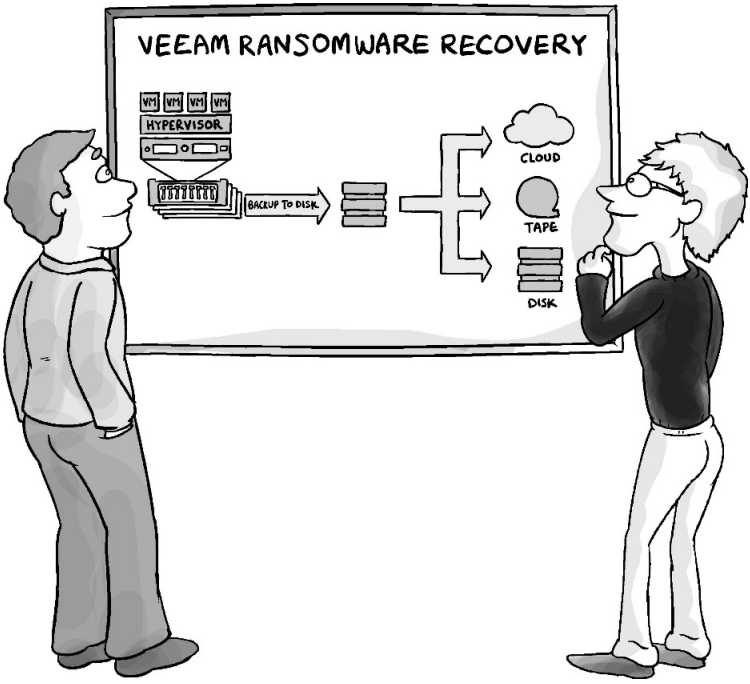
5. Remove and recover. The next phase is to eradicate the ransomware from your computers and network. If you've

successfully contained the attack, the infected machines can be wiped clean, re-imaged, and restored from backup.

6. Investigate. It's key to retain evidence, so make sure your logs are retained for all gateway services, as well as the infected computers. If you've got the initial infection point identified, that disk image or even physical disk will be useful for law enforcement as evidence. Contact the local authorities, as they may already be investigating similar attacks. It's also important to report these attacks so the wider security community can build up an accurate picture of the problem and work on defenses together. You can report the crime to the FBI through their Internet Crime Complain Center or IC3 at www.ic3.gov, or in the UK to the police at www.actionfraud.police.uk.

7. Remediate. Lastly, it's important to identify and remove the problem that caused the issue in the first place. It may be that your SEG let through a malicious attachment that wasn't identified. Or perhaps your endpoint AV and protection failed to react to the threat once inside the business. It's also likely there's going to be some end user training needed to make sure everyone fully understands how the threat is affecting the organization. Above all, this should be a learning experience for you, your end users, and your management. Take some time when the smoke clears to assess what you did well and what didn't work. Then, make sure your plans are modified to ensure you can perform better next time—be that with technology, training, or processes.

Vendor Sponsored Chapter:
Veeam Hyper-Availability Platform



In recent times, ransomware has become the most significant threat facing enterprise IT environments. This is no surprise given how successful ransomware is as a money-maker activity for cybercrime gangs around the world. They quickly invested their R&D budgets (yes, they do have those too, just like you) into ransomware, at the expense of what we might call more classic attacks like phishing or malware, when they realized there was (very) easy money to be made here.

Because of this interest in ransomware by the cybercrime community, we can be sure that the threat won't go away any time soon, and we'll see it get a lot worse before it gets better. There are already signs of increasing complexity and sophistication in the way ransomware is written and in its execution, and this book touches on a few of those advances.

Sadly, as the criminals improve their technology and the ways in which they can make ransomware more effective against our users, many organizations will struggle to keep up.

So with every advancement of this malware, we see more and more enterprises being affected and losing out to the cybercriminals. It's fair to say that many of the most well-known primary defenses are letting ransomware sneak through; by this we mean platforms like email security gateways and web content filters. Ransomware is often delivered via a malicious email attachment, or through some sort of drive-by or watering hole attack on a compromised website, so when the systems protecting those services fail to detect the threat, ransomware is successful.

By then it is, of course, too late. An end user has opened the attachment or clicked a link, and before you know it there's a help desk call being logged because they can't access any of their files any more, or there's a skull and crossbones on their desktop. In the worst case scenarios, where ransomware has used SMB shares to propagate around the network, it's likely all sorts of proverbial stuff is breaking loose, and your IT team is in for a long and complicated few days (and nights). Your users will be left unproductive, of course.

That's why Veeam thinks about countering ransomware as a recovery scenario. The initial infection may be inevitable, so the best protection is preparation. Veeam doesn't prevent ransomware, but it does allow you to be ready to recover when the attack comes. They apply the 3-2-1 methodology to help IT teams think about how best to ensure their data are safe, and their integrity is maintained, so when you lose systems they can be quickly and painlessly recovered to production-ready status.

Veeam Availability Suite, a core component of the Veeam Hyper-Availability Platform, gives you the ability to quickly and effectively restore critical data that's been infected by ransomware by leveraging their 3-2-1-0 rule. Three copies of

the data, on two different media types, including one off-site copy, and backed up by SureBackup and SureReplica to verify the primary backup. This way, you can be sure that it is recoverable and consistent. Any ransomware activity that could present a threat to your network can be quickly identified and alerted upon.

Adding Veeam backup and replication software to your security strategy, specifically for ransomware protection, will put you in control of the situation whenever it may arise. When ransomware strikes one or many of your endpoints, you can rely on rapid restoration of infrastructure to get back into production fast. This includes databases, applications, single or multiple files, and even operating systems.

Veeam also integrates with large-scale storage platforms like HPE, Dell EMC, NetApp, Lenovo, INFINIDAT, Pure Storage, and IBM, so there is no need for additional hardware or application expenditure.

One magical part of Veeam's technology, which is especially relevant when thinking about ransomware, is the On-demand Sandbox for testing recovery points. This effectively gives you the ability to easily discover the last known good restore point and to check it in a safe sandbox before fully restoring it to production, instead of re-writing infected systems with infected backups.

Protecting your backups is vital. There's no point backing up data to a drive or device that the ransomware is going to find and encrypt. Yes, this does happen (as has been mentioned a few times in this book). Make sure you're using different credentials for backups and their storage—not DOMAIN\Administrator. Veeam recommends not joining your backup infrastructure to the domain or, for large environments, putting it on its own separate domain all together.

Then, of course, there's off-lining your storage too. Powering off VMs, auto-ejecting removable storage, and using Cloud

Connect backups are all ways of air-gapping your backed-up data. Veeam Cloud Connect is quickly becoming the de-facto standard for the safest way to run and store backups. It's a complete out-of-band protection solution where backups are taken via the same Backup Copy Job on the network, then automatically sent to a service provider in the cloud; pure safety and perfect preparation for a ransomware attack.

Until now, we've only thought about ransomware recovery and protection at a macro, server, and network level. But, as our networks move further away from what we think the classic LAN looks like, we're forced to rethink our position on ransomware resilience, recovery, and availability. Increased complexity, stringent regulatory requirements, and a variety of other factors can cause serious headaches.

This is where Veeam Agent® *for Microsoft Windows* and Veeam Agent® *for Linux* can help us. The former, for Microsoft Windows compute resources, helps us by closing the gap that some enterprises face with large heterogeneous or multi-cloud environments. It increases workload mobility and accelerates recovery of those resources running on endpoint devices, physical servers, and in cloud-based environments.

For enterprises stretching their Linux-based wings, Veeam Agent for Linux enables the complete backup and restoratrion of Linux-based workloads in the public cloud. The primary purpose: to minimize downtime, maximize business continuity, and do it all without the usual considerable expenses of time, money, and manual efforts. I remember thinking, when I had first heard about Veeam's Agents, that blaming the intricacy of BCDR for any shortcomings in preparedness was no longer going to be a viable option to shirk accountability. O*h well, time to do things the right way.*

Ransomware isn't a problem that looks like it'll fade away any time soon. In fact, all of the signs point to an escalation in capability and effectiveness of the threat. This makes your

protections against the threat vital, and planning for the inevitable disaster tantamount to success.

Perfect preparation with the help of Veeam will mean you can complete that planning loop easily, as well as sleep soundly at night knowing your data are readily available and quickly recoverable. There's no need to worry excessively about ransomware, but it should focus your attention on technologies that, perhaps, haven't been refreshed or reviewed for a while.

If you'd like to talk to someone about a wider and holistic approach to ransomware protection and recovery in your organization, please talk to the person who gave you this book to find out how they can help.


Introducing the
Hyper-Available Enterprise
accelerating innovation to meet tomorrow's demand
Intelligent Data Management for the Hyper-Available Enterprise™
VEEAM®

Easily converse about Ransomware defense and survival in any setting.

Don't pay the ransom! That's the advice given when asked about ransomware and how to deal with it. But how does one defend themselves against ransomware and survive an attack successfully get through your defenses? That is the key to this book. Because, if you aren't going to pay the ransom, you better have an alternative means of recovery!

About Orlando Scott-Cowley

Orlando Scott-Cowley is a cybersecurity consultant and strategist. He is an unlikely geek, having never really got into Star (Wars | Trek), but grew up as an Oracle DBA, sysadmin and then a penetration tester. Today, he helps organizations secure themselves and their users from the malicious threats, hackers and villains, around the world.

Follow him on Twitter @orlando_sc

ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.