RansoMwaRe

Is your business ready?

When it comes to crypto-ransomware, it's not the ransom that's so damaging to business. It's the downtime. This study explains what to do about it.

Your private key will be destroyed by:

71h:55m:23s

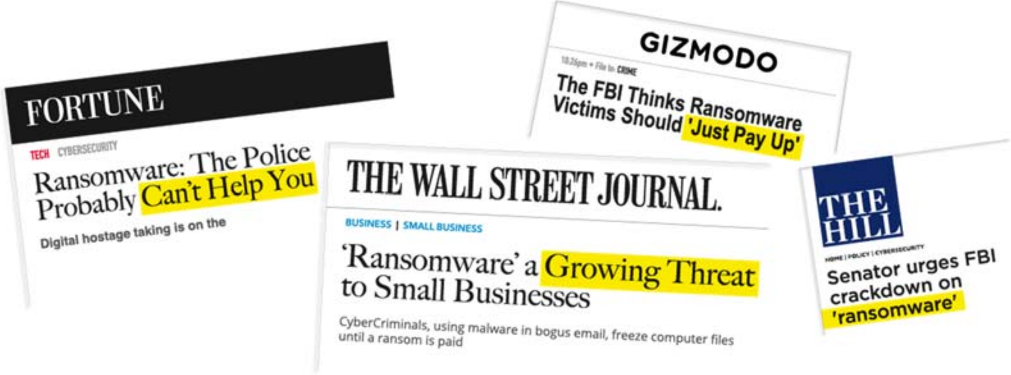
INTRODUCTION

Ransomware is a category of viruses that encrypts files on a victim’s computer and keeps them locked until the victim pays up. If you don’t pay the criminals who spread it—up to $5,000 per user, according to the FBI—you lose the files forever.

These screenshots are taken from computers infected by ransomware.

Imagine you arrive at your office to find all your computers padlocked, and a man in a mask demanding $5,000 per user to give you the key. That’s what ransomware is like.

Numerous tech publications have listed ransomware among the biggest digital threats facing businesses today. This is due to its capacity to slip through corporate security and its potential to replicate itself across a corporate network. The first ransomware targeting Macs has recently been spotted in the wild.



FORTUNE

TECH CYBERSECURITY

Ransomware: The Police Probably Can't Help You

Digital hostage taking is on the

GIZMODO

10:26pm • Filed to: CRIME

The FBI Thinks Ransomware Victims Should 'Just Pay Up'

THE WALL STREET JOURNAL.

BUSINESS | SMALL BUSINESS

'Ransomware' a Growing Threat to Small Businesses

CyberCriminals, using malware in bogus email, freeze computer files until a ransom is paid

THE HILL

HOME | POLICY | CYBERSECURITY

Senator urges FBI crackdown on 'ransomware'

If your company gets infected, you face two very hard choices: Either spend multiple days recovering the locked files from backups—during which time you'll endure user downtime, lost sales and angry customers—or pay ransom to an organized crime syndicate.

(Even then, still need to wipe and restore your computers to remove the virus. Without a business continuity plan in place, your business suffers downtime regardless. More on that later.)

The employees of the Hollywood Presbyterian Medical Center can tell you what it's like. This February, they were forced to take their PCs offline so I.T. could contain a ransomware outbreak and restore the files.

They spent 10 days relying on fax machines and paper charts. They made unwanted headlines in the New York Times, the BBC and countless other publications. In the end, they ended up paying $17,000 in ransom, just to avoid even more protracted downtime.

This report, which is based on a survey of 300 IT experts, helps you understand the true cost of ransomware, learn some basic prevention and containment techniques, and plan for business continuity to avoid downtime in the increasingly likely even that your business will get hit.

CHAPTER TWO

THE SCOPE OF THE THREAT

Below are the results of a survey of nearly 300 IT experts about the crypto-ransomware threat. The survey respondent panel was carefully screened to include people who consult with businesses of all size on setting up and maintaining IT infrastructures. These are the men and women who are on the front line of business IT challenges.

The survey revealed three key findings: the biggest cost to businesses is downtime, not the ransom payment; ransomware is targeting bigger businesses and spreading within corporate networks; and a widespread lack of business continuity planning is what makes ransomware so dangerous (and so lucrative for criminals).

Paying ransom is the least of your worries

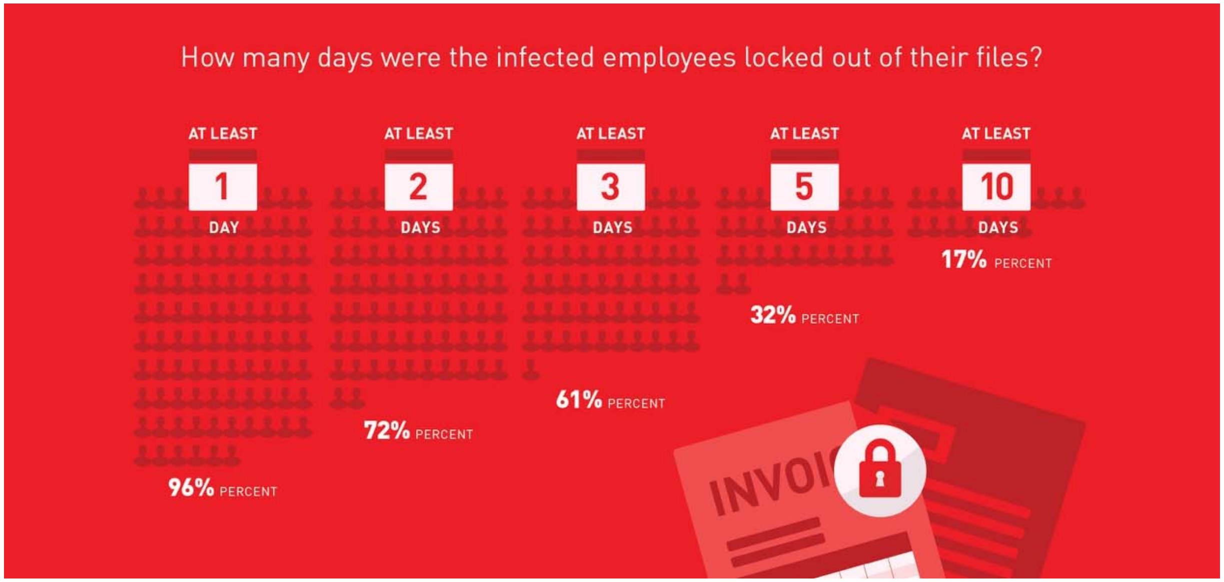
When asked to name the business impact of ransomware outbreaks that these consultants have assisted with first-hand, the actual cost of the ransom came in dead last. In other words, contrary to popular belief, the worst part of ransomware is hardly the ransom.

Downtime lasts for days

Infected computers need to be immediately isolated from the network to avoid spreading the malware. This leaves users without access to their PC while IT contains the virus and restores the device. But even if they can get to their files through alternate devices, the files themselves are encrypted and thus unusable.

There are business continuity solutions that enable you to instantly roll-back your file folders to clean versions and access them using alternate devices. (More on this below.)

But the survey results suggest that few businesses have business continuity solutions in place: 82% of business users lost access to data for at least two days, and 32% lost access for five days or more.



Downtime occurs even if you pay the ransom

An infected computer must be wiped and restored. 52% of experts reported that the wipe-and-restore process took two or more days for the infected devices.

Also, you should note that 19% of companies that paid the ransom still didn’t get their files back.

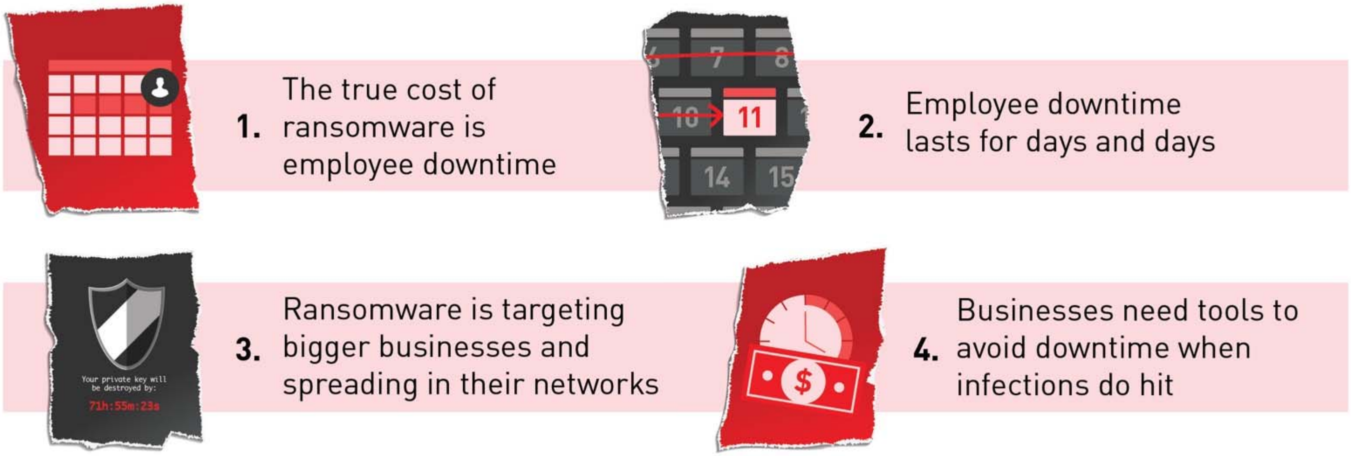
Bigger businesses are being targeted

Ransomware is going after businesses of all sizes. 89% of the businesses hit by ransomware were 10 employees or more, while 60% were bigger than 100 employees. And when ransomware hit, it spread; 75% of outbreaks affected 3 or more people, and 47% of outbreaks spread to at least 20 people.

Ransomware is a growth industry

43% of IT consultants have had customers fall victim to ransomware. 48% saw an increase in ransomware-related support inquires in the past year—across customers in 22 different industries.

Key takeaways



1. The true cost of ransomware is employee downtime
2. Employee downtime lasts for days and days
3. Ransomware is targeting bigger businesses and spreading in their networks
4. Businesses need tools to avoid downtime when infections do hit

PREVENTING RANSOMWARE

Like most forms of malware, ransomware infections may arrive through malicious web pages, infected thumb drives, or other common attack vectors. But the most common infection vectors are email-based—specifically, phishing emails.

“Phishing” is when criminals send a seemingly legitimate email that disguises a malware-laden attachment or link to an infected website. Criminals often use phishing to trick users into submitting sensitive information such as passwords or credit cards; but these days, they’re also using it to spread ransomware.

Phishing is particularly well-suited to ransomware. In a recent study, 94% of people couldn’t tell the difference between a real email and a phishing email 100% of the time. When study participants received an email that was spoofed to appear as if it was sent by UPS, 62% trusted it enough to click the link.

Protection against ransomware goes hand-in-hand with phishing prevention. Here are your top three activities:

Protect	Educate	Prepare
Your email defense should go beyond spam and virus scanning. It should also be sophisticated enough to recognize and block phishing attempts.	Technology can only go so far to stop phishing. Employees and executives have to be trained to spot phishing emails before they click.	While you need to block every single attack, the criminals only need to succeed once. Plan in advance for how you'll contain the damage before they do finally break through.

CHAPTER FOUR

CONTAINING A RANSOMWARE OUTBREAK

Ransomware is hard to spot while it's encrypting user files. The user may notice his or her machine acting strange during the encryption process: file extensions will change, files won't open, or the computer's fan may whir loudly as the processor copes with the computing demands of encryption. But the average user may not recognize the danger until the ransom demand finally appears.

This means that you typically don't learn about the infection until after the damage has begun and the malware is already inside the network.

At this point, your priority has to be to contain the virus and prevent it from spreading within the network. More sophisticated ransomware variants may attempt to propagate. Malware of all forms has been observed to send malicious messages using the user's email or chat clients, or even to deposit infected files in open shared folders on other users' computers.

Top three ransomware containment tips:

Isolate the infection	Size up the outbreak	Find the attack vector
Your top priority is to make sure the infection doesn't spread. Remove infected machines from the network. Shut down the network if you have to.	Figure out the scope of your infection—the type of infection, how many machines, how much data, etc. Consider contacting law enforcement.	Identify the source of the virus and fix your security weaknesses. Otherwise, more outbreaks may be in your future.

CHAPTER FIVE

BUSINESS CONTINUITY DURING A RANSOMWARE OUTBREAK

“Business continuity” is the ability for the business to continue operations immediately after a disaster, or even while a disaster is ongoing.

Many businesses have a crisis response plan in place for natural disasters, power outages and other disruptions. Fewer have “e-crisis” response plans for cyber threats such as ransomware. That’s one of the reasons ransomware has been so disruptive to businesses and so profitable for criminals: business continuity solutions have not previously existed.

In order for users to continue working during a ransomware outbreak, two capabilities are required.

The capability to roll back to uninfected files instantly

The capability to immediately access those clean files

Some of these capabilities exist in file sync and share products. Other capabilities exist in backup products. Ransomware has been so lucrative for criminals because these two capabilities have never before been present in a single product.

CHAPTER SIX

BUSINESS CONTINUITY WITH SHARESYNC

2-in-1 file sharing and backup offers instant rollback and instant access, enabling users to keep working during a ransomware outbreak

ShareSync is a universal file management tool: it combines real-time backup and file sharing into a single product.

This 2-in-1 feature set enables users to collaborate like Box and Dropbox, while offering complete file backup & recovery across any failure scenario like Carbonite and Mozy.

Among its feature set is the ability to roll back a user's complete file set to any point in time. It's a simple, do-it-yourself process: you select the archive you want to restore, select the target point in time—down to the minute—and press the button. Your archive is instantly rolled back to its state at that point in time. A user can then access those files instantly through the web or mobile devices, even as they're re-syncing to the user's computer.

	ShareSync	File sharing services (Dropbox, Box, OneDrive)	Backup services (Carbonite, Mozy, Crashplan)
Web and mobile access to files	Y	Y	X
Real-time (not scheduled) backups: Files are backed up every time they change	Y	Y	X
Syncs major content folders (Desktop, Documents + shared folders)	Y	X	Y
Point-in-time restoration from backup	Y	X	Y

"Business continuity" is the ability for the business to continue operations immediately after a disaster, or even while a disaster is ongoing.

Many businesses have a crisis response plan in place for natural disasters, power outages and other disruptions. Fewer have "e-crisis" response plans for cyber threats such as ransomware. That's one of the reasons ransomware has been so disruptive to businesses and so profitable for criminals: business continuity solutions have not previously existed.

In order for users to continue working during a ransomware outbreak, two capabilities are required.

INSTANT ROLLBACK
+
INSTANT ACCESS

The capability to roll back to uninfected files instantly

The capability to immediately access those clean files

Some of these capabilities exist in file sync and share products. Other capabilities exist in backup products. Ransomware has been so lucrative for criminals because these two capabilities have never before been present in a single product.

In the event of a ransomware outbreak, this combination of features—which can only be found in a 2-in-1 file sharing and backup service—keeps infected users productive.

ShareSync is designed with enterprise-grade control and security to offer at-rest and in-transit encryption, remote wipe of ShareSync data off any device, and the ability to change access permissions for folders or files that have been shared internally or externally.

Step 1

Close or isolate the infected computer(s)

Your first priority is to ensure the crypto-ransomware doesn't spread. Close any computer that's infected. Cut off network access if you have to—whatever you have to do until you get the infection contained. Call IT support immediately.

Step 2

Roll back ShareSync's file archive

Using an uninfected computer, your IT support person will access ShareSync's admin settings and roll-back the user's folders to the moment in time just before the infection occurred.

Step 3

Get back to work using alternate devices

You can get back to work using any other PC or mobile device. On the PC, you can access files through ShareSync's web interface; on a tablet or phone, you can use the ShareSync app. Meanwhile, your IT support will work on restoring the original device. Any edits you make to files will be synced to the original device as it is being restored.

CHAPTER SEVEN

CONCLUSION

Why plan for business continuity in the event of ransomware?

For users—Ransomware becomes a mild disruption instead of a major disaster

For your business—Avoid lost sales, angry customers and bad PR • Plus, no need to pay ransom

Ask us about establishing business continuity protection against crypto-ransomware with ShareSync.