

TERRIFYING TECHNOLOGY TALES™



VOLUME 1, ISSUE 3.

CONTENTS

THE TERRIFYING TALES.....3

THE RANSOMING 2.....4

DEADLY DOWNTIME.....6

THE PHANTOM SERVER.....8

DECODING THE IT CODE WORDS11

TERRIFYING TECHNOLOGY TALES

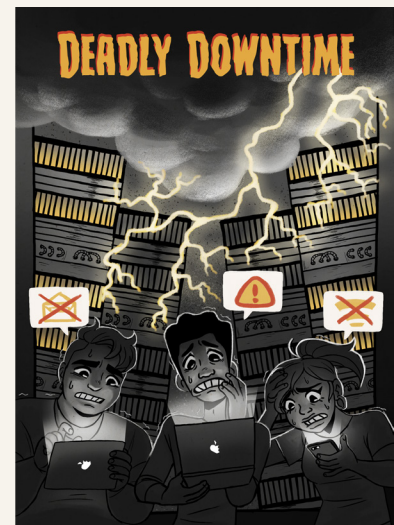


THE RANSOMING 2

An unwary drug testing facility who never thought they would become a victim of terrifying proportions. That changed one day when they discovered all their data was encrypted. You'd never guess how it happened. Hear the shocking twist and how they paid the price.

DEADLY DOWNTIME

It was a dark and stormy night. A powerful lightning strike fries a company's local server beyond recognition. In a flash, all their data was toast! Their business was trapped in the dark for what seemed like an eternity. Was this nightmare something they could recover from? Find out.



THE PHANTOM SERVER

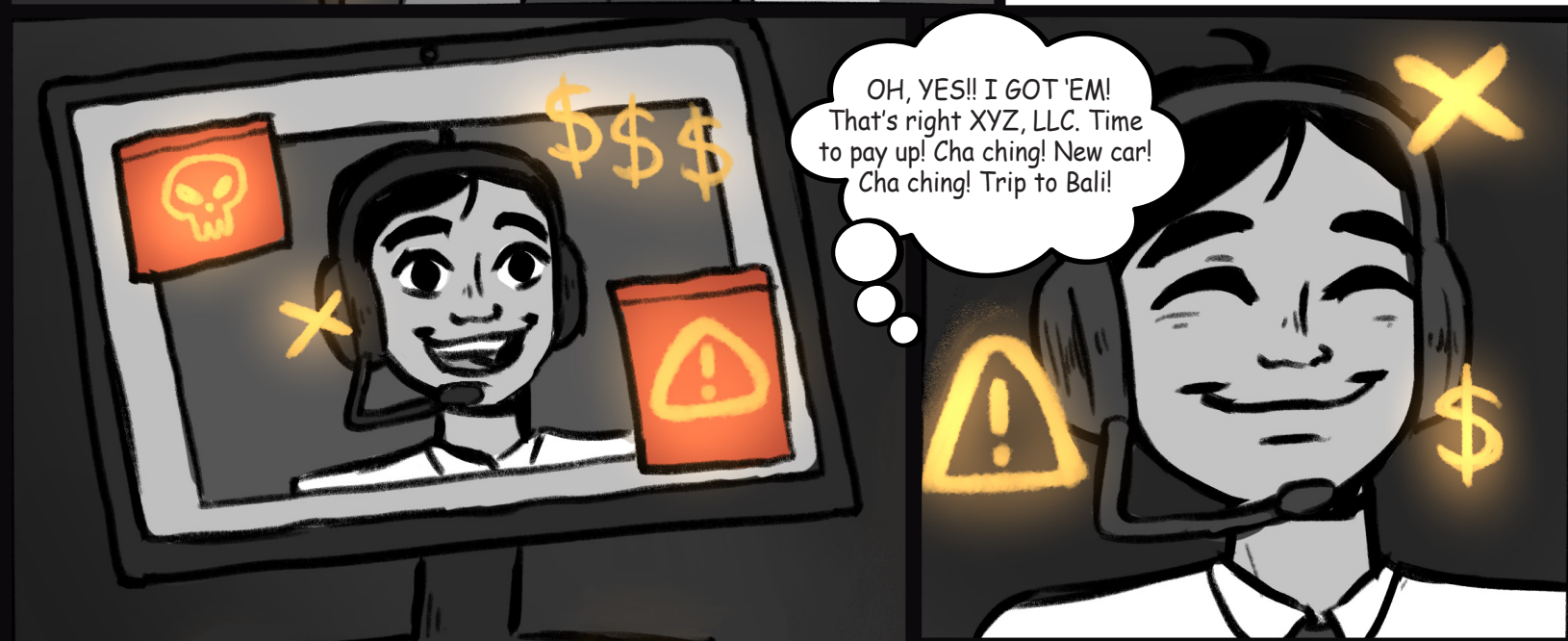
It was an ordinary day at a successful law firm's office. All of a sudden, an insidious intrusion from an outside organized operation took control of their system through the email server. The grueling details of how the possessed system terrorized the firm would make anyone scream.

THE RANSOMING 2



Unbeknownst to Bill, something gruesome and festering has appeared in an industrious company's systems.

Meanwhile, an unassuming, clean-cut chap... er... hacker... is sitting comfortably at his computer having the time of his life.



Four days later, after losing half their clientele, the weary company exhausted all options to regain their systems.

Defeated, they handed over the ransom... \$150,000!!!!

IT SUPER KNOWLEDGE



RANSOMWARE?!

START WITH THESE STEPS...

Shut down infected systems immediately

To avoid ransomware spreading, disconnect the infected device from any network it is on and turn off any wireless capabilities such as Wi-Fi or Bluetooth. Unplug any storage devices such as USB or external hard drives.

Determine the strain and the scope

Determine how many devices were infected, as well as what kind of data was encrypted.

Report the incident

You should let your organization know about the attack, but it's also important to report it to the FBI or your local authorities depending on where you are located.

Evaluate your options

If you don't have a backup solution, your other options are to do nothing (lose your data) or decrypt your files using a 3rd party decryptor. If all else fails, you can pay the ransom, but beware of this option as it increases the chances that you'll be targeted again.

Prevent future ransomware attacks

Educate your employees on cybersecurity awareness. You should also invest in endpoint security with a firewall or third party service that protects against ransomware.

To learn more about ransomware and how to protect your organization, check out these additional resources.

- [Ransomware Checklist](#)
- [Quick Guide to Ransomware Defense](#)
- [Ransomware Report Infographic](#)

SCARY STATS!



Do not have a specific plan in place to manage an attack



Suffered significant loss of revenue



Said cyber insurance did not cover all costs

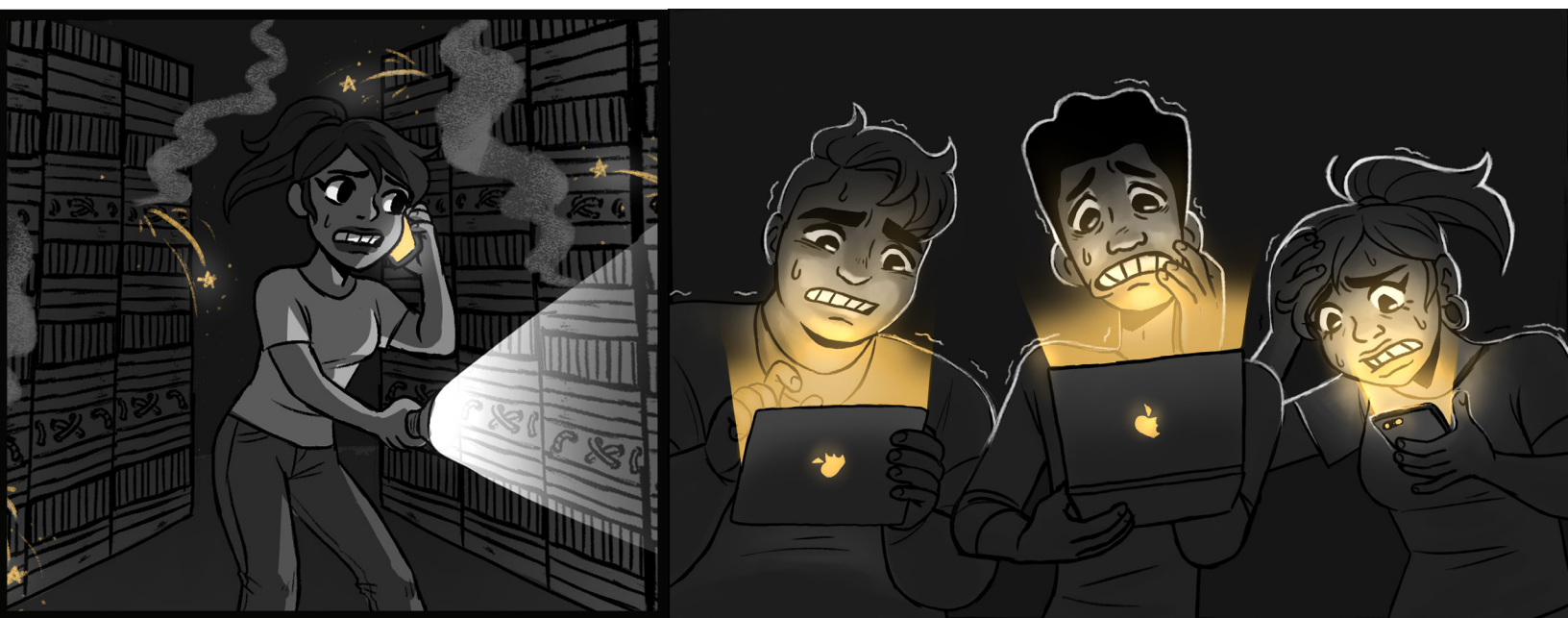
Source: Cybereason

DEADLY DOWNTIME



It was a dark and stormy night. Thunder rumbling in the distance when suddenly, "CRACK!" A powerful lightning strike fries the server of a busy company beyond recognition. They didn't know it yet, but in that flash all their data was toast!

Oh, no! The company couldn't believe this was happening. Just a few months before they'd had the chance to protect their server with a more thorough solution but made the less expensive choice. Now this!



The company was unable to access their email or their data... no accounting records, no client files and no documents or files to conduct their day-to-day business. Their server was a ghost of its former self!

Although the server data was backed up, the company would experience a week of downtime and endure a server replacement before their data and their business could be restored.

IT SUPER KNOWLEDGE



DATA AT RISK?!

START WITH THESE STEPS...

Consider cloud backups

Cloud backup solutions offer businesses a much more streamlined, effective, and cost-efficient way to save their data in the event of a disaster than traditional hard drive backups. They offer plenty of redundancy (your data being replicated across multiple sources) and improved levels of security.

Backup on a consistent basis

You're continually adding new information to your databases. That includes daily sales, new customer or vendor information, and other important data. In other words, you'll want to ensure that the data backs up on a consistent basis so that you don't lose any important information.

Use data encryption

Company data is often compromised by internal means — that is to say, theft. Even just simple incompetence on the part of employees can cause data loss to fall into the wrong hands. Using data encryption software can keep your data protected from those without the authority to access it.

Have a disaster recovery plan

A disaster recovery plan helps you keep your team organized and your recovery efforts concentrated. It typically consists of a detailed, step-by-step guide that breaks down every aspect of recovery into a clear and concise instruction.

To learn more about backup and disaster recovery, check out these additional resources:

- [Quick Guide to Backup and Recovery](#)
- [Managed IT Service Provider Checklist](#)

SCARY STATS!



96% of businesses experienced an outage in a 3-year period



39% of SMBs don't have any response plan in place



33% of folders used by a company are not protected in any way from a breach

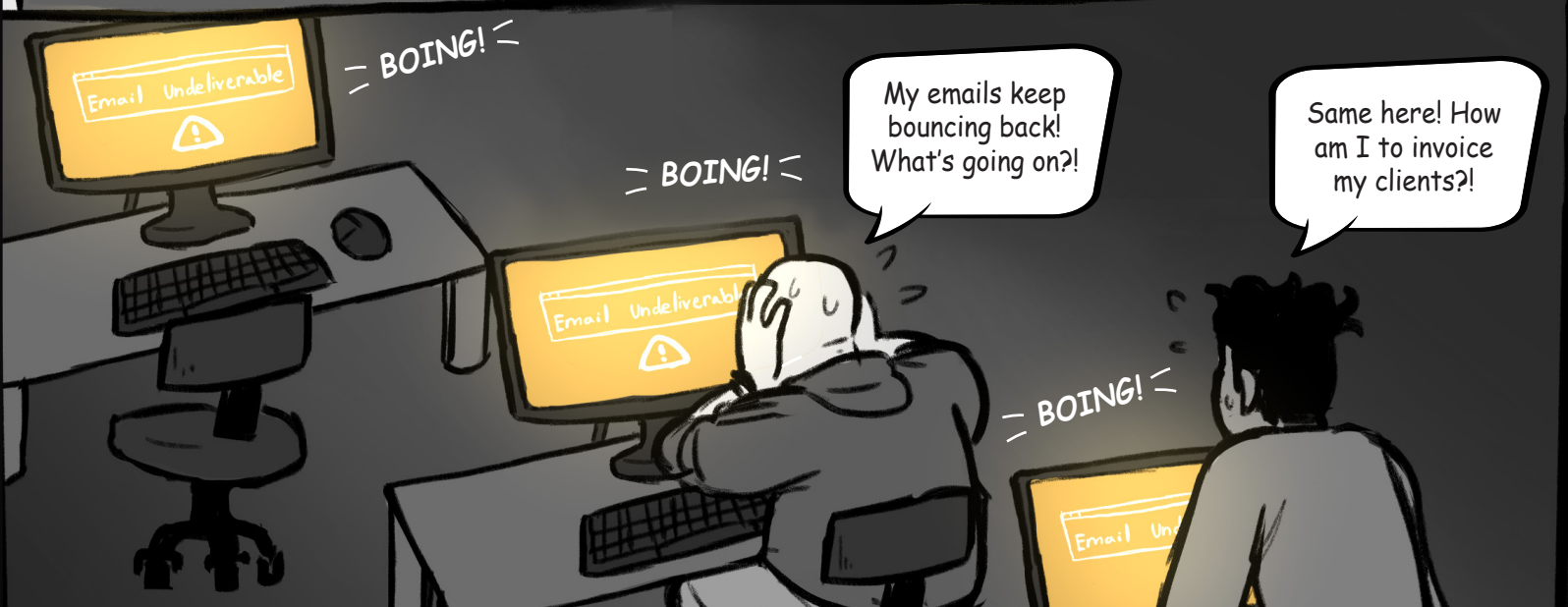


98% of organizations say a single hour of downtime costs more than \$100,000

Sources: LogicMonitor, Ponemon Institute, Varonis, ITIC

THE PHANTOM SERVER

THE LAW OFFICES OF
X, Y AND Z



THE PHANTOM SERVER

Once upon a time in a law firm not so far away, it was business as usual... a very ordinary day, indeed... until it wasn't.

Without warning, an insidious intrusion occurred!

In fact, this firm joined a long list of businesses who fell prey to the zero-day Hafnium hack — a wildly unbelievable event which compromised tens of thousands of organizations. It was an unprecedented email server takeover, believed to have originated from a state-sponsored Chinese hacking group known as Hafnium.

"What's going on? What does zero-day mean?" asked the law firm's gobsmacked employees.

They learned too late that the moniker "zero-day" signified the amount of time companies had before they were irreversibly exploited it was the making of a corporate horror story!

The hack was so insidious, and so far-reaching that the FBI made an unprecedented decision to deliberately seek out, reverse hack and remove the malware from servers the agency had been unable to secure in a conventional manner.

That operation, approved by a federal court, removed the malicious software, but stopped short of fixing the vulnerability entirely...

Meanwhile, for our hard-working friends at the law firm, email continued to flow but staff started seeing email bounce-backs and were receiving reports of countless "undeliverable" replies.

WHAT A CATASTROPHE!

Email is extremely important to the law firm, so this greatly impacted operations and revenue for more than a week! In fact, most law firms report that a down email system can result in losses totaling up to \$60,000 an hour.

With the help of their savvy-service-provider superheroes, the law firm's email server underwent detailed troubleshooting and was thoroughly cleaned. All was well with the firm once again.

IT SUPER KNOWLEDGE



EMAILS AT RISK?!

START WITH THESE STEPS...

Consider moving to Cloud

Most providers make cloud computing their number one priority. You'll benefit from the enhanced security as well as having built-in redundancy. Data can be restored more quickly and easily.

Use complex passwords

Passwords must be complex, reasonably long, and different across all account.

Use multi-factor authentication

Aside from you entering your credentials, require a second form of authentication for successful logins.

Perform a security risk assessment

Having an assessment will determine what safeguards should be in place that are currently not.

Perform updates

Software updates are often used to fix a vulnerability. Not performing regular updates can leave your business susceptible to an attack.

Recognize you are a target

EVERY organization is a target and no industry is off-limits.

To learn more about email security and cloud computing, check out these additional resources:

- [Cloud Migration Checklist for Strategic Business Considerations](#)
- [Quick Guide to Cloud Computing](#)
- [Cybercrime Infographic](#)

SCARY STATS!



of attacked businesses reported fraudulent emails



of attacked businesses aren't confident they could recover



of SMBs lack the skills in-house to deal with security issues

Sources: Cyber Security Breaches Survey, Fortune, The State of SMB Cyber Security

DECODING THE IT CODE WORDS

Advanced End-Point Protection - Protects systems from file, fileless, script-based and zero-day threats by using machine-learning or behavioral analysis. Traditional, reactive endpoint security tools such as firewalls and anti-virus software generally depend upon known threat information to detect attacks.

Anti-virus - Also known as anti-malware, is a computer program used to prevent, detect, and remove malware. Anti-virus software was originally developed to detect and remove computer viruses, hence the name. Anti-virus software is not comprehensive enough to protect business systems against today's threats.

Cybersecurity - Cybersecurity or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

Data Backup - In information technology, a backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. Backing up the business' data is the only real protection against data loss.

Disaster Recovery - Involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Cloud - A technology that allows us to access our files or services through the internet from anywhere in the world. It is a collection of computers with large storage capabilities that remotely serve requests.

Data breach - The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to see the information.

Encryption - The process of encoding data so that it can only be accessed with a key.

Hacker - An unauthorized user who attempts to or gains access to an information system.

HAFNIUM - A hacking group assessed to be state-sponsored and operating out of China, sought to be responsible for the Microsoft Exchange Server attacks beginning in March 2021. The Hafnium attacks are largely automated attacks that seek unpatched Exchange Servers.

Malware - An umbrella term that describes all forms of malicious software designed to cause harm, disclose information, or violate the stability of a system. Common forms include viruses, worms, trojans, spyware and ransomware.

Microsoft Exchange Server - A mail and calendaring server developed by Microsoft. It runs exclusively on Windows Server operating systems.

MSP (Managed Service Provider) - A third-party company that specializes in handling IT operations for organizations. Are responsible for the entirety or portions of the business' IT systems including managing the customer infrastructure and end-user systems, security and around-the-clock monitoring, issue resolution and reporting, and more.

Ransomware - A form of malware that encrypts files to deliberately prevent you from accessing those files on your computer – holding your data hostage. It is followed by a demand that a ransom be paid, typically in the form of Bitcoin (an untraceable digital current) in order to have the data decrypted or recovered.

Virus - A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

VPN (Virtual Private Network) - A communication link between systems or networks that is typically encrypted in order to provide a secured, private, isolate pathway of communications.

Zero-day attack - When hackers take advantage of a software security flaw to perform a cyberattack and there is currently no patch to fix it. There are “zero days” to fix the vulnerability because it's already been exploited.



Reach out anytime to ask a question or to
schedule a no obligation IT security review.

www.visualedgeit.com
(866) 863-2266

**VISUAL
EDGE IT**TM

SECURE TECHNOLOGY SOLUTIONS