SynchroNet

Beware That Which Lies In Wait

There are Monsters ‘Under the Desk’

Use this SynchroNet Guide to Identify the Wicked Things that Endanger Data Security and Employee Productivity

1800 North America Drive
West Seneca, NY 14224
(716) 677-2677
SynchroNet.net

The Inspiration for this White Paper

The threats we face are familiar to all of us—but often only in the abstract.

We know about hackers and cybercrime. We know that lack of maintenance and monitoring of systems can hurt operational efficiency. We know the importance of establishing security protocols and best practices for IT networks.

We understand all these things ... but nagging concern may eventually be dismissed as "something that happens to other people or other businesses." Sometimes it takes an actual event to refocus our attention on these real dangers; but it's much less painful to prevent an attack than deal with the repercussions.

For the purpose of discussion, we are going to look at the threats that are out there, the risks that they pose, and solutions for mitigating or preventing damage from malefactors or malfeasance. We have categorized the monsters in two sorts: those that are the result of ill-intentions; and those seem to arise of their own accord.

If you have any questions about the topics covered in this white paper, contact SynchroNet anytime at **716-677-2677**.

Sometimes it takes an actual event to refocus our attention on these real dangers; but it's much less painful to prevent an attack than deal with the repercussions.

First, a Ghost Story to Tell Around the Fire

Monsters are out there … lying in wait and plotting their attacks.

Recently, one of our clients brought a scary incident to our attention. Here's what went down. (We changed a few non-critical details for client privacy.)

The HR director of a fairly large company received an email carrying the name of the CEO. It was a request for employee payroll information, including date of birth and social security numbers. While the email recipient had the information at her disposal, she couldn't help but wonder why the "big boss" would need it. Fortunately, her curiosity got the better of her, so she picked up her phone and called the CEO. As it turns out, he knew nothing about it.

They looked at the email. The CEO's name, the director's name, the format … everything appeared as it should, so they contacted SynchroNet to ask us what was going on. At first, the message appeared to be legitimate; but then we noticed that the spelling of the company name in the CEO's email address was slightly misspelled. Cybercriminals were spoofing the real email domain in order to run a scam! Only the HR director's willingness to question her superior saved putting the sensitive employee records in criminal hands.

Type 1 Monsters: Evil by Design

It's no longer a surprise that there are evil experts who use the Internet to do your business harm. They are best categorized as cybercriminals. Their objective is to usually to take your money or your customers' money—though some seem primarily motivated by pure meanness. "Thanks" to the World Wide Web, these miscreants often operate outside the U.S. borders (Russia is a notorious hotspot for cybercrime) and tracking them down can be nearly impossible. When their 'evil-by-design' monsters manifest themselves in the realm of our daily routines, they will usually appear in the following forms:

- **Malware**
- **Ransomeware**
- **Social Engineering**
- **Phishing**

TYPE 2: Evil through Circumstance

Monsters can arise from within as a result of apathy, system entropy, insufficient information, or a lapse in processes. While none of these monsters are a direct product of some nefarious scheme, they are no less damaging to business productivity. In some respects, they may even more dangerous than external monsters; they come from systems that you may take for granted. The most common of these monsters (and their role in your business) include:

- **Outdated Technology (The Living Dead)**
- **Delinquent Patches and Updates (Werewolves)**
- **Inadequate Security Protocols (The Blob)**
- **Poor System Interoperability (Frankenstein's Monster)**

TYPE 1 MONSTERS

Evil by Design

Malware

We've all heard the horror stories about viruses. When a new virus appears on the national or international scene, it rapidly becomes headline news with companies warning employees and friends alerting friends through social media. (For instance, Mydoom, a computer worm affecting Microsoft Windows that originated in 2004, is believed responsible for $38 billion in economic losses worldwide over its lifetime.)

However, some malware is more like a gremlin than a virtual Godzilla. Consider the class of software categorized as "potentially unwanted programs" (PUPs). They may come loaded on your computer by manufacturers and generally cause little harm beyond occupying memory. Other, more intrusive PUPs however, often piggy-back on programs that you willingly download from the Internet if you aren't careful, and may change some of your browser settings—such as the search engine you use or your homepage.

Here is a SynchroNet mini glossary of malware terms:

Virus - A computer virus is a contagious piece of code that infects software and then spreads from file to file on a system. When infected software or files are shared between computers, the virus then spreads to the new host.

Spyware – Hackers use spyware to track your internet activities and steal your information without your knowledge or consent. Credit card numbers and passwords are the most common targets of spyware.

Worms – Similar to viruses, worms also replicate themselves and spread when they infect a computer. The difference between a worm and a virus is that a worm doesn't require a human or host program (like email) to spread. Instead, they self-replicate and infect networks without the guidance of a hacker or a file/program to latch onto.

Trojan – Like the Trojan horse from Greek mythology, this type of malware is disguised as a safe program designed to fool users who unwittingly install it on their own system. Generally, the hacker uses a Trojan to steal both financial and personal information. It can do this by creating a "backdoor" to your computer that allows the hacker to remotely control it.

Keeping Malware at Bay

Protocols against one type of monster will usually be effective against another, and the best ways to prevent malware from infecting your system are:

- Never open email **attachments** from unknown sources
- Install reliable **anti-virus software** and keep it updated
- Install a **firewall**, then make sure it's activated and working properly
- Automate precaution by setting up an **email filter** to filter out messages with .exe file extensions and also make sure Windows is set to show hidden file extensions. (Criminals often try to pass off .exe files as something innocuous, like a .pdf or .docx file)
- Stay away from questionable **websites** (some anti-virus software programs and browsers will warn you if you try to visit a site with a 'bad reputation')

A single piece of ransomware, CrytopWall v3, caused about $325M in damages worldwide over its lifetime.

Ransomware

One especially nasty form of malware is 'ransomware.' Usually transmitted by email, ransomware encrypts your computer files, thereby rendering them inaccessible. Once your files have been 'taken hostage,' you'll receive be a 'ransom note', either in the form of an email or a notice that appears directly on your screen.

Like a real-life kidnapping, you will be advised that you'll never see your files again unless you pay a sum of money. After making payment you (may) receive a code allowing you to decrypt your files.

Of course, we all know not to open attachments from sources we don't know. But ransomware won't appear in your email inbox as a message from some shady stranger. Instead, they may appear to be from a reputable company that you do business with, or they might claim to be from a government agency or well-known non-profit organization. The purveyors of ransomware also play upon admirable human qualities of curiosity or compassion to trick victims into downloading the virus.

The good news for ransomware victims—to the extent there is any—is that the cyber thieves behind these crimes will usually provide the code to unlock files once the ransom is paid. (After all, if victims can't hope to get their files back, they'll never pay.) Ransoms are usually a few hundred to a few thousand dollars—depending on the size of the company—because the cost of buying back file access has to be less than losing it.

Casting out Ransomware

Preventing a ransomware virus from infecting your system is, of course, the best strategy. In addition to reminding staff to remain ever vigilant against these attacks (download nothing unless you are sure of the source), anti-virus software may provide some protection. However, the best precaution is to back up important files in a secure and remote location.

If it becomes clear that your system has become infected by a ransomware virus, you'll have to evaluate how long you can be without the locked files before their loss become too damaging. Frustratingly, you may have no choice but to pay and hope the thieves let you have your files back. If time isn't of critical essence, IT forensic experts may be able to launch a counter-attack. In any case, you should:

1. **Disconnect** the infected system from the network

2. **Restore** copies of the compromised data from your backed-up files (if possible)

3. **Notify** law enforcement about the crime

Social Engineering

What exactly is 'social engineering?' You might think it has something to do with making business contacts, but no. This is one of the more nefarious cyber evils as it establishes trust solely for the purpose of ripping off a victim. Usually the perpetrator accomplishes this by assuming the identity of friends, family, co-workers ... or a company that the victim does business with. ('Phishing' is also a form of social engineering, but we'll discuss that separately.)

A social engineering scam may work like this:

You receive a phone call from someone who claims to be with 'Microsoft Software Support.' He wants to know if you've had any trouble with the new Windows 10 OS. (In this scenario, he's gambling that you have Windows 10. If you don't, he'll simply cut the call short.)

Once he has his claws in you, the caller may ask if he can run a diagnostic on your system to identify and fix bugs. This procedure will require you to give him remote access to your computer. If you go along, he can start rummaging through your files, gathering sensitive information, passwords ... whatever.

And once you and he finish your session, he can come back whenever he wants ... much like a vampire. Obviously, the best advice is, like a vampire, to never invite him in.

Defang the Social Engineers

Consider it a huge red flag if an unexpected caller or visitor asks: for credit card information; about your IT systems; about your passwords or applications; or about any matter that doesn't concern them. (If you've ever sat on hold for an hour waiting for technical support, you know companies don't go looking for customers to help!) If by some remote chance they seem legitimate, and the service or product sounds worthwhile, you still shouldn't make a move without first independently verifying their credentials (e.g., YOU look up their company's headquarters and call or email for confirmation yourself).

Make sure everyone in your organization—and especially gatekeepers—know about the threat of social engineering. Set rules for: sharing credit card information over the phone; signing in visitors to your office; and dealing with unexpected calls from vendors.

The more ingratiating the caller or visitor, the more cautious you should be when revealing data.

Fight ransomeware like a pro by following these important steps:

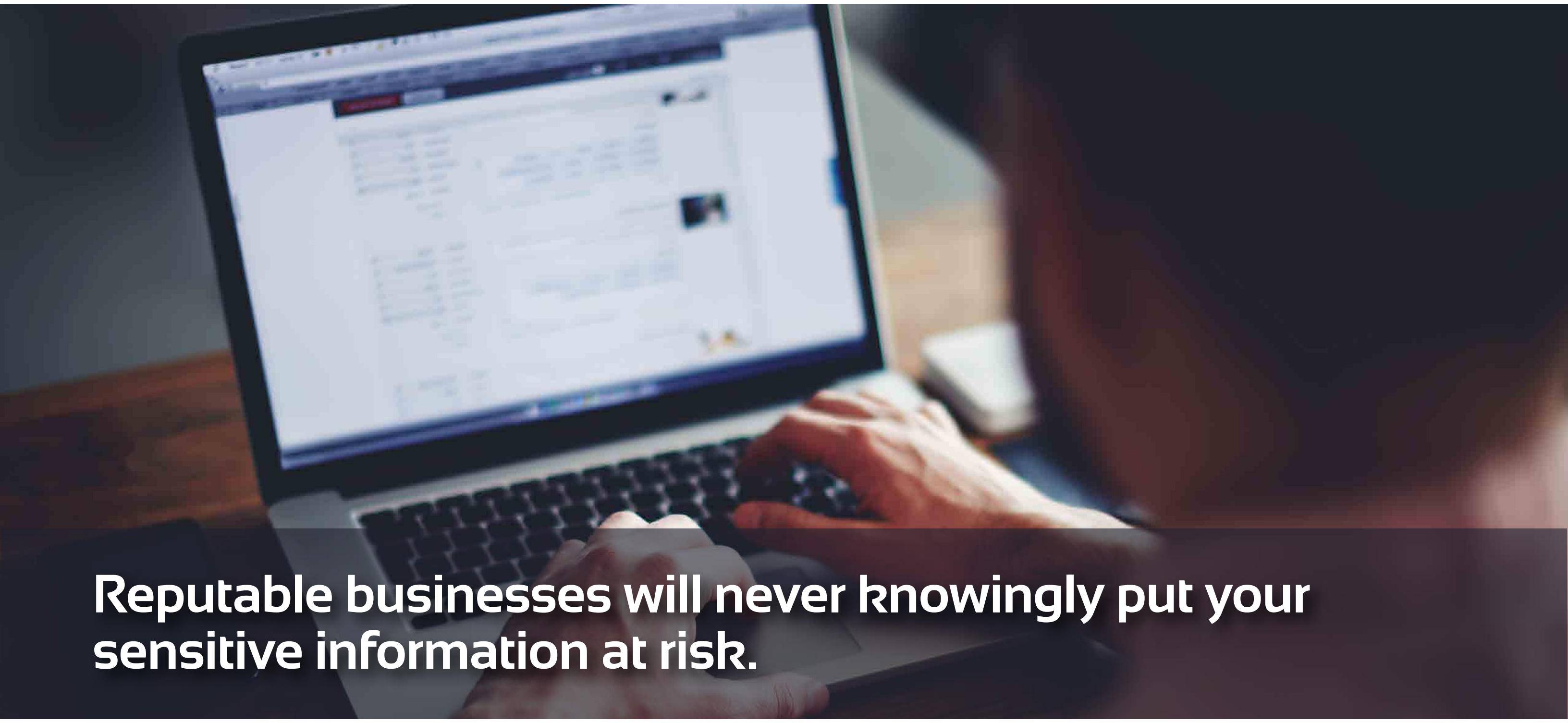
- If someone comes to your office posing as a workman, **ask for physical proof** of their identity and get a photocopy of their ID.
- It's also okay to **call the visitor's 'headquarters' or employer** to verify identity—especially if the person is unknown or the call was unexpected.
- It's important to **be skeptical** at all times because healthy skepticism breeds a more cautious attitude.
- Carefully **vet a caller or visitor**. Ask a lot of questions; a legitimate caller will patiently answer you while the social engineer will get nervous and hang up or leave.
- **Never allow yourself to be pressured.** Any offer or suggestion from a salesperson can—and should—wait for verification or authorization.

Phishing

You receive an email that appears to be from your bank. Certainly, the logo is correct and all the other branding looks familiar. The message ask you to follow a link to update your personal identification information and change your password on their recently upgraded online banking site. They apologize for any inconvenience. It may look legitimate, but chances are that this is a "phishing" attack.

- **Phishing is often by people who don't speak English natively** … and it shows. Look for errors: spelling, grammar, and syntax.
- **Don't just follow a link to check out a questionable site.** Scammers can set up fake SSL certificates and can easily spoof URLs.
- **Locate the organization's real Website via Google, Bing … etc.** and see what you can find out.
- **Don't be shy about contacting the real company.** Legitimate organizations will appreciate you letting them know that scammers have stolen their identity.

Reputable businesses will never knowingly put your sensitive information at risk, and they will never request it in a way that doesn't require two-way verification (also called two-step authentication): they prove who they are, and you prove you are who you say you are.



Reputable businesses will never knowingly put your sensitive information at risk.

TYPE 2 MONSTERS

Evil through Circumstance

Things that are neglected or abused frequently become monsters. And certainly this can become true of IT systems as well. Failure to provide adequate monitoring, maintenance and strategic management can spawn four particularly vicious creatures that devour productivity, staff morale, customer satisfaction and, of course, profitability. Coming to get you are:

Outdated Technology (The Living Dead)

We've all seen enough zombie movies to know that the living dead don't move or communicate very well, but they do bite. Likewise, hardware and software that's past its prime will fail to perform as necessary, and can also bring take a serious bite out of productivity.

Delinquent Patches and Updates (Werewolves)

If you ignore the warning signs of a full moon and forget your silver bullets, you are just asking for trouble. Software needs to be updated regularly to work correctly, but without conscientious scheduling, you may as well howl at the moon.

Inadequate Security Protocols (The Blob)

How many ways, and how many places, can threats ooze in and compromise business data and customer records? Weak passwords, unmonitored system access, absence of anti-virus protection … these failures may leave a wake of horror through your entire organization.

Poor System Interoperability (Frankenstein's Monster)

You can't just scavenge various parts and systems from a lot of different sources and expect them to work together. Smooth integration of network systems demands careful planning, understanding requirements and specifications, and experienced installation and implementation.

Type 2 monsters eat employee productivity and waste your precious resources.

Give Your Staff the Weapons They Need

Your IT network isn't just the hardware, software, channels and repositories that sort, send and secure vast amounts of data, or that command myriad aspects of modern business operations. Your network also encompasses managers and users who must also double as dragon slayers.

To enable the human component of your network to better fulfill their guardianship role, you need plans and processes that:

Drive Purpose – Every component of your IT network should be there for a reason. Know how the parts are supposed to help the whole (your company) achieve short or long term goals. This awareness will not only inspire you to make careful management of your system a priority, but it will also help you evaluate your IT investments.

Foster a Culture for Success – Communicate your policies and expectations to everyone in your organization. Provide training on using IT equipment and applications, including rules for when, where and how to properly work with—and within—your systems. You also need to make sure your IT professionals have the efficient, up-to-date tools they need to do their work.

Promote Efficiency – Encourage your IT staff to establish a logically planned work routine that allows them to fulfill ongoing duties as well as special-project obligations. They should also be able to block out sections of the calendar to create uninterrupted work time. Additionally, don't require unnecessary reporting, and automate routine procedures wherever possible.

Offer Development Opportunities – Be committed to keeping IT training and technical certifications up-to-date. Not only will this increase morale and confidence among staff, but as your team's IT skills grow, the value that they provide your company will increase as well.

Need help with these essential tasks? Call SynchroNet today at **716-677-2677** for more information.

SynchroNet's Proven Processes and Solutions for Monster Slaying

Business owners and managers—as well as their employees—are always going to serve as the first line of defense against the monsters that inhabit the IT realm. Yet without a first-class IT department on staff, evil of one sort or another is bound to materialize to threaten your systems … and possibly your entire operation. That's where **The SynchroNet Way** comes in.

The SynchroNet Way is all about smart, repeatable processes that ensure positive and desired outcomes.

Smart, repeatable processes … that is the approach we'll take in customizing a strategy and then helping you implement solutions to keep your business from harm.

The monsters are out there … and the monster slayers are here. SynchroNet's team of experts and implementation specialists are the cost-effective answer to your IT support needs.

It's time to get started. Call **716-677-2677** to schedule a free, no-obligation consultation and root out the monsters under your desk today. There's no reason to fear that which lies in wait when you're on **The SynchroNet Way.**

Among our many services offerings, we suggest the following as especially effective in destroying the monsters highlighted in this white paper:

- **Security Assessments and Protocols** – We'll identify threats, show you where vulnerabilities lie, evaluate risks, and develop a comprehensive plan of proactive protocols and effective countermeasures.
- **Managed Services** – We monitor, maintain and help protect your computer systems and applications from harm, and work to ensure that they operate a peak efficiency 24/7.
- **Business Continuity** – We offer solutions to protect critical information and disaster planning that prevents costly system downtime.
- **E-mail Management** – We'll work with you to prevent email from bcoming a security risk or a drain on productivity while enhancing its inherent indispensability.
- **Hosted Solutions and Cloud Computing** – We have the expertise and resources to help your organization utilize great software without the hardship of managing and maintaining the equipment those applications require.
- **Secure Remote Access Solutions** – We'll cover all aspects of security, connectivity and mobility in devising, implementing and managing a remote access solution for your organization.
- **Technology Upgrades and Patches** – We put your company's needs and goals first in helping you take advantage of latest advances in technology.
- **HIPAA Best Practices** – Indispensable to healthcare services providers for meeting guidelines regarding the electronic records of patients, many aspects of this offering are applicable to businesses that frequently work with sensitive data … like yours.

You can defeat the monsters threatening your business! SynchroNet is here to help you every step of the way.

If you'd like to schedule a free, no-obligation conversation to learn more about **The SynchroNet Way** and what it can do for your business, just call **716-677-2677** today.