THE SMALL BUSINESS

CYBER THREAT CHECKLIST

There is one major drawback to our internet-centric culture: Your business faces more threats than ever before.

Threats are defined as malicious actions that act on your company's vulnerabilities with a determinable likelihood and negative consequences. To understand these threats, we must discuss the different attack vectors that can be exploited—and the consequences of failing to address them.

The Biggest Threats Your Business Will Face

Cyber attacks are serious concerns for any organization, but are particularly dangerous for medical and dental practices. Medical offices are fast paced and bound by complex HIPAA privacy laws. Practices risk being held liable when patient information is lost or stolen; this can mean steep fines, loss of business partnerships, and damage to reputation.

And system downtime is just as serious. **Should a healthcare clinic's system go down, it disrupts schedules, planned appointments, and each patient's ability to get the care he/she needs.**

If a system gets brought down by a cyber threat shortly before a patient's appointment, their treatment may need to be delayed until the clinicians can safely access the patient's records again. Naturally, this seriously damages the relationship the clinic has built with its clients.

Timing of these events can further increase the impact. Just think of how damaging system downtime can be when it occurs near periods of peak insurance filing, such as the end of the year. Patients often rush to schedule appointments with practitioners before their insurance "resets" at the turn of the year; if a clinic's system goes dark during these critical windows of opportunity, patients will be understandably frustrated—and will likely turn to another provider who can keep its promises!

Patient trust is hard to gain, yet easy to lose. Once it's lost, it's nearly impossible to get back.

To protect your business, you need to be aware of each type of cyber threat that could potentially affect your company.

Use this checklist as an overview of the most common types of threats.

Knowing the possibilities will help you take steps to protect your business from them:

☐ Outdated Software and equipment

According to the Wall Street Journal ***"Several companies have suffered more than $100 million in lost revenue over the past year due to a common and frequently overlooked cybersecurity issue: outdated software."*** The article, published in May 2018, highlights how companies struggle to stay on top of security patches that are crucial in protecting them from such revenue loss. In addition to outdated software is outdated equipment; computers, phone technology, servers, routers, etc. which increases vulnerability.

☐ Malware

Malware is defined as any type of malicious software designed to corrupt, disable, or infect a computer system. Malware has increased substantially over the years, with AV Test registering nearly 800 million different malware applications as of 2018. Depending on the severity of the threat, a malware infection can be anything from a minor inconvenience to a serious concern that requires a complete shutdown of the system.

Spam

Spam is generally defined as unsolicited and un-personalized email communications. While spam itself isn't dangerous, it's a common way to deliver malicious code to large numbers of users.

Employees mailboxes filled with spam increases your exposure to this type of attack.

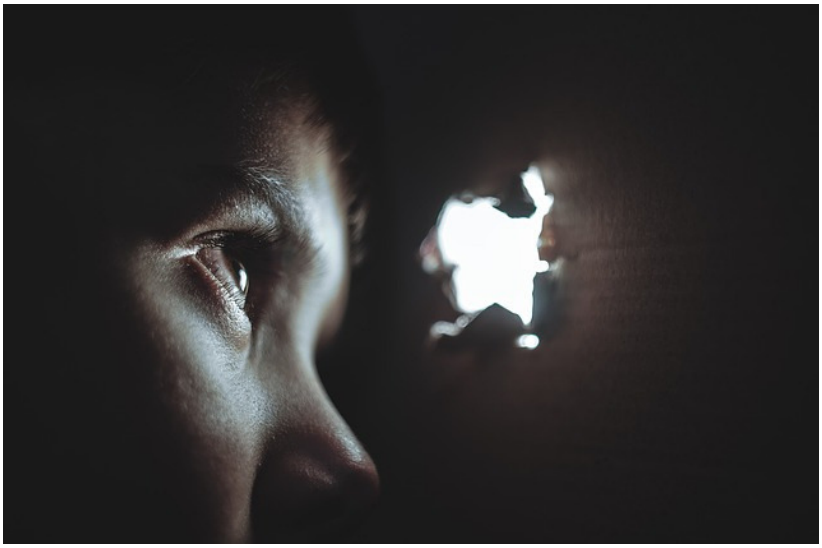
Spoofing

Spoofing attacks occur when users falsify data to present themselves as someone else. The goal of spoofing is to get a user to take an action (such as opening a malicious email or link) that quietly downloads malware into their system. In 2016, the German manufacturer Leoni AG lost $44.6 million to thieves who had spoofed professional credentials.

Phishing

Similar to spoofing, phishing occurs when users misrepresent themselves to access secure systems. The difference is that with phishing, the goal isn't to infect systems with malware, but to trick users into providing sensitive data on their own. Spear phishing is a variant of this, where fraudsters customize attacks to specific users based on data they gain elsewhere. This attack is common for businesses—**as many as 76 percent of businesses reported phishing attacks in 2016.**

Snooping



Snooping is the eavesdropping of cybersecurity. This occurs when unauthorized users gain access to protected information by viewing an open email on a coworker's computer or stealing a login to view their emails.

It can also include more sophisticated processes, such as malware that remotely tracks user activity.

Social Engineering

Social engineering involves manipulating users into giving up personal data. A common example would be a fraudster attempting to break into someone's account, learning which security question they're using for password recovery, then going on social media to mine that data.

Ransomware

Ransomware is a nasty form of malware that infects a system, locks out the user, and demands that the victim make a payment to an outside account in exchange for release. The highly-publicized WannaCry and NotPetya attacks of 2017 are two examples, affecting hundreds of thousands of systems across the world. This type of attack has grown in popularity over the past few years, with Kaspersky estimating that one out of every five businesses were affected in 2016.

Ransomware is particularly dangerous for medical practices, as a full-scale ransomware attack can render an entire clinic's system inoperable from a single breach. Until the threat can be handled, the clinic has no way to look up records, call patients to reschedule appointments, or access critical health information that may be requested by other offices.

Identity Theft

Identity theft is more common than ever thanks to the wealth of personal data we put online. These attacks occur when fraudsters locate personal details and then open new accounts in the victim's name—usually in the form of a credit card or loan. In the worst-case scenario, these fraudsters can empty a user's bank account and abscond with the funds before the victim is aware of the issue. According to one report, as many as 16.7 million people were victims of identity fraud in 2017.

Compromised Web Pages

Legitimate web pages can be turned into attack vectors without even realizing they've been affected. This is most often done through malicious code inserted into banner ads. When a user loads the webpage, the code copies itself into the viewer's system and gains access to its data.

Email Interception

Email traffic isn't always as secure as it seems. With a bit of technical know-how, fraudsters can set up email interception tools that let them view "private" emails being sent on someone else's server. This is a serious threat to medical offices who coordinate patient details and information among third-party clinics and insurance providers.

Keystroke Logging

Software exists that can record keystrokes and transfer the data to a central collection point. This gives hackers easy access to login credentials, passwords, and any data entered through the computer's input device. By the time users realize what has happened, the damage is done. Adams County Wisconsin suffered such a data breach in early 2018. An employee was arrested and "the warrant alleges that she installed a computer logging tool and captured keystrokes from the county's computers."

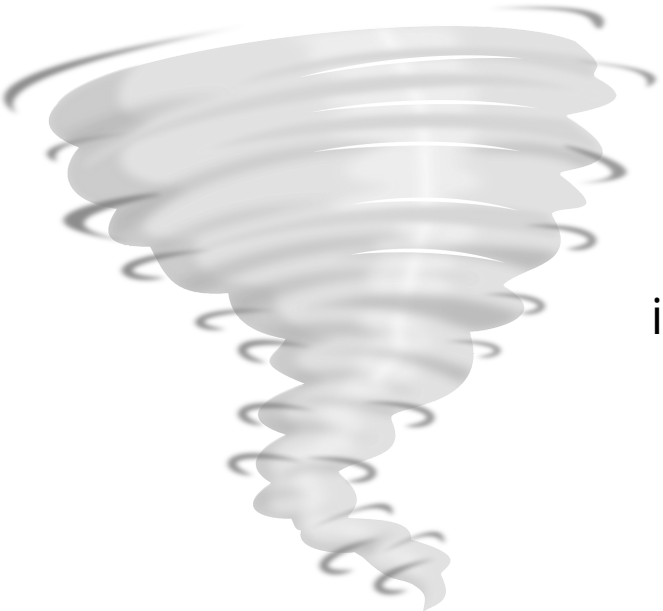
Malicious Actions

Malicious users can attack businesses in ways that are hard to prevent. These may include employees stealing data for competitors, changing passwords, or abusing their privileges to take revenge on a company. The attacks are difficult to prevent but your company should engage every possible safeguard to prevent them.

Human Error

Attacks aren't always intentional. Users can leave their businesses vulnerable by accident and create weaknesses for others to exploit. In most cases, humans are the weakest link of any security chain. Consider research showing that up to 56 percent of email recipients will click links from unknown senders—even while claiming to understand the risks of virus infection!

Natural Disaster



Natural disasters such as tornadoes, fires, or floods can damage your company's devices, servers, and infrastructure. In 2017, the U.S. saw an estimated $649 million in property damage from tornadoes alone.

Disasters are common causes of downtime, as large-scale catastrophes can completely destroy a company's IT infrastructure. And as our world becomes more connected, the risks increase—a medical clinic in New York, for example, may be receiving computing services from servers in Florida. Should a hurricane strike these servers, the New York clinic may go dark.

Protecting Your Enterprise

There are threats on all sides. How can you protect your organization? We recommend starting with a thorough assessment of your business's cybersecurity policies, procedures, and infrastructure. This is an important part of taking a proactive approach to data security, but it's also crucial for developing disaster recovery strategies should breaches occur. Let us give you a hand with a free IT audit.