IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER:

7 WAYS WE SHIELD YOUR BUSINESS FROM CYBERTHREATS

Sunset Technologies

Rest Assured.

INTRODUCTION

As your practice becomes increasingly more digital, you're using more systems and running more applications to manage day-to-day operations, share critical information and complete vital tasks. All of these different devices, back-end systems and applications generate an exchange of overwhelming amounts of data and this will only continue to increase.

A multitude of different data sources presents risk; they have potential vulnerabilities that make your practice an easy target for cybercriminals and ransomware.

Your ePHI and patient data, as well as financial information, may be exposed and, therefore, vulnerable to an attack.

The increasing number of employees working remotely and on-the-go has created more risk, too. The BYOD (bring-your-own-device) movement is on the rise, and that's making things easier for the hackers.

> Sixty million computers will fail in the next 12 months, and only 1 in 4 laptops are backed up regularly.[3]

When your employees exchange critical business data using smartphones, tablets and personal laptops, they are especially vulnerable to cybercriminals. They can easily download malicious applications that will infect their devices and hold data hostage.

That's why we believe in the power of a sustainable and repeatable seven-layer process to protect your practice from ransomware.

BY 2020, REMOTE WORKERS WILL ACCOUNT FOR **72%** OF THE U.S. WORKFORCE.[2]

NEW CYBER THREATS POSE NEW SECURITY REALITIES

When thinking about cybersecurity; it's not just about "if" your practice will be attacked; it's about "when" it will be attacked. Infection methods are more sophisticated and phishing scams look more realistic. Two of the more relevant ransomware attacks serve as valuable evidence.

In May 2017, a phishing scam posed as a Google Docs request. When people clicked a link within the email, the hacker was able to access all their emails and contacts, as well as send and delete emails within the accounts.

> The attack compromised more than 1 million Gmail accounts.[4]

PayPal accounts were also targeted with a highly sophisticated phishing scam that asked people to take a selfie while holding credit cards and a form of identitification.[5]

Why were these attacks so successful? Because people immediately trusted the emails they received. By leveraging the logos and powerful brand recognition that Google and PayPal have, the creators of these attacks were able to catch people off guard and, in turn, infect more devices.[6]

Perhaps the most destructive ransomware thus far is WannaCry, which also has worm-like capabilities. While ransomware typically limits infection to the device that clicked and installed it, malware like WannaCry can spread across a network and replicate itself onto other devices.

Once WannaCry infects a device, it finds and encrypts files, displays a “ransom note” and demands bitcoin payment from infected users.

> Reports indicate that the ransomware strain has spread to 150 countries, impacting 10,000 organizations, 200,000 individuals[7] and 400,000 machines.[8]

Recently, a new variant of WannaCry has emerged infecting 3,600 computers per hour. [9]

These occurrences reaffirm that cybercriminals are more clever than ever, their targets are larger, and their attack methods are more aggressive. We want to help you be prepared in the event ransomware infects your devices and, most importantly, minimize or prevent critical PHI from being stolen.

SMALL BUT DEADLY:
THE ANATOMY OF RANSOMWARE

With attacks like WannaCry dominating media headlines, it's easy to believe that the cybercriminals that design these viruses have a lot of time and resources. But the truth reveals the contrary:

- Ransomware attack kits are free to download online.
- Anyone can create a new strain of ransomware within hours.
- Virus protection can only detect **existing** ransomware.
- Because new viruses are being developed every day, a virus checker needs to be used in conjunction with File/Folder Continuous Backup to provide the highest level of security.

OUR SEVEN-STEP APPROACH TO KEEPING YOUR DATA SAFE

Much like biological viruses, there are many ransomware threats circulating the web. Some are well known, some are new, and others not yet known or developed. With every occurrence, the sophistication of these viruses increases in a multitude of ways, including how they spread and how they encrypt data.

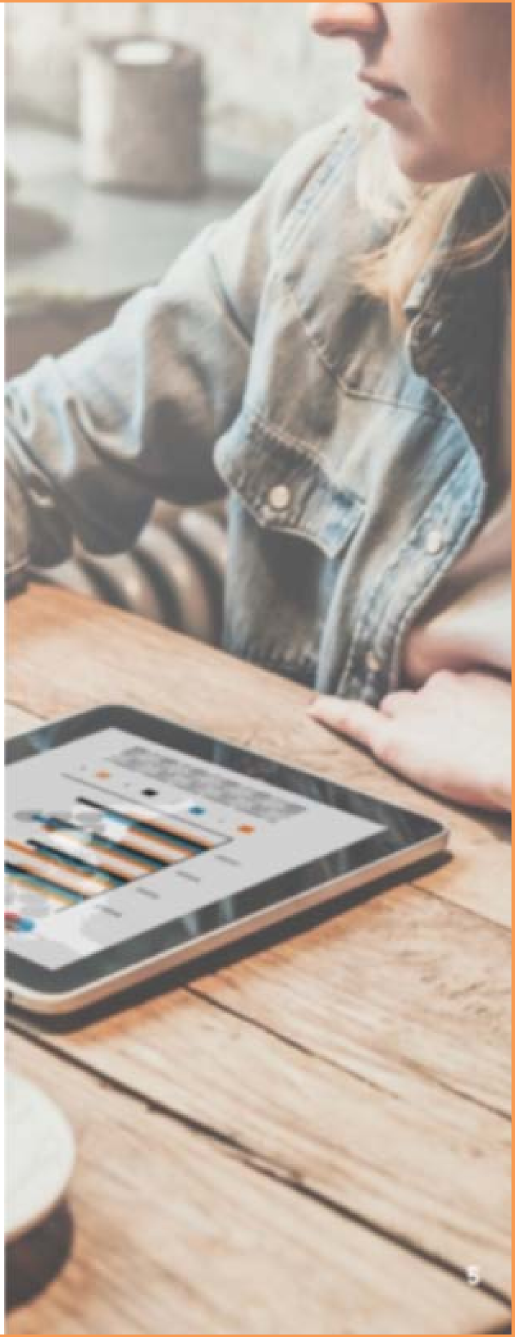
As your Technology Partner, we know that protecting your practice from ransomware is not a single-pronged approach. Being able to mitigate or prevent attacks is our top priority. We have put in place an agile, multi-layered approach that can adapt as new and increasingly hostile threats emerge. At Sunset, we begin with our **Five Pillars of Protection:**

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

Within these Five Pillars, we have tools we use as part of our overall protection package. Following are seven ways we help protect your practice:

1 INVENTORY (Identify)

The best place to begin any security effort is to know all the pathways of entrance for a cyber-criminal. In short, you must know all the devices and connections that are in your environment. It is also critical to keep your IT partner up-to-date on any changes. Many times, customers will simply plug a "new thing" into the environment without telling their IT partner. This introduces risk as a possible new doorway for cyber-attacks.



2 EDUCATION AND AWARENESS (Protect)

The most important step in our process is to create awareness about these threats. We offer training and education to help your employees understand about cybersecurity risks, new ransomware strains and best practices for spotting phishing attempts, suspicious emails, and other security risks. Empowering and encouraging them to be proactive increases awareness and decreases overall risk.

3 ANTI-VIRUS/MALWARE & NETWORK MONITORING (Protect & Detect)

People are being targeted through more sources than ever – email, ad networks, mobile applications, and devices. Anti-virus/malware and network monitoring examines all files and traffic, then filters them against all known threats. We keep virus definition files updated to protect these systems.

4 PATCHING (Protect & Detect)

The most basic layer of protection is to monitor and patch all computers and applications. Utilizing the latest patches, we can address all known operating system vulnerabilities. The patching process provides this basic layer to operating systems, especially once a security flaw is uncovered. We provide the latest patches to ensure your systems are running at peak performance and that all system vulnerabilities are addressed.

5 FIREWALL WITH INTRUSION PREVENTION SYSTEM (IPS) (Protect, Detect & Respond)

Every firewall provides a layer of protection; however, our IPS supplements the predefined rules of the firewall filter. It inspects communications and analyzes traffic patterns in real time to detect malicious activity and prevent attacks. This dual function has a significant impact on business security, reduces cost as it simplifies device management, which in turn increases business profitability.

6 DISASTER RESPONSE PLAN (Respond)

As business owners, we don't have insurance because we plan to use it; we have it in case of an emergency, so we are prepared. The same can be said for creating a disaster response plan. It is essential in mitigating the fallout from a breach. A proper response plan starts with a complete inventory as discussed earlier. It will also include making sure all devices are scanned and passwords changed, logs reviewed and saved for forensic analysis, and confirmation that all systems are operating as expected. A complete response plan should also include an **approved** communication plan that covers both internal and external entities.

7 BACKUP AND DISASTER RECOVERY (Recover)

There is sometimes a gap between when a threat is first introduced and when we receive notification and can develop a remedy. We do a full-system backup to protect your back-office systems. This enables us to stay on top of things when an attack occurs and provide a recovery option for unknown threats in even the most catastrophic failures.

WE PROTECT YOUR PRACTICE WITH A COMPREHENSIVE SOLUTION

New ransomware threats are constantly emerging and evolving.

To learn how we can protect your practice and provide a secure and collaborative environment for all your employees, contact us today.

www.sunsetsecure.com
ph: 855-861-8833
RestAssured@sunsetsecure.com

SOURCES

1. http://zdnet.com/article/research-74-percent-using-or-adopting-byod/
2. BusinessWire.pressrelease: “IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020” June 23, 2015
3. World Backup Day
4. Recode, “More than a million people were affected by the GoogleDocs phishing attack” May 4, 2017
5. International Business Times, “PayPal Phishing Scam: Victims Asked to Take Selfie With Credit Card, ID” June 6, 2017
6. Autotask, “Expert FAQ: What you need to know about WannaCry” May 18, 2017
7. The Verge, “The WannaCry ransomware attack has spread to 150 countries” May 14, 2017
8. Barclay, “WannaCry Ransomware Statistics: The Numbers Behind the Outbreak” May 2017
9. ZeroHedge, “New Variant of WannaCry” Virus Emerges Infecting 3,600 Computers Per Hour” May 15, 2017