A Guide to Understanding & Resolving

THE 5 BIGGEST BUSINESS TO IT HEADACHES

in Medical Private Practice

PACIFIC NORTHWEST
MANAGED I.T. SERVICES

6848 N Government Way, Suite 114-47
Coeur d'Alene, ID 83815-7719
Phone: 208-449-1133

- Electronic Health Records Management entry and integration?
- HIPAA compliance needs and actions?
- Internet and Application Security?
- Secure Data backup and Recovery?
- Dropped calls, poor call quality, little integration, high expense?

SO, TIRED OF INFORMATION TECHNOLOGY (IT) YET?

If you are like most business folks, the answer is a resounding yes. Not necessarily because IT is a bad thing, I mean, where would your business be without IT technology? Producing documents, spreadsheets, virtual meetings, training videos, project management, presentations, finances, manufacturing automation and the list goes on and on. Truly, information technology has and continues to be a part of our personal and work lives. The question we should really be asking ourselves however is this; Is my business driving the information technology we use or is the information technology driving the way we do business. A close examination of your current operation may find that you are more driven by your technology then by the way you want to operate your business. This guide reviews this question and then dives into the 5 BIGGEST Business to IT Headaches in Medical Private Practice. The review will help you decide whether the dog is wagging the tail or the tail the dog, if you know what we mean.

The title of this guide subtlety hints at one of the BIGGEST problems in Business today, did you catch it? Business to IT Headaches. In over 33 years as an IT manager, engineer, SWAT team member, operations manager and analyst, the single hardest issue confronted is Business to IT connectivity. No, not in the technical bits and bytes, I got your email, text, or whatever scenario, but rather, in the desire to have technology

service the business culture, processes and goals. Here is how it normally works. Executives drive the vision of where the company should go, what it services, sells, what it researches…etc. Others then take that vision and break down into departments, projects, timelines, budgets, launch dates and so forth. Along this matrix of vision breakdown is the IT department and what they can do to expedite processes with automation, communication, management helps that will cut time to market. All of this done with the HIDDEN culture that whispers, the executives are really suits that dream about things that cannot really be done, and the IT guys are just geeks that don't really understand the needs of business. The truth, both have some validity and thus the problem of yesterday is still the problem today and the result is that business never operates fully the way it wants to, and technology seldom really hits it full stride in understanding and accomplishing the needs of business. Business is constantly working to improve and recreate itself while IT continues to evolve to resolve. Looking for examples, let us look at the 5 BIGGEST Business to IT Headaches in Medical Private Practice and how to resolve them.

1 ELECTRONIC RECORDS MANAGEMENT OR ELECTRONIC HEALTH RECORDS

This may be one the best examples of how Business to IT connects or dis-connects as the case maybe. The business case is one of the needs for better accuracy and speed in diagnosis, prognosis, prescription, and overall treatment. There is no doubt we have come a long way from clipboards, telephone calls and medical file folders in tracking health conditions and treatment. Well, let us say many have, there are still those who resist technology for personal touch and commitment, service, and privacy sake. They prefer the human touch all the way through the process, fair enough and like anything

else, if it's not broke, do not fix it. We could argue about the virtues of both sides, but today were specifically focused on the Business to IT connection, what private practice wants, and the connection of technology meets the wants and needs.

Private medical practice today consists of health care professionals on many different levels and specialties all woven together to meet the health care needs of those they serve. The general family practice must connect to other private specialty practices, clinics, and hospitals to take care of their patients. The very nature of this connection means a lot of disparity in understanding and communication. Now just for a moment, let's imagine a patient with migraine headaches. The family doctor makes a general exam that includes, height, weight, blood pressure, close review of symptoms, how long they have existed, when do they start, end, your diet and various other related or perhaps non-related questions. The migraine is aimed more towards neurology than family medicine, right? So just to make sure he orders up an MRI to ensure the neck is good shape. Now, the fun begins, how to get the exact information to the MRI lab so that the right pictures are taken. The family doctor has the file in digital format residing in one of many different EHR applications. He soon discovers that he cannot just transfer the file to the lab without some type of consideration. Why? Because the lab is using a different record system that is not completely compatible and transparent to his. This means that some form of translation or change is needed to get it there. This may be as basic as sending it via email or fax, however the real issue is having the information in the labs system if needed moving forward and even more important is getting the lab results back into the family doctor's system transparently and securely. Multiply this by the number or specialist and or hospitals within the case by the diversity of EHR systems being used. There is a universal standard for file sharing, HL7, but that has morphed to several and can bring the same issue as described above.

What happens is manual entry to make up the gap. In most cases 1 hour for every 2 – 3 hours of patient time or more depending on record input. Remember, this is all to increase speed and accuracy of health care.

Certainly, technology has moved patient care a long way including records creation, sharing and security. The scenario above reflects additional evolution that needs to happen to meet total resolution. Software development is normally more evolutionary in the overall resolution, so we are sure the gaps of today will become the features of tomorrow.

In terms of today, we are working to expedite the issue of transparent file sharing by researching and developing various API's that will enhance file transaction among different EHR systems. The goal is to bring a more fluid bi-directional synchronization with patient files, allowing for less manual handling and transfer. Secondly, we are constantly looking at current and new systems that are less proprietary with a focus on working the way heath care specialist works, rather than forcing business operations to mold to the way of the application.

2 HIPAA COMPLIANCE

What does HIPAA stand for? **Health Insurance Portability and Accountability Act of 1996**, or the Act for short. HIPAA is comprised of a US privacy law to protect medical information like patients records and allow for secure and confidential communication between patients and medical professionals.

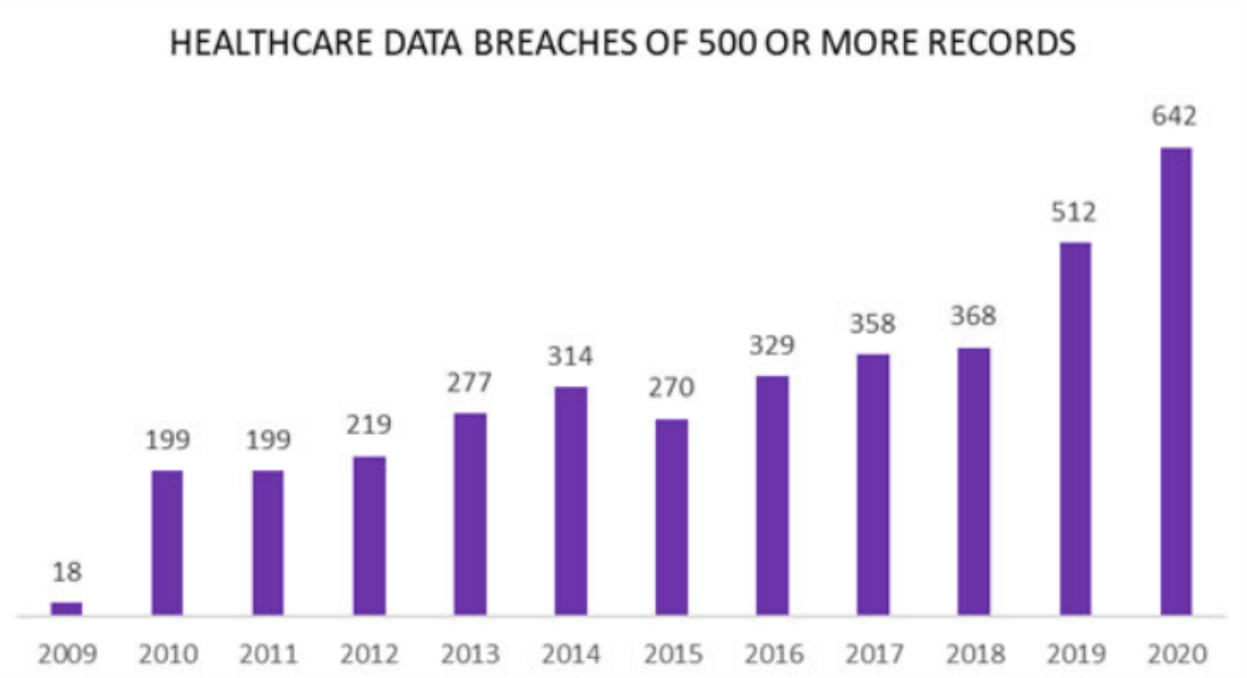
HIPAA has two main objectives specified in Title I and Title II of the act. Title I centers on health care access, portability, and renewability and protects health insurance coverage for workers and their families when they change or lose their jobs. Title II focus is preventing health care fraud and abuse, administrative simplicity, and medical liability reform.

HIPAA laws state that health providers must take responsibility for the authorized disclosure of **Protected Health Information** (PHI) but does not disclose that notice of breach of such information has to be provided to the individual(s) records that were breached. In February of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) was enacted and significantly changed HIPAA simplification measures. Under HITECH regulations, breaches must not only be disclosed to individuals, but when 500 or more individual's information is breached, notice must also be sent to the Department of Health and Human Service (DHHS) and the media. HITECH also increases the civil penalties for non-compliance and gives more enforcement.

In private practice, HIPAA HITECH means scrutiny of Private Health Information (PHI) security, transport, storage, and use. More regulation in billing and encourage use of technology for better compliance. All of this brings complexity to the practice while it guarantees certain protections to individuals. The implementation of HIPAA HITECH, when implemented at different levels in practices, is often based on personal understanding and not on professional analysis. This, of course, can lead to non-compliance and breach of health information.

Healthcare Data Breaches by Year

Between 2009, (the year HIPAA was enacted) and the end of 2020, 3,705 healthcare data breaches of 500 or more records were reported to the Health and Human Services Office for Civil Rights. These breaches resulted in the loss, theft, exposure, or intolerable disclosure of 268 million + healthcare records. This equates to more than 70% of the U.S. population. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. In December 2020, that rate had doubled.[1]



First question to ask: “How many patient files are at risk in my practice?” Normally that answer will exceed 500 easily. A breach at this level means public notification and media disclosure, Ouch! Many, if not most, private practices would have difficulty weathering that storm. Wait there is more. The HITECH ACT enforces penalties for HIPAA violations based on a tier score.

New Interpretation of the HITECH ACT's Penalties for HIPAA Violations

Penalty Tier	Level of Culpability	Minimum Penalty per Violation	Maximum Penalty per Violation	Old Maximum Annual Penalty	New Maximum Annual Penalty
1	No Knowledge	$100	$50,000	$1,500,000	**$25,000**
2	Reasonable Cause	$1,000	$50,000	$1,500,000	**$100,000**
3	Willful Neglect – Corrective Action Taken	$10,000	$50,000	$1,500,000	**$250,000**
4	Willful Neglect – No Corrective Action Taken	$50,000	$50,000	$1,500,000	**$1,500,000**

Understand, these fines for non-compliance are per offense and can lead to a maximum of 10 years of imprisonment. Additionally, a maximum penalty across all four tiers was set at $1.5 million for violations of an identical provision during a single year.

Most private practices are conscientious and working to be compliant. Tiers 1 and 2 speak directly to their efforts. Tiers 3 and 4 reflect those who willfully neglect and either act or do not. In either case understand that the economic, business, and personal reputations are severely damaged if not destroyed.[2]

Now that you have a good understanding of HIPAA, the importance of compliance for the protection of private health information, what is the business to IT connection that is so important and how should you handle it? In a single word it is compliance. Is your private practice completely HIPAA compliant, how do you know, and what process do you have in place to ensure it stays that way?

10 Most common HIPAA Violation & Resolutions

1. **Keeping Unsecured Records**
    a. Physical files containing PHI should be locked in a desk, filing cabinet or office. Digital files should require secure passwords to access them, in addition to being encrypted whenever possible.

2. **Unencrypted Data**

    a. Encrypting the data is added protection if a device containing PHI is lost or stolen. It offers an additional layer of security if a password protected device is somehow accessed, such as through hacking.

3. **Hacking**

    a. Keeping antivirus software updated and active on all devices containing ePHI is a great place to start. Using firewalls adds another layer of protection as well. Finally, creating unique and difficult to hack passwords, then changing them frequently.

4. **Loss of Theft of Devices**

    a. A single cell phone from the Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) was stolen in June of 2016. A combination of nursing home residents and family members totaling 412 people were affected by the data breach, and the facility was fined $650,000. Devices containing ePHI need to be always stored in a secure location, they are subject to the possibility of loss or theft. If the information stored on such devices is not encrypted or password protected, the loss or theft of the device becomes an even more severe issue.

5. **Lack of Employee Training**

    a. Employee HIPAA training is more than a recommendation - it is a requirement of the HIPAA law. All staff members must be well-trained on the law, as well as on the policies and procedures set forth by your individual practice.

6. **Gossiping / Sharing PHI**

    a. Keep conversations about PHI behind closed doors, and only with appropriate office personnel. There are hefty fines for sharing such

information either directly or indirectly with unauthorized personnel who may be listening.

7. **Employee Dishonesty**
    a. While seldom done with a malicious purpose, when employees try to access PHI that they are not authorized to view, this is a HIPAA violation. Precise training that outlines who can access what, as well as consequences that will result, can help prevent occurrences of this HIPAA violation.

8. **Improper Disposal of Records**
    a. Staff members should understand that all information that contains PHI, such as social security numbers, medical procedures, diagnoses, etc., should be shredded, destroyed, wiped from the hard drive, etc.…

9. **Unauthorized Release of Information**
    a. This occurs when medical personnel release PHI to family members that are unauthorized. Only dependents and those with a Power of Attorney are allowed access to the PHI of a family member.

10. **3rd Party Disclosure of PHI**
    a. If you have access to PHI and discuss it with those who do not have the right access to this information is a direct violation of HIPAA. Discussing PHI with people without access happens frequently. Through proper education to all staff, you can eliminate most of the data breaches caused by this violation.

Resolving the HIPAA Headache

Given all that we have discussed, you can see that HIPAA compliance is very important to patients and business. The complete resolution of HIPAA concerns will come with the following:

Initial and regular HIPAA analysis which includes:

1. Physical and electronic security measures.
2. Audit of PHI handling process and physical checks.
3. Employee training and continued review.
4. Management Staying up to date on changes to HIPAA compliance rules.

Keeping these four issues close at hand will negate most HIPAA issues and keep you in compliance. Because of human nature it will be impossible to keep 100% clean all the time, but frequent audits, bi-annually or quarterly, will serve as a great help in all HIPAA compliance matters.

HIPAA trained individuals will be required to train staff, and HIPAA professionals, whether internal or external should be part of the regular audit cycle. Of course, there is some cost involved to ensure compliancy, but the cost is negligible compared to fines and /or loss of reputation and business.

3 INTERNET + APPLICATION SECURITY

"A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network."[4]

Did you know that more than half of all small businesses suffered a cyber security breach within the last year with the average cost of $200,000 for each breach, ouch! Did you know that forty-three percent of cyberattacks are aimed at small businesses, but only 14% are prepared to defend themselves?

Former Cisco CEO John Chambers once said, “There are two types of companies: those that have been hacked, and those who don’t yet know they have been hacked.”

So where does your private practice fall? All of this may sound like scare tactics to get you to use a service, but I assure you that all that we have addressed thus far in this guide is real, with actual and real consequences. The truth is, we are only one breach away from significant damage to our businesses, our patients, or customers and the possible ruin of our reputations. Those who listen the least, suffer the most. Let’s talk about cyber and application security.

MOST COMMON CYBER ATTACKS:

MALWARE:

Malware, short for malicious software, includes spyware, ransomware, viruses, and worms. Malicious software (Malware) breaches a network through some type of vulnerability, typically when a system user clicks on a link or email attachment that installs the software. Once the software is installed, malware can do the following:

1. Block access to key components of the network, locking production down and then asking the company or user for a ransom to release the blockage. **(ransomware)**
2. Install malware and or additional harmful software such as **viruses**.
3. Behind the scenes, without detection, obtain information by transmitting data from the hard drive **(spyware)**
4. Disrupt physical operation, such as system bios, application layers, or other components that render the system inoperable.

PHISHING:

Phishing is a common practice of sending fraudulent communications that appear to come from a reputable source. Usually done through email, the goal is to steal desired data such as credit cards, login information and is often used to install Malware on the user's machine.

Cybercriminals start by identifying a group they want to target. They then create email and /or text messages that appear legitimate but contain malicious links or attachments. These links and attachments, lure or trick their targets into taking unknown and risky actions. In brief:

1. Phishers often use human emotions such as fear, urgency, or greed to entice recipients to open attachments or to clink on the links sent in the email.
2. Phishing attacks are purposely designed to look as though they come from legitimate companies and /or individuals and thus successfully deceive many who review such communications.
3. Please note: It only takes one successful phishing attack to compromise your network and steal your data.

There are many different types of phishing attacks. We would refer you to our website to read an entire article on phishing written by Cisco.

Seven tips to help in prevention of phishing attacks.

1. Closely monitor your online accounts regularly
2. Keep your browser updated as security packs are often added to thwart phishing attacks.
3. Do Not click on email links from sources you are not familiar with, period.
4. Beware of pop-up windows that can be an element of trigger. Ensure the popup is familiar and authorized.
5. DO NOT give out your personal information over email.
6. Be careful with emotional or social driven lures, (attachments or links) that appear in an email regardless of who they are from.
7. Examine email hypertext links by ensuring the destination URL equals what is in the email. Also watch out for strange characters in links or strange abbreviations.

No single cybersecurity action will avert every phishing attack your system receives. Reports show that employees in smaller organizations are more likely to receive malicious type emails. “Organizations with 1–250 employees, roughly one in 323 emails will be malicious. For an organization of 1001–1500 employees, the rate is far lower with one in 823 emails being malicious.”

MAN–IN–THE–MIDDLE ATTACK:

Man-in-the-middle attacks, or eavesdropping attacks, happen when attackers insert themselves into a two-party communication or transaction. Once the attacker can interrupt the traffic, they can then successfully filter through and steal data.

Two most common ways the man-in-the-middle succeeds with attacks:

1. On **unsecure** public Wi-Fi, attackers insert themselves between a visitor's device and the network. Un-beknown to the visitor they pass all information through the attacker.

2. One a malware breach is successful, and attacker installs software that will process all the user's information without detection of what is happening.

HOW TO PREVENT MAN-IN-THE-MIDDLE ATTACKS:

1. HTTPS in the URL bar

Always check to see if there is an "HTTPS" on the website address you visit. DO NOT visit or exchange information with sites that do not have HTTPS.

2. Avoid connecting to public Wi-Fi routers directly.

Public WI-FI normally warns you that this is a public, unsecure connection. If there is no option but to use one, make sure you are using a Virtual Private Network, (VPN) or Secure Socket Layer plugin to protect your data privacy. A VPN is used to encrypt your internet connection on public hotspots to protect the private data you send and receive while using public Wi-Fi.

3. Be aware of phishing emails.

DO NOT click links in your emails. Test the link by manually typing the website address in your browser. Following these rules will dismiss fraudulent address and malicious code.

Be particularly careful when it comes to emails (phishing) from attackers asking for or asking to update your password or any other login credentials.

4. Keep your system always protected.

Man-in-the-middle attacks primarily use malware for their execution. The malware and spyware are installed when the system is not properly protected by an antivirus program.

Make sure you install a comprehensive internet security software and always keep it up to date. If done, this software should successfully identify malicious items you never thought existed and keep your online activities safe and secure.

In addition to maintaining your software you should plan on doing timely and regular scans to make sure that no malware is transmitting data to attackers.

5. Set up an intrusion detection system (IDS)

The intrusion detection system basically monitors your network flow. If anyone attempts to hijack the traffic the IDS will give immediate alerts.

The IDS uses advanced address resolution and dynamic host configuration to snoop on switches and limit or prevent certain forms of spoofing.

While unfortunate, IDS may on occasion raise a false attack alert that may trigger the user to disable it. Be careful about disabling, consider tuning the alerts and better understanding what is happening. Disabling may get rid of a false alert but make you vulnerable to many more.

6. Use the virtual private network (VPN)

Use of Virtual Private Network, (VPN) is another inexpensive and good way to prevent man in the middle attacks. Essentially the VPN creates additional secure layers when you access the internet.

DENIAL OF SERVICE ATTACK

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack.

Three General types of DDoS attacks

1. ***Volume-based attacks***

    - UDP flood: User Datagram Protocol (UDP) floods attack random ports on a remote server with requests called UDP packets. Requests are made to the server ports for the appropriate application, but no application is found, destination unreachable. The attack has overwhelmed the system and made it inoperable.

    - ICMP (ping) flood: This flood sends Internet Control Message Protocol, (ICMP) pings to a user system. Pings are a common way to measure connectivity between system and servers. In a ping flood, the attacker uses a massive series of pings to consume the incoming and outgoing bandwidth of the target server.

2. ***Application attacks***
    - HTTP flood: Targeting the web server or application, this attack, floods the target with standard GET and POST requests. Because of the inundation with requests the server may shut down. HTTP floods can be very difficult to detect because they appear to be valid traffic.
    - Slowloris: Named after the Asian primate (Slow Loris), the Slowloris moves slowly. Unlike floods, this attack carefully uses timed portions of HTTP requests sent to a server. Being timed so that the server does not time out, rather, the server waits for the request to be completed, thus exhausting server bandwidth and affects ability to handle legitimate requests.

3. ***Protocol attacks***
    - SYN flood: A synchronization attack removes the acknowledgement request and leaves the server waiting for SYN-ACK requests. In a very short time, the backlog of SYN-ACK requests burden the system, slows, or stops production completely.
    - Ping of Death: In a Ping of Death attack, the attacker tries to crash or freeze a server by sending a normal ping request that is either fragmented or oversized. The standard size is 65,535 bytes. Using a larger ping request forces the server to fragment the file. In the reassembly of the file for response the server buffer can be overloaded and crash.

DDOS ATTACK PREVENTION

Step 1: Understand that Every Business is Vulnerable

Vulnerability in this case goes beyond the safe measures put in place, though, we will discuss the tools, it is equally as important to understand what drives the denial-of-service attack. Many DDoS attacks are motivated by revenge, politics, trolling and terrorism, money is frequently involved. According to cybersecurity analysts, ransom and blackmail are the most common motives behind DDoS attacks. Understanding this, the size, scope, and power of a company influences targeting. Rare for small businesses to see this type of attack because blackmail is the main cause and there are bigger fish in the ocean. Given this, DO NOT assume that it will not happen to you. In matters of business, always assume the possibility and prepare.

Step 2: Deploy Protection Tools

Using a web application firewall (WAF) is the best protection against common types of application denial of service attacks. A WAF, combined with the work of cybersecurity experts, that receive the notifications and apply additional rules, most if not all malicious activity can be significantly reduced or stopped.

Step 3: Monitor Application Traffic Continuously

The number one preventive, proactive and preemptive measures to networks and hosts is the use of effective monitoring. In the case of cybersecurity, continuous monitoring with security experts distinguishing sudden spikes, taking corrective action by applying system wide rules, and watching for additional attacks, helps to preempt DDoS attacks.

Step 4: Inhouse DDoS Security or Managed Application Security.

Hiring trained security specialists for application security can be a bit out of reach for many small businesses. New or smaller businesses will often look to managed application security service vendors to monitor and stop DDoS attacks. These services offer 24x7 monitoring and attack mitigation and additional security measures.

SQL INJECTION ATTACK

A Structured Query Language (SQL) injection attack happens when the attacker inserts malicious code into an SQL server that forces the server to reveal information it normally would not. The attack can be as simple as placing malicious code within a website search box.

DEFENSE AGAINST SQL INJECTION

An SQL injection attack can be detected and potentially blocked using two different intervals within application traffic flow: The application traffic itself, and in the network.

The application itself can use two approaches to input a validation to help protect for injection, Blacklisting and Whitelisting.

1. In Blacklisting, known malicious characters are removed or replaced in the application input thus preventing specific unwanted code from entering the system.

2. Whitelisting, the more preferred method, examines each piece of the user input against a list of permitted characters. If there are any character differences, the code is considered malicious and is not executed.

In either case, continuous updated maintenance of the listing is necessary as additional applications are often added or unknowingly brought in by users.

ZERO-DAY EXPLOIT

A zero-day attack hits after a network vulnerability is revealed and announced, but before the company can patch or complete a solution. The Attackers target the vulnerability prior to the solution being implemented. Because this is time frame based, the Zero Day vulnerability requires constant awareness.

PROTECTING AGAINST ZERO DAY ATTACKS

There are three different strategies that can help defend against Zero Day Attacks. Note: It can be very difficult to completely protect against Zero Day attacks, as they come in many forms based the nature of the vulnerability. Producing patch solutions vary in time and complexity, and this effects timeliness in fixing vulnerabilities, thus providing different and sometimes multiple windows for Zero Day Attacks.

1. **Stay Informed**

    a. Zero-day issues are not always published but as they are you will be able to examine the potential vulnerability. Staying in tune to vulnerabilities and releases may allow you time to put in security measures to respond to a threat.

2. **Keep Systems Updated**

    a. Software developers live and die by development. When you're through developing, you're through. Patch needs are part of the nature of development; thus, developers work constantly to keep software updated and patched. In the end, it is up to you to make sure your software is always up to date. Setting applications to auto update can expedite the updating, however, some level testing should be done to ensure the patch does not break other elements of the application or system.

3. **Employ additional security measures.**

    a. Ensure that you are using varied security solutions that protect against zero-day attack because a single security measure may not be enough to fully protect you from a zero-day attack. There are various probes that

can be done to reveal vulnerabilities. Security vendors like Check Point have system analysis tools to help reveal vulnerabilities. Additionally, the industry focuses on solutions using hybrid detection techniques that normally produce more accurate results than a single approach.

4 SECURE DATA BACKUP & RECOVERY

Thus far this guide has focused on huge issues in data compliance and protection. Now we want to look at effective data backup and recovery, which is vitally important to business and business data survival. Imagine any one of the previously mentioned malicious attacks including physical theft, without having the ability to recover key business or customer data. Such a scenario can lead directly to a company's ending, with ongoing compliance fines.

STATISTICS ABOUT DATA BACKUP AND RECOVERY [6]

1. This year, 40% of small to medium sized businesses that manage their own network and use the Internet for more than e-mail will have their network accessed by a hacker, and more than 50% will not even know they were attacked. ***(Source: Gartner Group)***

2. 20% of all small businesses will be hacked within one year. ***(source: National Cyber Security Alliance)***

3. 20% of small to medium sized businesses will suffer a major disaster causing loss of critical data every 5 years. *(Source: Richmond House Group)*

4. 31% of targeted attacks focus on businesses with fewer than 250 employees *(source: Symantec)*

5. 93% of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. *(Source: National Archives & Records Administration in Washington DC.)"*

A data backup and recovery plan are essential to business success. Especially when that business deals with, and is reliant upon, health records. Such records are the life blood of the business, no pun intended.

The most common mistake in business continuity, (the ability to keep business going with loss of data) is not having data records in at least two locations. Particularly in small business, server data is backed-up to an onsite storage or drive system. While this addresses the backup need it does very little for recovery protection. Statistics show that 60% of backups are incomplete and 50% of data restores fail. Add to this statistic the possibility of malicious attacks expressed earlier and the possibility of data loss becomes very real.

One more possibility that is rarely addressed is damage to the current storage. Natural causes such as water, fire, heat, cold can destroy technology components and some or all data on them. It does not really matter how it happens, the point is, you should have an offsite data store. This data store can be as complete as the entire infrastructure or as small as data files.

Ensure you backup workstations, laptops and well as your servers. Too often the loss of a single laptop or workstation seriously cripples business operations either through loss of critical data or serious compliance issues with probable fines.

TIPS FOR BACKUP AND RECOVERY

1. **Consistently backup your data. Depending on your data cycle that can be often as several times a day, to weekly.**
2. **Monitor your backup for completion and immediately resolve incomplete backup issues to ensure complete data backup and integrity.**
3. **Create and execute a disaster recovery plan that ensures your business will continue to operate if a partial or full data loss is experienced. This would include a separate physical or cloud-based component to ensure your data is protected if disaster strikes your facility.**
4. **Audit and test your disaster recovery plan at least annually to ensure you can bring your business back to production status in a timely manner.**
5. **Backup power supplies or generators that can allow data backup, proper system shut down, and prevent database corruption or life critical systems going offline.**
6. **Additional internet providers, using different providers that will allow operations to continue if connection is lost or down.**

We live and work in world today that is driven by data. What would happen if your power, internet, or network went down for days or weeks? You could not access your databases, financial records, client, or patient records. Could the business still function and how would you recover?

5 DROPPED CALLS, POOR CALL QUALITY, LITTLE INTEGRATION, HIGH EXPENSE

Given the topic heading, you are thinking we are going to discuss phone systems. NOT TRUE, we really want to talk about small business internal and external communication, business operations, employee engagement and profit.

Some important statistics [7]

1. 65% of employees are not engaged at work. They work autonomous with little input or collaboration.
2. When employees are engaged profitability increases by 21%
3. 31% of employees never use the company intranet.
4. High performing companies are TWICE as likely to keep communications simple and jargon free.
5. 93% of communication professionals value creativity in internal communications but on 6% think it's used to full extent.
6. 74% of employees would work harder if they were better appreciated.
7. 60% of internal communicators don't measure the effectiveness of their strategy.

So, what do all these statistics have in common? Yep, you nailed it, they are all communication based. Further, there is a recognition that communication goes far beyond a phone, email, or text. The entire business operation, workflow and success is affected by communication, human integration, collaboration, and acknowledgement.

As with nearly everything else we have discussed, private practice finds itself at different levels, depending on understanding, need, and focus. Let's get focused for a moment.

Adding more receptionists to ensure a live voice and friendly smile is a good idea, but seldom adds to the integrated workflow and engagement necessary for profitability increase.

Ensuring key healthcare personnel have application-based tablets to feed the EHR can certainly expedite and increase accuracy of medical records but adds little to operational creativity. Desktop and system support keeps business rolling, but operational silo's, affect employee morale and ideas.

The point being is that we are back to initial question. Is your business driving the technology or is technology driving your business? Communications, both internal and external reveal how things are really going. DO NOT look at communications from a "What phone system should we use? "or "What email package is right?" or "Whether we should have document collaboration?" etc... Ask yourself how your business will humanly function better. Once you do, your operation will change, so will your technology, and your profit.

Communication evolution

PBX, which stands for Private Branch Exchange, is a private telephone network used in a company or organization. The PBX consists of both hardware and software and has been around since about 1944. The system can integrate Voice over IP as a protocol and can be used for calls, video conferencing, chat, and other communications.

VOIP, voice over internet protocol, are phones/communication systems that exclusively use the internet for communication. This can be a soft phone (from your computer) or a hard, actual device or both. Software drives the operation and uses far less equipment and maintenance than PBX.

UCaaS, Unified Communications as a Service, incorporates phone, email, document and team collaboration, video, and business operations into a single platform. UCaaS, makes big strides in recognizing employee engagement, innovation, and creativity in the workplace. UCaaS incorporates all the power of PBX and VOIP but goes much further in operational integration. Applications like Microsoft teams with

completed integration to the company's base phones. IT service companies normally team with telecom providers and their customers to customize the solution that works the way they do. This includes phone, on hold music and messages, effective phone transfer, video meeting, text, chat, project teams, document, and message collaboration and more. The quickest way to become irrelevant in business is to stay the same. Take time to review, listen and involve your staff in operation and direction of your business. The first step to all of this is communication. Hopefully, you have a better understanding of the 5 biggest headaches in private practice, and many other small business entities. Our goal was bringing enlightenment and driving change to make your business, smarter, safer, more secure, and profitable. If you have additional questions or would like us to help with business and / IT process, operations or analysis feel free to contact us for an appointment.

WE WISH YOU ONLY THE BEST IN YOUR PRACTICE.

Bibliography

[1] *Healthcare Data Breach Statistics (hipaajournal.com),* December 2020

[2] *HHS Changes HITECH Act Penalties for HIPAA Violations (hipaajournal.com)* April, 2019

[3] *Top 10 Most Common HIPAA Violations (revelemd.com) ,* Kaitlyn Houseman, REVELE, December 3, 2016

[4] *Cyber Attack - What Are Common Cyberthreats? - Cisco*, pg. 1, Date unknown

[5] *Phishing statistics and facts for 2019–2021 | Comparitech ,* Sam Cook, Data Journalist, privacy advocate and cord-cutting expert, Updated: February 7, 2021

[6] *5 Startling Statistics About Data Backup and Recovery (ontech.com),* Date & author unknown

[7] *7 Surprising Internal Communications Statistics (enplug.com) ,* Cassie Paton, ENPLUG Blog, 01 May 2020