Cyber Security and the Dental Office (Part II):
Be Prepared: Hacker Tricks and Security Emergencies

Scott Aurnou, CIPP/US, CIPT
Continuing Education Units: 2 hours


Disclaimer: Participants must always be aware of the hazards of using limited knowledge in integrating new techniques or procedures into their practice. Only sound evidence-based dentistry should be used in patient therapy.

Note to State of Florida dental professionals: This course does not meet the 3 credit hour minimum for Practice Management courses; therefore, it is only being offered for informational purposes in Florida.

This course will give dental professionals and office staff a basic understanding of the potential cyber threats facing a modern dental office. This will include secure day-to-day practices, the methods hackers use to trick people when attacking computer systems, the proper use of passwords, potential dangers when browsing the Web, and how to be prepared when a security incident strikes.

Please note this is Part II of a two-part series. This course builds upon the concepts covered in Part I (Protecting Your Office Computer Network) and should be read after Part I has been completed.

Conflict of Interest Disclosure Statement
• Mr. Aurnou reports no conflicts of interest associated with this course.

ADA CERP
The Procter & Gamble Company is an ADA CERP Recognized Provider.

ADA CERP is a service of the American Dental Association to assist dental professionals in identifying quality providers of continuing dental education. ADA CERP does not approve or endorse individual courses or instructors, nor does it imply acceptance of credit hours by boards of dentistry.

Concerns or complaints about a CE provider may be directed to the provider or to ADA CERP at: http://www.ada.org/cerp
Overview

Modern dental practice means computers, mobile devices and the need to protect sensitive office and patient data. This course will introduce you to a number of basic cyber security concepts as first steps on the path towards protecting yourself and your practice.

Learning Objectives

Upon completion of this course, the dental professional should be able to:

- Understand how hackers try to trick people and how to avoid becoming a victim.
- Comprehend the importance of using secure day-to-day processes to protect your office.
- Recognize the potential risks when browsing the Web.
- Appreciate the role of “the Cloud” and the Internet of Things in a modern dental office.
- Understand how to prepare for and react when something goes wrong.

Course Contents

- Introduction
- The Importance of Secure Processes
- The Human Element
  - Deception and Social Engineering
  - The Dangers of Browsing the Web
  - The Threat from Within
  - Using Passwords
- Newer Technology – The Cloud and the Internet of Things
- Reacting to a Security Incident
- Cyber Security Do’s and Don’ts
- Conclusion
- Course Test
- References
- About the Author

Introduction

In Part I of this course (Protecting Your Office Computer Network), we discussed the role of legal standards such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the tech basics underpinning the use of computers and electronic data that come with having a modern dental office; and fundamental computer, mobile device and network security measures to safeguard them. Now we’re going to build upon those first steps towards protecting your practice. In Part II we will delve into the crucial role of secure daily routines, hackers’ tricks designed to separate you from your data (and more), using passwords securely, the risks that come with browsing the Internet, and how to prepare for a security emergency.

The Importance of Secure Processes

Secure processes are effectively standardized procedures (expressed as policies) that revolve around the way your office handles day-to-day activities, and there are a number that can make your practice safer. These policies should all be documented. That will both encourage consistent behavior in following the policies and give you something to attest to your office's security practices should you encounter an investigation or audit through the Department of Health and Human Services (HHS)' Office for Civil Rights (OCR).

One of the most important steps you can take is to keep your software up-to-date. It’s a straightforward yet absolutely crucial step to safeguarding any individual computer, server or network. The vast majority of malware targets flaws in software that have already been discovered and fixed. If the updates fixing those flaws have been put in place, the attacks will fail to penetrate your system and effectively bounce off since the
Weaknesses they’re looking to exploit won’t be there. Moreover, any software that is no longer being updated by its developer (like the Windows XP operating system) should be replaced at once.

It’s also critical to change the default settings on your equipment. Basically anything that has a password and just works right out of the box will have a default password (and sometimes a default username) an attacker can look up easily. Apple products, for example, typically use “Alpine.” A good place to start is with the router connecting your office to the Internet. In addition to the password concern, there are a number of steps that should be taken to secure it. While routers often do the job of connecting you to the Web effectively, they are also vulnerable to a number of different attacks if they aren’t set up (aka “configured”) properly. For example it’s unfortunately all-too-common for an older wireless router to use WEP (which stands for “Wired Equivalent Privacy”) protection. This is a serious problem because WEP encryption was cracked over ten years ago – a hacker with minimal skills can easily break into any network using it. Instead, make sure your router is using a current encryption, like WPA (“Wireless Protected Access”) with the Advanced Encryption Standard (AES) or WPA2. WPA2 should be on any equipment manufactured since early 2006. The type of encryption a router is using is often written right on it. If it isn’t, you can check – and often change – it on the router’s online configuration page.

A process known as operating system (OS) hardening involves removing any unnecessary software and functions from the computers and servers in your office. While it may not seem like that big of a deal if no one is using the software or function, a hacker with minimal skills can easily break into any of them to get inside your network. Less software, etc. means fewer potential weak spots for an attacker to target.

Your computers should be shut down at the end of the day. Electronic attacks only work against computers that are powered up.

Data encryption should be a given for an office handling Protected Health Information (PHI). While the full-disk encryption we discussed in Part I certainly can’t hurt, file-based encryption is better at safeguarding the data stored within your network. A critical aspect of storing sensitive encrypted data is the secure storage of the decryption keys (referred to as “key management”). While HIPAA’s Breach Notification Rule doesn’t apply to encrypted data, that isn’t the case if the thieves also make off with the decryption keys to unscramble the data they’ve stolen. In information security circles, key management is often viewed as the potential weakest link in an otherwise well-executed encryption scheme, and there is additional information available on best practices for key management.

The data on your system should be backed up regularly. Properly maintained backups prevent potentially catastrophic data loss in the event of an accident or malicious destruction. This is especially important when dealing with sabotage, ransomware, etc. The backups should be multi-tiered (i.e., use different types of storage methods in case one of them fails) and be offsite. If there’s a fire, flood, etc., onsite backups can be destroyed along with everything else. They should also be encrypted to the extent the system data is encrypted (if not more). The backup process should not be mindless repetition. An altered or destroyed file can be inadvertently saved over an important file if the integrity of your files isn’t checked.

Hackers will naturally target the people using your network, so it’s important your secure processes include the human element of security, too.

For starters, the fewer admin (administrator) accounts on your network, the better. Like the administrative accounts noted in the computer and laptop section in Part I, network admin accounts allow full access to your equipment and files, including the ability to download, modify and delete programs. If an attacker is able to gain access to one of those accounts, he or she can cause tremendous damage to your system. To keep this from happening, keep the number of admin accounts on your system as limited as possible and add extra protections for those accounts like two-factor authentication (discussed in the password section below).

Have regular security awareness training for everyone in the office. Topics covered should include security and privacy of PHI, phishing attacks.
Can also be used to lure victims into contact with scam artists posing as colleagues or vendors.

A spear phishing email is a personalized version of a phishing attack aimed at a specific target (rather than a general phishing email intended to ensnare whoever falls for it). It typically includes personal and/or professional information to make the recipient trust the sender. These details can come from online sources like LinkedIn, Facebook and other social networks and information available via business-related websites, as well as particulars obtained directly from coworkers via social engineering.

In addition to these details, emails like this often appear to come from a familiar source like a friend, family member, colleague or a business you deal with regularly. This is possible because a sender’s name and/or email address can be altered to appear as though the message is coming from someone else. Likewise, a different phone number can be made to show up on a call recipient’s caller ID. This process is called “spoofing.”

Whaling is an attack that deliberately targets the high-ranking people within a business. The idea behind this approach is these targets are “big fish” within the organization who have wide access.
within the network yet may not take the precautions needed to keep their own accounts secure.

**Pretexting** is effectively in-person phishing to gain information and/or access to a restricted area. The term "pretexting" refers to the set up used to convince the target there is a justifiable reason (or pretext) to divulge the information or access the person is after. These attacks can take a wide variety of forms often revolving around someone (or a team) creating a distraction and/or masquerading as someone who could have legitimate access to the system they're targeting. It could be someone who claims to be from a vendor or a contractor, fake IT personnel or something as random as a "fire inspector" allegedly checking the office for imagined safety hazards while an assistant/accomplice surreptitiously places devices to monitor and/or siphon sensitive data from the victim network.

Pretexting attacks are effectively in-person phishing to gain information and/or access to a restricted area. The term "pretexting" refers to the set up used to convince the target there is a justifiable reason (or pretext) to divulge the information or access the person is after. These attacks can take a wide variety of forms often revolving around someone (or a team) creating a distraction and/or masquerading as someone who could have legitimate access to the system they're targeting. It could be someone who claims to be from a vendor or a contractor, fake IT personnel or something as random as a "fire inspector" allegedly checking the office for imagined safety hazards while an assistant/accomplice surreptitiously places devices to monitor and/or siphon sensitive data from the victim network.

Live social engineering attacks can also come by phone, such as fake "technical support" calls offering to fix imaginary problems with your computer if you will just allow the caller to briefly take control of it remotely. These are always scams. Whether at your office or at home, never allow someone who initiates contact with you to take remote control of your computer. Ever.

**Baiting** is a type of attack in which a piece of portable electronic storage media like a CD-ROM, laptop or USB stick drive is left at or close to the target's workplace in order to tempt the curious victim into seeing what's on it. These will often include an official-looking logo or markings to make them especially tempting to look at. How curious would you be to look at something labeled "Partner Compensation – 2015" (with your organization's logo on it)? In effect, the CD, stick drive, etc. is the worm on the fishhook. You're the fish. Of course, once the CD, laptop or stick drive is connected, it will quietly download malware onto the network. And yes, this initial intrusion into the network will likely be traceable back to you.

**What can you do to avoid falling for a social engineering attack?** The one thing these attacks all have in common is they rely on you to go along with the story they're selling. The single best thing you can do whenever you receive an unsolicited electronic message or call from a business or someone you don't know personally is to assume it's fake. Never click on links, open attachments, call phone numbers, or use any other method of contact contained in any unsolicited emails, texts or calls. If you think the email, etc. could possibly be legitimate, contact the alleged sender directly via phone or their official website. Again, don't use any numbers or links contained in the email, text, etc. sent to you.

**Learn to recognize (and avoid) phishing emails.** Phishing attacks are generally designed to make you take action by either frightening or tempting you. The attempt to scare you may be something like a problem with the delivery of an important-sounding package, an IRS question regarding your tax bill, or a "problem" with an online bank account. In the case of a bank, the phishing attempt may claim your account has been frozen and you have to enter your log in information to fix the problem. Another type of attack claims your account has been compromised and your log in information is needed to secure the account. Needless to say, the email itself is the real threat. These emails can look very convincing, but they are still fake. Their real intent is to trick you into entering your personal or log in information, clicking on a link for an infected website or opening a malware-laden attachment. If you do click on a link in a phishing email, you will often be taken to a website that looks real, but is only there to steal your account and log in information. Often, by the time you realize what's happened, the thieves have already emptied your account.

Even if an email appears to be from someone you know, keep in mind the sender's address can be faked. If the message appears out of character or strange in any way, give the sender a call to see if it really came from them. And of course, if an email allegedly from someone you know somehow winds up in your spam folder that's a red flag-and-a-half something's wrong.

In addition to your own common sense, an effective defense against phishing and spear-phishing attacks is a well thought out office procedure. An example of this might be no disclosure of PHI or wire transfers without a confirmation phone call to a number verified outside the initial point of contact (i.e., don't just call the number in the email asking for the information and don't assume that a caller
you don’t know is actually from where he or she claims to be).

**Extra risk for smartphones.** Phishing emails can be particularly dangerous to deal with on smartphones and other mobile devices. On a desktop or laptop computer, you can hover over a link with your mouse (without clicking on it) to see where that link actually goes – it will appear on the lower left of your browser window. Mobile devices typically do not allow for this sort of “preview” of a link and the address bar indicating which site you are actually on is often hidden off-screen to maximize the available viewing area.

**Responding to in-person deception.** When someone asks you to help him or her access something – or someplace – restricted, ask yourself why he or she needs your help. Also, it never hurts to take a moment to check out the story you’re given. A quick phone call (not using a number he or she gives you) can derail a social engineering attack before it starts.

**Don’t fall for the baiting attack.** Tempting though it may be, opening that conveniently abandoned stick drive, etc. yourself is a bad idea. If you have dedicated security or IT personnel, take it to them and definitely tell your office manager. That way he or she can get the word out so someone else in the office doesn’t fall for it.

Speaking of, an IT department can (and should) take steps to help protect a network from electronic intruders, including the installation of network security software, but don’t forget the first line of defense against a social engineering attack is you.

**The Dangers of Browsing the Web**

It’s common sense to lock your car doors whenever you park in a sketchy neighborhood, and the Internet is a sketchy neighborhood. When you’re online, you’re often one ill-advised click away from a stealthy malware attack that can damage your computer or network, and/or steal patient, office or your own sensitive data. This can include PHI, private messages, passwords and even the login information for your bank accounts. How can these attacks happen and what can you do to protect yourself and your practice? Let’s discuss...

**Drive-by downloads.** A drive-by download is a piece of malware that is downloaded onto your computer or mobile device without your knowledge when you visit an infected website. Although they are frequently found on malicious websites, drive-by downloads can also be lurking on normal ones that have been compromised by hackers. A similar tactic referred to as “malvertising” uses malicious code in the advertisements on otherwise trusted websites (many of which outsource the ads that appear on them). The best things you can do to defend yourself are to keep your software up-to-date (since malware often attacks through older security flaws the software manufacturer has already fixed via an update) and think before you click. If you’re using a desktop or laptop computer, you can also hover over a given link before clicking on it. The destination address will appear on the lower left of your screen. If it’s something you don’t expect or haven’t seen before, don’t click on the link.

**Fake websites.** Another thing to look out for is slightly misspelled or plausible-sounding – but fake – website names. This can be something like www.welllsfargo.com (with an extra L) or www.securityupdate.[yourbank'sname].com. These sorts of misleading websites can be found both within phishing emails and as standalone sites that serve the same purpose as the emails. As a result, you should be absolutely sure you are on the actual website for your bank or other business before entering any personal, financial or log in information. One way to approach this is to go directly to the bank’s or business’ site and bookmark it for future use. If you are using a smartphone or tablet, many banks and other businesses will have a dedicated app you can use instead of going through a (possibly fake) web link. Make sure to download the apps either directly through an official app store such as Google Play for Android devices or Apple’s App Store or the business’ actual website.

**Social networks.** Facebook, LinkedIn and other social media sites can come with risks. Only connect to people you know and be mindful of your account’s privacy settings. Hackers can use information found on social media profiles to craft spear phishing attacks.
What steps should you take to protect yourself? Here are a few that can help:

**Keep your software up-to-date.** As noted above (and in Part I), nearly every type of malware targets flaws in software that have already been fixed by the developer through software updates. If the computers in your office network are up-to-date, the vast majority of malware attacks against them will fail.

**Don’t forget to hover** over weblinks before you actually click on them.

**Make sure to use HTTPS whenever you access a banking or financial website.** HTTPS provides a more secure way to access the Internet. It is used to encrypt the communication between your web browser (Internet Explorer, Safari, Microsoft Edge, Google Chrome, Firefox, etc.) and the web server you are accessing when you visit a website. This helps protect against several types of attacks. A particularly prevalent one is a man-in-the-middle attack, in which someone else is able to effectively eavesdrop on your web session and steal (or alter) sensitive information. When using HTTPS, you will see a locked padlock and “https” on the left side of the address bar at the top of your computer screen. A good approach is to use HTTPS whenever it’s available. One simple step that can help is to use a free web browser add-on called “HTTPS Everywhere.” It automatically uses the secure version of hundreds of popular websites whenever you connect to them.

**No banking or financial transactions via public wi-fi.** Using a public wireless network – like one you might find in a coffee shop – is not secure and can expose you to a variety of spying software. You should never engage in any electronic banking or other financial transactions when on a public wireless network.

**Know how to identify – and avoid – a webinject attack.** A webinject attack is a type of a man-in-the-middle attack that will often appear as extra text fields or a fake pop-up window while you are actually logged in with your bank. The text fields or pop-up will generally ask for your account and/or log in credentials again “to enhance your security” or something similar. The problem is that it’s not from your bank. Banks do not communicate with their clients like that. If you see something like it, it’s an attempt to steal your log in information. Do not respond and notify your bank immediately. Like many other attacks, a web inject will attack through flaws in software that hasn’t been updated. Be sure to update the web browsing and other software on your computer and perform an updated anti-virus scan. This may not be enough to remove the infection once it’s on your computer, so you may wish to contact a security expert to ensure the problem is completely eradicated.

**Browse the Web with a non-administrative account.** Computers come with a primary user account featuring “administrative privileges.” Those privileges allow full access to the computer, including the ability to download, modify and delete programs. While you need that to add, change or remove any software on your computer, you don’t need it to browse the Web. If an attacker is able to gain access to your administrator account, he or she will be able to control your system. To keep this from happening, set up a user account with non-administrator access to browse the Web (and limit the potential damage an attacker can do).

**Secure your social media accounts.** The methods used to lock down social media accounts vary based on which site you’re using. Advice on securing them can be found online.
The Threat from Within
Potential threats can also come from inside your own office. These come in two basic flavors: mistakes... and malice. Mistakes often lead to the inadvertent disclosure of PHI or other sensitive data. This can take place via misdelivery, publication errors, lost media and disposal errors.

Misdelivery primarily relates to mistakes made when sending out emails containing sensitive information. An incorrectly typed email address can easily lead to the disclosure of sensitive information. This sort of thing can also happen with paper records, x-rays, etc. if mailing addresses aren't checked carefully (and yes, that still constitutes a breach). There is a big risk for this sort of disclosure when office personnel are doing mundane tasks involving sensitive data. Small mistakes can lead to big problems.

Publication errors involve posting non-public information on a public resource, like PHI on social media or your office website. Have rules in place regarding which information can be posted publicly and be sure to double-check the work before it goes live.

Lost media underscores importance of encryption and is discussed in more detail in the sections in Part I covering computers and mobile devices.

Disposal errors involve failing to properly purge an electronic device or shred paper data containing PHI or other sensitive data before throwing it away. Proper data disposal is covered in detail in the sections on computers, mobile devices and network security in Part I.

There is also a significant risk of business partners making any of these types of errors (since business associates are staffed by people and can make these mistakes just as easily as anyone else can).

Moreover, much of the time, the office suffering the breach is not the first one to find out about it. The majority of these errors are discovered externally, either by customers (or patients, as the case may be) or other external entities. That type of publicity is definitely best avoided.

What should you do? A few steps can help. Data Loss Prevention (DLP) software can catch sensitive data (credit card numbers, PHI, billing info, etc.) before it leaves the system. While there are ways for a skilled hacker to get around it, DLP software can help prevent inadvertent disclosures of sensitive data on its way outside the network (before it gets away).

Put procedures in place to prevent inadvertent disclosures. This can include saving patient and vendor email addresses into your email contacts instead of manually typing each email address when sending outgoing email, and double-checking addresses on outgoing paper mail. Also, keep in mind if the information inadvertently disclosed is encrypted, that disclosure does not constitute a breach under HIPAA and most state breach notification laws. A simple rule that could save your office some serious potential headaches: no emailing unencrypted PHI, regardless of recipient.

Proper disposal of electronic and paper PHI is covered in Part I in the sections on computers, mobile devices and network security.

Malicious insiders are just what they sound like – people with legitimate access to your system who mean to do harm to you and/or your office. This can mean someone looking to quietly sell PHI for profit or a disgruntled current or former employee seeking revenge for a perceived offense.

While nothing is foolproof, there are a few measures that can help reduce the potential threat. Employee background checks are a simple step that can literally nip the problem in the bud. In addition, access to your network should always be as restricted as possible. Current employees should not have any system access beyond that which they actually need. A security or IT professional can easily set up employee accounts that control each employee’s degree of access to certain files or parts of your office network. Moreover, when any employee leaves your office – regardless of reason – their access to the system should be rescinded immediately (including keys and building entry badges).

Technological measures that can help include network monitoring and the DLP software noted above. Network monitoring essentially involves
keeping an eye on who accesses what and where data is moving within your network. It can be outsourced or there are a number of software packages available to do it in-house. These measures are covered in more detail in the network security section in Part I.

**Using Passwords**

Creating a strong password may seem like a chore, but sometimes it can literally be the only thing standing between a cybercriminal and your own personal and financial information or access to your office’s network and PHI. Here are some tips for creating a strong password (that you can actually remember):

1. **The most important factor in creating a secure password is length.** Hackers often use software that essentially makes millions of guesses per second to crack a given password (this is called a “brute force” attack). A longer sequence of characters (letters, numbers and possibly punctuation marks) means more possible combinations to help thwart an attacker. The absolute minimum should be twelve characters, though the longer the better. If a password has eight characters, for example, modern password cracking software will break it in a matter of hours. A difference of four characters in a password may not seem like much, but there is a huge increase in the number of possible combinations it will yield (and hence attempts that the cracking software will have to make before it can break the password in question). Even if only letters and numbers are allowed, there are 14 million times as many combinations with a twelve character password vs. an eight character one. And if punctuation marks are included, the figure goes 81 million. Simply put, longer passwords are always better.

2. **Use a nonsensical (or completely personal) passphrase.** That way, you can pick a password that is both easier for you to remember and harder for an attacker to figure out. If you really want to, you can mix in random characters like $, @, etc., though hackers are well aware people try this trick. Truth be told, it’s really the length that makes a passphrase difficult to crack, so it will essentially make the password more difficult for you to remember while not making it any harder for an attacker to break.

When creating your phrase, make sure it’s really unique to you (or genuinely random). Avoid famous literary quotes and song lyrics – hackers can check for those. A good nonsensical passphrase might be something like: CyanStapleWashingtonBanana44 (don’t use this exact one – or any other password/passphrase suggestion you see online – yourself. Hackers can find those, too). A personal phrase can be effective because it relates to something that’s memorable to you. Just make sure it isn’t a widely known event. Perhaps that time you were surprised at the aquarium: “BlueLobstersAreReal!!!” It’s long enough that a machine won’t break it anytime soon, no one is going to guess it and you will remember it.

3. **Don’t use the same password for multiple sites.** This is known as “daisy-chaining.” If one account gets compromised, it will instantly expose others with the same (or a similar) password to attacks.

4. **Don’t have a file or email called “passwords” anywhere on your computer (or saved in an email).** These are easy for a hacker to find if he or she searches for “password” on either one.

5. **Change passwords regularly – perhaps every few months.** If a database storing a site’s passwords has been compromised (which is often not discovered right away), changing a given password makes it effectively useless to an attacker even if it’s stolen and eventually cracked.

6. **Use “two-factor authentication” (2FA) whenever it’s available.** Additional “authentication factors” are just ways to ensure you are who you say you are. This can mean something like a fingerprint scanner or a code sent to your phone via text message that is then entered in addition to your password. If an attacker only has your password, he or she still won’t be able to get access. Two-factor authentication is especially helpful in safeguarding administrator accounts and remote logins to your network.

7. **Avoid using security questions, if you can.** Frequently these questions are used as a way around the dreaded “I forgot my password” problem. This may sound helpful, but they almost always focus on information that can be found elsewhere online (where you went to school, pet’s name, favorite color, etc.). Any hacker will know to look for this information and can use it to get into your account – and potentially lock you out. Unfortunately, some sites require you to use the
questions. If possible, try to select questions that don't have just a few or even a single answer that a hacker can find (your mother's maiden name, for example).

8. **Use a password manager.** Password management software helps you create nearly unbreakable super complicated passwords. The passwords are encrypted and locked behind a single master password only you know. The software securely saves your login information, and you can automatically login to your accounts either directly through the software or via a browser button add-on. A portable version of the software can also be installed on a USB drive and used to view and login to your accounts on other computers. There are excellent paid versions, including RoboForm Everywhere, Sticky Password, Dashlane Premium and LastPass, as well as good free versions including KeePass (best for techies) and LastPass Free.  

**Newer Technology – The Cloud and the Internet of Things**

By its very nature, emerging technology is still (and will always be) developing. Two increasingly familiar technologies that can have a strong effect upon a dental office are the "Cloud" and the "Internet of Things." What are each of these?

The concept behind the cloud really isn't new. "Cloud" is mainly used as a marketing term for a very simple idea: using electronic storage, software or other functionality hosted on someone else's computer(s) which you access via the Internet (like Planet DDS, Dropbox, Gmail, etc.). That's it. That's the entire concept. A typical use of the cloud might be with a vendor acting as a Business Associate under HIPAA.

The nature of the cloud means someone else is literally in control of your data (including PHI), though your office can also be held responsible if those business associates violate HIPAA and there's a data breach. Having office data, PHI, etc. handled and/or stored by someone else means any risks or vulnerabilities found in their systems are cumulative to any issues or concerns with your own office network or equipment.

There are a number of steps you can take to protect data in the cloud:

**On the vendor side:** For starters, you need to know what level of access your vendors have to your – and your patients’ – data. Any vendor you do business with should be HIPAA compliant, and you should have a written business associate agreement (BAA) with them clearly saying so. These vendors should have written policies in place regarding the storage and handling of PHI and other data, including detailed data backup procedures and security measures. Technical controls should be in place to track the data moving through a cloud vendor's network, and the vendors must also have fully developed business continuity (BCP) and disaster recovery (DRP) plans.

**On your side:** Be sure to protect the computers and/or mobile devices used to access cloud data. If an attacker can compromise one of those "endpoints," he or she can simply steal information off it directly. Additional detail can be found in the sections discussing computers and mobile devices in Part I. Attackers can also use stolen login credentials to access cloud data themselves, so cloud access and the credentials used for access should be carefully managed. Use strong passwords as discussed in the previous section and two-factor authentication whenever it’s available.

The Internet of Things (IoT) refers to rapidly growing types of "smart" devices including anything from baby monitors you can access when you’re not at home to refrigerators that use web-based monitoring to let you know when your food is likely spoiled. In the healthcare field, it relates directly to Internet-connected medical devices like picture archive and communications systems (PACS) and x-ray systems. Unfortunately, security is often an afterthought when these devices are designed and hackers are perfectly happy to use them as a poorly defended gateway into a healthcare network.

It’s not uncommon for medical devices to use outdated software, have poor password protections, and not receive any updates even after security issues are discovered. Until these devices come better secured, protective measures such as firewalls and network segmentation (described in the network security section in Part I) can help to effectively secure the rest of your network from them. This is not a do-it-yourself
Reacting to a Security Incident

When something does go wrong, the first thing to do is identify what happened. Essentially you’re figuring out whether or not it’s actually a security incident. Some situations are obvious, like a natural disaster or a defaced website, while others aren’t so clear and should be investigated by technical personnel (security professionals, system administrators, etc.) to determine if there was a security incident. Some of the possibilities are physical damage (fire, flood, etc.), human error, an insider attack or an external cyber attack leading to data theft, destruction, etc. Proper responses will naturally vary considerably depending on the type of crisis you’re facing.

Upon discovering a security incident, the next step is to mitigate the potential damage, effectively stopping the bleeding as quickly as possible. This may involve taking systems offline and/or contacting the authorities. Preset written responses like Incident Response Procedures, Business Continuity Plans and Disaster Recovery Plans kick in here. Then the problem needs to be fixed – this is typically a technical solution that will have to be addressed by security personnel. Finally, it’s important to understand what happened so your office can be better prepared next time.

But we’re getting ahead of ourselves...

Whether you have one office or twenty, the proper first steps in reacting to any security incident happen well before the incident itself. That’s because the plans and procedures essential to responding to a security incident need to be ready to go as soon as something is discovered. Otherwise, you’re effectively just starting to pick your team while the opposition is already on the field and charging towards your goal. This sort of delay is absolutely unnecessary and can result in bad PR, lost business and compromised information (and perhaps even a spot on HHS’ lovely Wall of Shame).¹⁹

A written procedure to refer to in case of an attack is critical. An Incident Response Procedure (or Plan – IRP) defines how an organization reacts to a security incident. Each incident is different, so the most important aspects of an IRP are who has the authority to act and what needs to be done (though not necessarily how). Once an incident has been discovered, the IRP should specify actions to address different levels of incidents, as well as who is on the incident response team. The IRP should clearly state:
• Who responds to the incident
• The timeframe in which to respond
• How the response team members get in touch with each other
• What resources they will need
• Who do they contact (and when)

The IRP should specify one or more incident handling objectives. These can include: protecting organizational systems or data, restoring operations and limiting bad PR/brand damage. With HIPAA in mind, protecting data should be paramount. The response to the incident will flow directly from the handling objectives. It’s also important to specify who has the authority to take action (like the taking systems offline, contacting authorities, etc., as noted above). There are numerous IRP templates and detailed information available. HHS recommends a few resources to get started, including NIST’s comprehensive Computer Security Incident Handling Guide.²⁰,²¹ The IRP should be created – and regularly updated – well in advance and tested periodically. As with anything designed for an emergency, if it doesn’t work, you’ll find out at the worst possible moment if you don’t test it first.

The plans mentioned above are a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP). While they are often grouped together, they’re not the same thing. A BCP is for keeping things running in the short-term and a DRP is directed at recovering office assets and systems within a reasonable amount of time after an incident (it’s often IT-centric). One other important consideration: be sure that any plans (or procedures) meant to be used while responding to an emergency are written in language that can be understood by the people who will actually be using them. The easier to read, the better. As you can imagine, these plans are typically needed with little or no advance warning.
Start the ball rolling with a **Business Impact Analysis (BIA)**. A BIA determines what needs to be recovered and how quickly. In effect, you’re identifying the processes or functions performed by each part of your office. With respect to each function, look at:
1. Financial risk of not performing that function
2. Regulatory risk of not performing that function
3. Customer or reputational risk of not performing that function

In essence, what needs to be back up and running in what timeframe to minimize the impact on the practice?
1. What will the impact be if a given process or function isn’t restored right away (i.e., what’s really needed day-to-day and what can wait)?
2. How soon until that impact will be felt?
3. How significant will the impact be?

For example, if you’re a bank, marketing isn’t as critical in the short-term as payment processing, etc.

This is a slow and involved process, but well-worth doing correctly. Numerous samples and step-by-step resources are available.

A **Business Continuity Plan (BCP)** is a plan to maintain (or rapidly restore) business functions in the event of a major disruption. This can include anything from a security incident to a flood or power outage. A BCP ensures critical business functions continue during a crisis and outlines the immediate steps to take in response to one. Specific steps will obviously depend upon the circumstances, though a BCP will cover business processes, your people, assets, business partners, etc. This will include considerations like communicating with patients and/or vendors, and where and how will staff continue working, if possible. Details vary, depending on the size and nature of your practice, though basic free templates are available. You can also use a BCP published by an organization similar to yours and modify it as necessary.

A **Disaster Recovery Plan (DRP)** covers the steps needed to recover and replace infrastructure, etc., within a reasonable amount of time after a disruptive event. “Reasonable” may depend on how critical the system in question is. A DRP should contemplate various types of disasters, ranging from a single system or device to your entire network. An office’s technological “environment” should be examined to determine the impact of any single system or device failure. The BIA and risk assessments should offer guidance with respect to the effect and importance of specific systems, functions and processes.

A DRP specifies what must be done to keep your office running without the affected system or systems. The DRP should also include the “how” of getting replacement equipment if it’s needed. Given what’s at stake, DRPs should be tested and kept up-to-date. It’s rare the first draft of a DRP is perfect, so it’s extremely risky to make the first run through a live one.

Resources to help in the preparation of a DRP are available online and elsewhere.

**Cyber Security Do’s and Don’ts**

**DO**
- Perform regular Security Risk Assessments.
- Apply all patches (updates) to the software on your computer and used by your network. Automate the process to the extent you can and use Secunia, AppFresh, etc. to see what additional software needs updating.
- If your office is using software old enough that it is no longer supported (updated) by its manufacturer, replace it with newer software that is supported.
- Use integrated security software (firewall, antivirus, IDS, etc.).
- Control who has access to what and strictly limit who has administrative privileges.
- Use strong passwords and change them regularly.
- Enable screensaver passwords on your computer (and set them to engage relatively quickly).
- Change all default settings (user IDs & passwords) immediately on computers, servers, routers, point-of-sale devices and any other tool or device connected to your network.
- Log out of all online services when not using them.
- Use file-based encryption to safeguard all PHI (and other sensitive information) on your network – remember, if encrypted PHI is lost or stolen, it’s not considered a data breach under HIPAA/HITECH.
• Enable full disk encryption on every hard drive (especially in laptops), mobile device, storage device (i.e., USB drives) and backup media.
• Store your encryption keys securely (and not in the same place as the data it can decrypt).
• Have multi-tiered, off-site, encrypted backups.
• Keep your office's servers under lock and key, literally.
• Use WPA (with the Advanced Encryption Standard) or WPA2 encryption for your office's wireless network.
• Prepare any smartphone connected to your network to be stolen.
• Enable phone tracking and remote wiping.
• Back up your mobile data on a computer or in the cloud (iCloud, etc.).
• When an employee is terminated, disable his or her network (user ID and password) and building access immediately.
• Securely dispose of anything potentially holding office or patient data.
• Have an incident response procedure (IRP) in place well before it might be needed.

DON'T
• Have a file called "Passwords" anywhere on your computer or office network.
• Use the same password over and over – if it gets cracked once, every other account with that password becomes vulnerable.
• Keep a post-it note with your password somewhere obvious (under the keyboard, top right side drawer in your desk, etc.).
• E-mail any passwords – an intruder can search your e-mail and find them.
• Give your password to anyone else (including co-workers). If you ever do, change it immediately afterwards.
• Use WEP encryption for your wireless network – it was compromised years ago.
• Use unsecured (i.e., no password needed) wireless access to send or receive any PHI, financial or other sensitive data.
• Enter credit card, financial or login information without seeing "HTTPS" in your browser’s address bar (i.e., make sure the site is encrypted).
• Use cloud services without first making a reasonable inquiry into the state of their security.
• Assume using Apple computers inherently means you can ignore malware (it doesn't).
• Download any software (including programs, updates and mobile apps) unless you know and trust the source.
• Forget to document your office's risk management, training and security efforts.

Conclusion
New technology has made modern dental practice increasingly efficient, with new features like easily accessible patient and office data. These changes have also created new challenges to protecting that data and your office from a host of cyber threats. These can come from electronic attacks, employee errors, or even a serious security vulnerability in popular dental office software. While there is no such thing as perfect security, the basic security measures discussed both here and in Part I can help you safeguard your practice and yourself in the future.
Course Test Preview
To receive Continuing Education credit for this course, you must complete the online test. Please go to:

1. **What is a drive-by download?**
   a. A wireless electronic attack delivered by a passing pedestrian or vehicle.
   b. Self-replicating malware that jumps from computer to computer within a network.
   c. Dormant malicious software which attacks when you visit an otherwise innocuous-looking website.
   d. A type of virus hidden within an e-mail attachment.

2. **What type of encryption should be used on a wireless router?**
   a. WEP
   b. HTTPS
   c. WPA2
   d. Any of the above.

3. **Operating system hardening relates to the removal of unnecessary software and functions from computers and servers.**
   a. True
   b. False

4. **What is a brute force attack?**
   a. A computer-aided attack in which hackers attempt to break into a system, computer or file by trying numerous password combinations until they guess the right one.
   b. The use of physical coercion to force someone to give up a password.
   c. Forcing a website to shut down by overwhelming it with web traffic from numerous, remotely controlled compromised computers.
   d. An unexpected pop up window warning that your computer has been infected by malware, with an offer to fix the problem if you just “click here.”

5. **When should an office prepare incident response and disaster recovery plans?**
   a. Immediately after a security incident is identified.
   b. Whenever the firm recognizes the possibility of a disaster or security incident in the near future.
   c. As soon as the extent of damage caused by a disaster or security incident can be quantified.
   d. As early as possible. Yesterday would be good.

6. **Daisy-chaining refers to _______.**
   a. malware spreading itself across a network
   b. using a public wi-fi hotspot
   c. using the same password to secure different accounts
   d. taking a system offline to stop an attack

7. **An in-person attempt by a hacker to effectively talk his or her way inside your office is called _______.**
   a. Misdelivery
   b. Baiting
   c. Pretexting
   d. Whitelisting
8. What steps should you take with regard to an employee’s network access when he or she stops working at your office (regardless of reason)?
   a. Preserve the ex-employee’s login, so that firm personnel can access any necessary information if the need arises.
   b. Immediately disable the ex-employee’s network access (login and password), including physical building access and any form of remote access to the network.
   c. Disable the ex-employee’s remote access. The in-network access is secure, since the ex-employee would have to physically be at the firm to use it.
   d. Negotiate an agreement with the departing employee regarding the access.

9. What is “spoofing”?
   a. A process by which online information is falsified to appear as though it’s coming from a different source, such as the names in the “to” and/or “from” fields in an email appearing to be someone other than the actual sender or recipient.
   b. A method used to defeat encryption.
   c. A fake wireless hotspot used to lure in users and potentially steal their data.
   d. An attempt by an attacker to distract someone so that an accomplice can steal an electronic device such as a laptop or smartphone.

10. The “Cloud” is simply someone else’s computer accessed via the Internet.
    a. True
    b. False

11. An Incident Response Procedure should include all of the following EXCEPT ____________.
    a. how incident response team members will get in touch with each other when an incident occurs
    b. which outside firms and/or companies the team members will contact (and when)
    c. who is on the incident response team
    d. the office network Master Key

12. Which one of these is the best password?
    a. Iate12mangopancakesinKyotolastmonth
    b. P@$w0rd1
    c. Wherefore_@rt_thou_Rom3o?
    d. $Y3-&#p7x

13. Which of these is a serious problem often seen in Internet-connected medical devices?
    a. Poor password protection.
    b. No security updates from vendors even after security vulnerabilities have been discovered.
    c. Outdated software.
    d. All of the above.

14. What is the difference between a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP)?
    a. There really isn’t one – it’s two different names for the same thing.
    b. A BCP focuses on keeping an organization functioning during a crisis; a DRP focuses on recovering and replacing infrastructure after a crisis.
    c. A BCP focuses on the long term functionality of the organization; a DRP focuses on immediate repairs to damaged systems.
    d. A BCP addresses smaller scale business setbacks; a DRP focuses on large-scale emergencies.
15. Which one is NOT a mistake that could lead to the inadvertent disclosure of PHI?
   a. Publication error
   b. Whitelisting
   c. Misdelivery
   d. Lost media

16. What is smishing?
   a. Hackers intentionally targeting the most senior people in an organization first.
   b. A process that stops third party programs from running on a system until they are expressly approved to run.
   c. A social engineering attack delivered via text message.
   d. A sudden data breach, with the attackers making no effort to conceal themselves.

17. Why is it important to have as few network administrator accounts as possible?
   a. Administrator accounts can download, modify and delete programs.
   b. Two-factor authentication cannot be used with an administrator account.
   c. Administrator accounts are more expensive to maintain.
   d. Administrator accounts are difficult to use.

18. If you find a CD with your organization’s logo labeled “Employee Salaries” in a parking area adjacent to your office, this is most likely an example of what kind of social engineering attack?
   a. Phishing
   b. Spear Phishing
   c. Pretexting
   d. Baiting
References
About the Author

Scott Aurnou, CIPP/US, CIPT

Scott Aurnou is a cyber security consultant, attorney and vice president at SOHO Solutions. He spent over a decade as a litigation attorney in the NYC area, served as lead counsel for a private client services group with Smith Barney, and provided consulting and management planning services for security startup AEI. Scott uses his legal, cyber security, and business background to make information security concepts understandable (and even entertaining on occasion) for non-technical audiences. He has published security related articles in national publications ranging from the New York Law Journal to SC Magazine. Scott has created and delivered numerous presentations on security and privacy issues for executives, managers, and non-technical professionals.

He is a Certified Information Privacy Technologist (CIPT), Certified Information Privacy Professional (CIPP/US) and is admitted to practice law in New York, Colorado, the U.S. District Courts for the Eastern and Southern Districts of New York; as well as the U.S. Court of Appeals for the Second Circuit. Scott is the author of the Introduction to Information Security LiveLessons video training series for Pearson Publishing.