**Cybersecurity Basics**

The Fundamentals of Protecting Sensitive Data in Health & Human Services October 24, 2024

---

Good afternoon and welcome to our Cyber Security Awareness Month (CSAM) webinar! Thank you all for joining in this discussion today about cyber security basics.

1

---

My name is Shayne Champion, and I'm the Chief Information Security Officer (CISO for short) for CaseWorthy, which develops a cloud-based case management platform to deliver whole-person care and provide comprehensive outcome reporting across social and human services. Here's what I looked like after my second occurrence of jaw cancer (and no, I don't either smoke or drink). As a result, I appreciate your patience as I use this text to voice system to help me today. I promise to try and make this interesting for you.

Before we move on, let me tell you why I'm qualified to talk about cyber-attacks in the Health & Human Services industry. Not only was I previously the cybersecurity program manager for Blue Cross Blue Shield of Tennessee, as well as having been the CISO here for four years, I also used to run a consulting practice with a lot of bearing on this topic. We did several major tasks there, including doing risk assessments and virtual CISO work for other companies, incident response services for companies across the country, but we also did penetration testing. If you don't know, pen testing is where you hire an organization to ethically attempt to break into your systems either electronically or physically. I did all of those services, but I excelled at the physical penetration testing, which I enjoyed and was very successful at. That's where you try to physically get inside a company to access places and data you shouldn't have access to in order to test the company's security controls.

One more thing… I'm going to fill this presentation with a lot of data. Not only will the slides be available for you afterwards, but there's a key slide at the end with links to all the research and applications we will talk about. I'm a note taker myself and I hope this saves you from trying to take tons of notes or screenshots so you can just settle down and listen for now.

2

---

Our agenda for today is simple. First we're going to talk in some detail about hackers and what they're doing, then we will take that information and look at four things you should be protecting against in your organizations in our cybersecurity basics section. After that we will do a quick review and move to our Q&A at the end.

3

Our first topic for today is about Hackers.  We're going to look at what a hacker really is, where they come from, how profitable it is for cyber criminals, how they're attacking the health care industry, and why they want that kind of data.

4

---

Let's start with a little level setting discussion.  When you hear the word "hacker", what do you think about?  It's probably somebody like this… the proverbial evil genius hunched over their computer at 2 AM in a hoodie working frantically to steal your life's savings.  Let's make this interactive… please open up your chat, put some of your ideas, and let's see what the group thinks of when they think about a hacker!

5

---

However, (and not to be confrontational) there's a few problems with everything about that!

To start with, what if I told you that even the term "hacker" is stolen?  It's true!  Originally the term "hacker" in relation to technical things was coined by a group of hard-core geeks at the MIT computer lab in the 1950s.  Those forerunner geeks created a hacking culture, which meant playful or creative solving of technical work that required a deep understanding.  In fact, it was a word first associated with MIT's Technical Model Railroad Club, not computers at all!  Today we would probably call those same people "makers", but it meant essentially the same thing.  By the way, if you want more information about that, I highly recommend Steven Levey's book "Hackers: Heroes of the Computer Revolution".  If you have any interest in the history of how computers went from mainframes to home personal computers anybody could afford or on computer games, it's a great and somewhat entertaining history on the subject (particularly if you're a geek like me).

Anyway, the term "hacker" started being associated with illegal computer activity or "computer thieves" in the 1980s. The press and law enforcement began to use the term to describe individuals involved in unauthorized computer access, particularly after the 1983 movie *WarGames* with Matthew Broderick, which featured a young hacker breaking into military computers.  So not only has the name hacker itself been hacked, but many computer security professionals find the term offensive… that's true!  Insider tip: the result is if you use the word hacker to mean a bad guy around information security pros, it makes you look like a noob.  Use the word "threat actor" instead… it will get you a little geek street cred.

6

While we're on the subject, hackers don't usually look like this either! In fact, here's a picture of me a few years ago with the most famous hacker in history… Kevin Mitnick. I had a chance to meet him several times at conferences, and got to know him decently well. Not only was he a very cool guy, but incidentally his story is very much tied in with the *WarGames* movie which sensationalized national outrage against computer intruders and led to a massive (and probably unfair) national manhunt for him. His book, *Ghost in the Wires* in really a fascinating read about his story if you want to know more… 5 thumbs way up on that one! Unfortunately, Kevin didn't survive his own battle with cancer and passed away July of last year.

On the left is one of the pen testers I worked with, so in fact all three people in this photo are (now at least) threat actors (and at the time, all did so ethically). But what do real threat actors look like? Here's some examples.

The first one is wanted Russian hacker Evgeniy Mikhailovich Bogachev. The next is wanted Chinese hacker Sun Kailiang… you can see their FBI wanted posters by following the links at the bottom of the screen.

7

---

Why would I point out Russia and China? Well, let's take a look at the 2024 World Cybercrime Index. Here we get a World Cybercrime Index (or WCI) score from a high of 58.39 to a low of 0.44 for the top 50 countries in the world. However, for brevity let's take a look at the top four because they have some bearing on what we are discussing today.

8

---

Number one in the WCI is Russia. At a 5,000 foot view, their tactics are usually pretty brash – the digital equivalent of a smash & grab where, for example, in the real world where a team of robbers might rush a jewelry shop in masks, smash the glass with hammers, grab what they can, and run away quickly.

However, it's important to understand the "who" and "how" when it comes to good old mother Russia. When the Soviet Union started up, it replaced much of religion with Science, Technology, Engineering, and Mathematics (STEM). In fact, 37% of today's Russian undergraduate students major in a STEM field compared to only 21% in the United States. Combine this with the fact that when the USSR collapsed in the 1990s and the government privatized much of the nation's assets, organized crime took over in a major way… just in time for the internet revolution.

While Putin's government now has the upper economic hand, there is still a solid, if somewhat shadow, public-private partnership between the Russian government and organized crime which has found the benefit of, and has heavily invested in, cyber-crime. As long as cyber criminals both stay away from Russian interests and support government targets - sometimes even with the help of the Federal Security Service (called the FSB) and the Foreign Intelligence Service (or SVR) which are the modern successors of the KGB – the government looks the other way. In fact, the Russian government uses these groups in connection with their own FSB and SVR cyber teams to directly advance its foreign policy goals. Of course, doing these activities for the government curries favor with politicians, so it's a very reciprocal relationship. Add on top of this the fact that it's notoriously difficult to get extradition from Russia, these often large and very structured organized crime groups are pulling as much as one trillion dollars annually through cyber-crime activities.

This structure has been leaned on heavily for Russia's "special operations" against Ukraine. However, there have been some negative impact on Russia's hacking capability as well. Between the West's heavy technology sanctions and Putin's first conscription to fill losses from the Ukrainian invasion, its estimated that 50,000 to 70,000 tech workers fled Russia. There was another wave when there was a second conscription announcement, resulting in a huge IT brain-drain for the Russians. It's gotten so bad that Russia is offering incentives for information technology workers to stay including exemptions from paying income tax and preferential mortgage rates! Nonetheless, Russia continues to be the world's hot bed for cyber-crime activity.

If you want more information about Russia's cyber-crime, I found a great paper from the U.S. Army's Cyber Defense Review by Alec Jackson that I have linked here… it's a great read and summarizes tons of information I've heard or read about over the years. If you like books (or audiobooks) I also highly recommend the book *Spam Nation* by Brian Krebs… it's a phenomenal resource on Russia's cyber-crime problem!

One side note before I move on here. When I say "organized crime" in terms of cyber threat actors, it's a literal truth. Some of these organizations are huge with their own programmers, quality assurance, technical support, in short everything you'd expect of a major company. I can't forget one incident I worked several years ago with the consultancy where the victim's organization was forced to pay for not one, but two ransom payments (the threat actor was charging by the server) because they could not restore several critical systems. The first payment in bitcoin worked just fine and we were able to decrypt the data with the encryption keys they sent. However, no matter what we did the second one would not work. We replied back to the hackers over the secure email channel they were using, and when we got their reply it was a thorough technical how-to where, at the end of their email, they offered to remote in to that system and restore it if we needed their help. Now, on one hand I thought that showed quite a bit of hutzpah to ask the company you just hacked if you could remote into their computers (again). However, I also believe that they were probably serious about being willing to help… even though I would not recommend that if you find yourself in the pickle in the future.



---

Number two on the WCI index is none other than Ukraine. As a former satellite republic of the USSR, Ukraine realizes some of the historical benefits from focusing on STEM education. They have leaned heavily on their cyber teams to not only protect the country from Russia's hackers (many people now consider Ukraine to have the world's best nation-level cyber defenses as a matter of necessity), but also to support its troops. Their hackers have supported offensive efforts by providing intelligence and support to boots on the ground troops. This has included everything from breaching Russian military networks for intel to disrupting troop transports by attacking Russian railway systems. There is no doubt that Ukraine's cyber security forces have been as much a force equalizer as it's drone pilots have been.

Now, let's be honest… it's not all quote "good guy" hacking in Ukraine either. Corruption has long been a part of both Russia and its former puppet states, and there are quite a few Ukrainian organized crime organizations making the most of the fog of war as well.

Third on the WCI index is none other than China who I talked about earlier. Chinese tactics are very different from Russia, and they have historically preferred the insider threat – getting a Chinese national either directly inside a company or doing business with them – to get around their target's defenses. Now, this is not to say that China (or Russia for that matter) is not capable of advanced cyber attacks which we call Advanced Persistent Threats (or APTs). These are very technically complicated attacks, often using zero-day (these are just vulnerabilities for which there is not currently a patch or update available, so the vendor has zero days to prepare) attacks and can be very difficult to get rid of once your system has been compromised. By the way, for a great read on the subject of zero days and the international economy over countries bidding for those vulnerabilities to use in their national arsenals, I recommend journalist Kim Zetter's book *Countdown To Zero Day*… that story will truly blow your mind.

Now, there is another very successful public-private partnership working in China, but its fundamentally different from what we found happening in Russia. Where Russia is the economic wild west, we find China having more formalized relationships and an unsurprising heavy hand in all matters within its country - including the relationship between the government, military, and industry. This is worth a bit of an explanation so that we all understand the dynamics and differences.

While China has separate government/military hacking groups (not the kind of lawless, organized crime we saw in Russia), these groups all work in concert with the military industrial complex. Let's think about it this way: What's the relationship between our government, its laws, and industry? Political leanings aside, the intent is for our government to create laws so that companies can compete in a safe and fair way. However, this has no resemblance to how that works in China.

A Chinese government official would have no problem directing a military hacking team to steal information from a Western company and handing that to a Chinese company to manufacture. From their world view, the government is helping the company. That company not only pays taxes, but they are also manufacturing equipment and weapons their military can use. That makes the military stronger, which in turn also furthers the government's desires. For them it's a win-win-win scenario. Can you imagine the shellacking our government would get for hacking another nation state's commercial data and giving that to one U.S. company to produce? It would be a scandal and considered an egregious misappropriation of governmental resources, manpower, and money.

This isn't a theory either… let me give you an example. Defense contractor Lockheed Martin started developing the F-35 Lightning II 5th generation multi-role stealth fighter in 1992, and it was 14 years before it took its first flight. The F-35 represented the next generation of American air supremacy, and we spent 1.5 trillion dollars developing one of the most advanced aircraft ever designed.

Reports came out in 2011 that China had stolen blueprints for the F-35, and the next year they just happen to roll out their new 5th generation fighter, the Shenyang FC-31 Gyrfalcon. Now, I don't know about you guys, but I spy with my little eye some drastic similarities between these two aircraft.

--- It turns out that a man named Stephen Su (actually Chinese national Su Bin) was running a small Canadian company called Lode-Tech that made aircraft cable harnesses. In 2008, Su worked with two hackers from the Chinese People's Liberation Army (PLA) to exploit his industry connections and stole 65 gigabytes of data (more than 630,000 files) about Boeing's C-17 heavy lift cargo aircraft. They then went through Lockheed Martin's contractors and sub-contractors to steal tens of thousands of files associated with the F-35 program and cover their tracks. He would supply all this to Chinese officials bragging in an email that these files would "allow us to rapidly catch up with U.S. levels … To stand easily on the giant's shoulders" as they re-designed their J-20 fighter to fit the mold of the F-25.

In 2014 the U.S. Department of Justice filed a criminal complaint and subsequent indictment against Su and 4 months later he was arrested by Canadian authorities. While he was facing 30 years in prison, Su eventually file a plea agreement in exchange for a 46 month sentence.

So think about the return on investment there. Three guys over the course of 6 years make up 14 years and one and a half TRILLION dollars of research and development. That's pretty horrifying stuff!

China continues its aggressive tactics today. According to the office of the director of national intelligence's 2024 annual threat assessment, "China remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks."

Looking at Russia and China's cyber threat in comparison, it boils down to this. While Russia in general is the source of almost twice as many cyber attacks as China, these are mostly the ransomware, extortion, and petty theft of organized crimes. By comparison, China tends to be a much more focused general attack on all aspects of American intellectual property and critical infrastructure on both the government and private sectors.



---

For our final WCI index leader, let's look at 4th place, the United States. A big part of that is our nation-level cyber offensive capabilities where we have some well-established national assets like the National Security Agency (NSA) as well as formalized cyber capabilities in each military branch.

The high technical capacity and stability of the US and its infrastructure also attracts a lot of cyber criminals. For example, in 2015 Ross Ulbricht, known online as "Dread Pirate Roberts", was arrested in 2013 for running the dark web site Silk Road. His site was used to buy and sell drugs and other illegal goods and services anonymously and outside the reach of law enforcement, and he earned $13 million in the process. In 2015 Ulbricht was sentenced to life in prison for his illegal activities.

Originally U.S. hackers broke into networks as a challenge or to get street cred with their tecno-friends; this was the case with infamous hackers like Kevin Mitnick we mentioned earlier or the 70's phone phreaker Doug Draper who was known as Captain Crunch because he discovered the toy whistle at the bottom of the cereal box could be used to fool the telephone system for free long-distance calls.

In current day, this has changed as many young technophiles turn to cyber-attacks for the enormous financial potential (we'll talk more about that in a minute). Law enforcement has discovered that some of the world's largest cyber-criminal gangs are not centralized like those you may find in Russia but could compose hundreds of individuals across the world - including people based in the US.

A great current example of this is the group known as Scattered Spider. This organization was behind widely publicized attacks against companies like MGM and Clorox, and many people believe its currently the world's third biggest cyber threat behind Russia and China. To understand the scale of their attacks, the attack against MGM resorts resulted in losses over about $100 million dollars alone. In January of 2024 Florida authorities arrested 19-year-old Noah Urban who they described as a "key figure" in Scattered Spider's organization.

Alternately, other hackers are what the industry calls hacktivists – individuals who attack computer systems to further social or political ends. This includes infamous groups like Anonymous who see themselves as modern-day digital Robin Hoods, attacking websites and networks from everything from defeating ISIS to supporting the George Floyd protests in 2020.

Finally, the US is just a big target, and we sometimes make these attacks far too easy for the bad guys – particularly in health care (more on that in a bit). Take it from me, I have some amazing stories about how as a pen tester easily I was able to trick or bluff my way into secure offices where I was able to see sensitive information that I should never have had access to. This is why I didn't stop at the top three from the index… we have to remember that not all bad guys are from other places. These attacks can be insider threats (attacks from frustrated or disgruntled members of your own company), politically motivated attacks (a real fear during this election year), or even just a guy using their legitimate access to your system to pull data about their ex-girlfriend or neighbor they hate that they don't have a legitimate work-related reason to access. A threat is a threat, no matter where that threat actor comes from.

We have talked a lot about the top four countries in the world's cyber-crime index, but we haven't talked much about why they would want to conduct cybercrime… so let's look at some astounding numbers.

13

---

According to the FBI, cybercrime cost the United States over 12.5 billion dollars in 2023 alone. That is a whole lot of money but not compared to the global cost.

--- When we look at the global cost of cyber-crime, the numbers are just staggering. According to the Official Cybercrime Report, 2023 costs were estimated to be 8 trillion dollars. That's more money that most of us can imagine, so let's break that down. That means that cybercrime costs the world 667 billion dollars a month, which is 154 billion per week, or 21.9 billion each day. If we keep breaking that down, ultimately cyber-crime is cashing in about 255,000 dollars per second… which means that these criminals have made over 282 million dollars since we've started this presentation!

--- While that's almost unimaginable, here's another statistic that will put it in perspective. If we were to move all cyber criminals to one spot in the globe, cyber-crime would represent the third largest gross domestic product (GDP) behind only the United States and China. Just for reference, that's about twice the economy of the real 3rd place country (Japan). We are talking about almost unimaginable sums of money here.

--- For a little more perspective, lets bring that all home with the sobering fact that the U.S. has 10.37 connected devices per person. This seems like a lot until we think about our cell phones, laptops, smart watches, and all the other connected devices from thermostats to cars we own. Each one of those devices, and all the data we store and/or share with them, are all squarely in the crosshairs of a very large, and very successful, digital criminal underground.

14

---

Next let's quickly discuss the kinds of attacks hackers are using. The first graph shows us the top three ways hackers are getting in, which we call action vectors. These numbers show us that the top three across all industries are web applications, emails, and carelessness.

--- This second graph from the FBI's IC3 report shows another interesting statistic about ransomware. If you're not aware, in 2014 President Obama's administration identified a series of critical infrastructure sectors that needed to be protected from cyber-attacks, including healthcare. As you can see, healthcare is the sector most impacted by ransomware. These are all attack vectors that we will discuss how to protect your systems from in a few minutes.

15

---

All of this begs the question… so why in the world would the Russians and the Chinese and all the other hackers in the world attack you or your organization? What is it that hackers want from you?

I'm glad you asked!

16

---

Most of us are familiar with Verizon; many of us have our cell phone service through them. But they also have a cybersecurity practice which has produced a Data Breach Investigations Report (or DBIR) annually for the last 17 years. These are really great, and usually cheeky, reports on the current status of cyber-attacks, trends they are seeing, and they include breakdowns by industry.

17

---

Let's take a minute to look at some critical statics for the healthcare industry from the Verizon DBIR.

--- This first chart is the top patterns for data breaches within healthcare. I bet that after what we just talked about with the Russians, Chinese, and organized crime that you expect system intrusion (what you would call hacking) to be number one. But in fact, it's dropped to become the lowest cause of data breaches according to this report.

--- Second here is privilege misuse, which are incidents predominantly driven by unapproved or malicious use of legitimate privileges. For example, a health care worker may have access to patient's charts who they are not assigned to care for but look at their information anyway.

--- However, the biggest threat Verizon found in health care is miscellaneous errors. Remember earlier when we talked about making things too easy for the bad guys? This is what I meant. Let's look at this next graph to see what kind of errors are included here.

--- The top error is mis-delivery – sending private data to the wrong recipient. If we were able to take a show of hands, I bet most of us either know or were part of a situation where patient information was accidentally emailed, faxed, or even mailed to the wrong person. These are simple mistakes, but if that's the results of your pregnancy or cancer test, it probably would feel like more than an "oops!". The second top error is loss… misplacing a patient file, walking away from your laptop for just a minute, or somebody grabbing a briefcase out of your car. The 4th category – gaffe – is when somebody talks about sensitive information in a non-private location. I see this all the time when I go to the doctor… "hello Mrs. Smith, you are here to see the doctor about your cancer diagnosis?" or hearing nurses casually chatting in the hall about the patient they just left.

--- The next chart shows the top attribute varieties of attacks… what the bad guys are trying to get or accomplish. Interestingly, it's not patient medical data… the leader is their personal information. Why would that be you might ask?

18

---

Great question; but before we get into details, here's one more credentials-related statistic from the DBIR. In the US, almost one third of data breaches over the last decade involved the use of stolen credentials. Now let's take a look at what threat actors are actually doing with the personal data they get.

19

---

One thing they want personal data for is to 'pivot' from that information to get to your email accounts, which can lead them to friends and personal acquaintances. This sort of 'data enrichment' allows them to not only do things like figuring out your mother's maiden name, but also gives them additional data points that can be used in everything from figuring out your password to writing better phishing emails (we'll talk about how they can do that at scale in a few seconds). This also helps them because if they can get a password you use, about two thirds of people use the same password for multiple accounts. It gets worse! 50% of people use the same password for all of their work accounts, while 13% of people use the same password for all of their accounts everywhere. To say the least, it starts to add up quickly with those kinds of bad practices.

--- As we hinted earlier, hackers can also use your personal information to find out more about you to better tailor their attacks against you (for example, spear phishing attacks). I mentioned earlier that I'd talk about how bad guys are now doing this at scale, and the answer is Artificial Intelligence. AI allows the bad guys to suck up all the data they steal (plus what we give to them on social media) to make better attacks, from social engineering to phishing. In fact, research shows it makes them not only more likely to craft successful phishing attacks, but it can cost them up to 95% less to create these targeted phishing emails. As a result, professionals expect AI to increase the number of phishing attacks we see by 60% or more.

--- With tailored attacks, then they use that information to get to your finances whether that's your bank account, taking out loans in your name, extortion, or other types of fraud. As we saw earlier, this is really big money and the threat actors will take it wherever they can get it. A great example of how this is used is North Korea (incidentally, this relatively small country is 7th on the WCI index) uses funds from cyberattacks to fund their programs for weapons of mass destruction (estimated to be about 3

billion dollars between 2017 and 2023). It's about more than your credit card… there are some very serious stakes at play.

--- Finally, these threat actors can use the personal information they obtain to disguise themselves as the individuals whose information they have stolen. With enough information, they can use an individual's identity to appear to be that individual online, apply for jobs they might not otherwise be eligible for, or even take out loans. Even more frightening is they can use this data to forge passports and other credentials to allow foreign nationals to enter the country illegally for their own purposes. Unfortunately, these threat actors prefer to find and use personal information from the elderly, deceased, and disabled for these purposes. Why would that be? It's because these populations may be less likely or even less able to detect that their identities are being used for other purposes or, if detected, potentially less able to do anything about it.

20

---

Here's the thing… we really need to be protecting everybody, and I know that can seem overwhelming. At CaseWorthy alone, our products contain the data for 2.95 million people. That's a lot of folks, but we train our employees that it's not about just protecting the company or this mass of people. It's about protecting individuals… people like Nathan.

21

---

Obviously Nathan is a hypothetical person, but he's exactly the kind of person that we, and all of you at ANCOR, are here to protect. We would tell them that Nathan is a real person, a person with dreams and challenges. He's living in a group home, holding down a job, but trying to move out and find love in his life. Nathan is the kind of person that we serve who already has his hands full with the challenges in his life.

--- We have to make sure that his data is safe, and that only him and the people he may authorize have access to his data. Nathan, and the over 70 million disabled people in the US, deserve to be protected. Let's talk about how we can help keep their data safe.

22

---

Our next major section is about cybersecurity basics – what you and your organization can do to stop the hackers. We're going to align this with the action vectors we learned about earlier, talk about specific techniques the attackers are using, and some real things both you and your organization can do to reduce the risk that you become the next cyber victim statistic. We will take these in turn: Web applications, email, carelessness, and ransomware.

23

Let's get started by talking about web applications. Why are web applications such a big deal? That's because we live in a connected society… remember that 10.37 connected devices per person statistic? There are two leading Cloud Service Providers (or CSPs), and the one you're probably most familiar with is Amazon's Web Services (or AWS).

24

---

Looking at this chart, we can see that AWS has grown dramatically in the last three years, almost tripling its revenue in just the last 5 years.

The second CSP is Microsoft's Azure services. When you think about Microsoft the first thing that comes to mind is probably its operating system (which today we just call Windows) that first appeared in 1975 or the ubiquitous Office line of products… not Azure.

However, when we take a look at their revenue chart, we see that Azure is bigger than either their personal computing or productivity product lines and constitutes about 45% of Microsoft's overall revenues. Since they took in just under 212 billion dollars last year, this means that Azure's revenues were around 94 billion last year. The temptation to throw in another Doctor Evil was just too much to resist!

The take-away here is that this is huge business and it's here to stay, and many providers (CaseWorthy is a good example) have moved their applications to being cloud-based to benefit from the scalability and cost-efficiency the cloud can offer.

A quick note on my reference to CaseWorthy: we implement all the controls we're going to talk about today throughout this Cybersecurity Basics section, so yes… we eat our own dog food so to speak. I just wanted to get that out of the way so this doesn't sound like you slipped into a surprise sales pitch. Fear not; I hate when that happens to me too!

Given that, let's look at how we can protect ourselves from web applications.

25

---

There are really two approaches to web app security. The first set we'll discuss quickly is specifically for those organizations that may develop web applications. Recommendation #1 is to use the top 10 list from the Open Worldwide Application Security Project (OWASP) which is commonly referred to as the OWASP Top 10. This is a standard awareness document for developers and web application security based on industry agreement on the biggest risks for developers, and it is updated annually. I'd be happy to show you the list, but since most of us probably aren't developers we can save a few eyes from glazing over in technical jargon.

--- Secondly, organizations need to make sure that their data is secured both in motion (for example, when a user is accessing their data) and at rest (like when its sitting unused on the server). Encryption is the default settings for storage both in AWS and Azure, but you must be sure that they stay that way. Likewise, access to these environments are usually encrypted for data in motion, but the system owners need to ensure they are maintaining the appropriate security certificates and configuration.

--- Third, ensure that you have web application firewalls in place to helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. These can normally

block a lot of common application risks (including several from the OWASP top 10 list) and are certainly a best practice for secure implementation.

26

---

If you're just using web applications, there are also some things you can do to help be secure, starting by ensuring that the web app uses Secure Links.  Here's how you can check.

27

---

In some web browsers, the browser shows you several indicators that you're on a secured site.  The first is the https that we see here.  HTTP, or Hyper Text Transfer Protocol, is the standard for transferring and displaying web data.  The "S" stands for HTTP Secure, so that's something you should look for.  Also, some browsers (for example, this is Microsoft Edge) will also show a lock symbol.

Now, you can also move your mouse pointer over the lock and click to get more information which, in this case, shows that the connect is secure.

28

---

However, not all browsers show either the lock or the https.  This is the ANCOR site in Google Chrome, and you can see that neither the https nor the lock are visible.  However, if you double click in the search bar, you can see the https prefix.  Alternately, you could click on the sliders icon and, just as with Edge, get more site details which will confirm that the site is secure.

29

---

Next we have Mobile Devices.  This may seem odd to include in web application security, but the reality is that a lot of business today gets done on mobile devices.  This has a few serious, but easily overlooked, impacts on security.  First of all, everything is going to be smaller so its easier to not pay as close attention to things like whether or not you see a lock symbol or https.  Secondly, almost by definition you're in more of a hurry when working off your mobile device and that makes us even less likely to pay attention to those same details.  Third, we tend to not get the same nagging reminders to update our mobile devices that we do with our laptops, so security of the applications we have installed might also be circumspect.

Ultimately, it's important that organizations attempt to have some control over mobile devices that connect to their systems or data.  I realize that we don't have time to get in the holy war about mobile device management vs mobile application management, but I will say that at CaseWorthy we decided to implement MAM.  Incidentally, if you're currently a Microsoft customer you can use Intune to implement MAM pretty easily and it is  already included with subscriptions to Microsoft 3 65 E3, E5, F1, and F3, Enterprise Mobility + Security E3 and E5, and Business Premium plans.  If you are listening to this recording after October 24th, 2024 you might want to check that since Microsoft likes to change it's licensing every few hours to keep everybody on their toes.

--- Another important web application security control at the organizational level is due diligence. It's been a real buzz word for supply chain management within information security for several years now, and after our earlier discussion about how the F-35's plans were stolen from Lockheed Martin through some of their affiliate contractor organizations, it's easy to see why. As you see from this DBIR infographic, 15% of the breaches they researched involved 3rd parties. You just need to make sure that you are checking out the providers you plan to do business with ahead of time to make sure they're implementing critical security controls (for example, everything that we just talked about for developers) so that you have a reasonable level of assurance that they are dedicated to the safety of your organization, it's data, and the data of the people we all serve.

--- Last, let's visit the merits of good old-fashioned Skepticism. What I mean here is that I want you to think and pay attention when you're using these applications online. You don't have to be a security expert to know when something is off with the system you use every day. When you see something that's off, odd, or just seems not quite right, trust your gut instincts and report it to your security or IT team. As Henry Kissinger remarked in jest, "even paranoids have enemies"… so there might just be something sinister going on. Keeping alert is a great way to stay safe, so if you see something, say something about it.

30

---

The next action vector up to talk through is email.

31

---

Most everybody is familiar with the dangers of phishing attacks at this point, so we won't go through that in too much detail. The normal indicators to watch out for with phishing emails are what you would expect: Look out for red flags like poor grammar, misspellings, and suspicious URLs. Always be cautious of unsolicited emails, especially those that request personal information or urgent action. That sort of thing; you know the drill.

--- However, there may be a relatively new one that you don't know about – favicons. While that sounds like a cool new sugary bubble gum for kids, it's short for "favorites icon" and a term for that little branding icon associated with a web page that you see in the top tab of your web browser.

--- You see them all the time (here's the one for ANCOR's web site), and it's a great little marking graphic that is common for most professional websites:

--- Google, CNN, Amazon, and even the White House… even though you may have not consciously noticed them. When visiting a website, quickly scan for the favicon to ensure it matches your expectations. If the favicon is different or missing, you should be suspicious, and it's an easy check to make sure you're on the site you think you're visiting.

32

---

Another really important action to help with phishing is regular phishing training for your users, and by regular I mean monthly. As you see from the DBIR demographic, it takes less than 60 seconds for users to fall for a phishing test. Many organizations want to just do one per year to check the proverbial box,

but the reality is that threat actors are sending 3.4 billion phishing emails every single day. You MUST train your organization's users just as hard to protect the Nathans of the world. While there are some limited free options out there, this is something worth putting in your fiscal year 25 budget if you don't already have it. I have two links at the bottom of the page to help you. One is a Forbes article about some of the best phishing simulators. The second is a free whitepaper I wrote about setting up a security training program in the human services industry that you may find to be helpful.

33

---

The next way to protect your organization from phishing is to implement three email authentication technologies that are relatively simple to implement but can really help protect against both phishing emails and SPAM. These three tools are called SPF, DKIM, and DMARC; let me tell you how they work.

SPF stands for Sender Policy Framework, and it is like getting a security certificate. SPF tells everybody else that emails from your domain are who you say you are… like a "guest list" for email servers. It tells receiving mail servers which servers are allowed to send emails on behalf of a domain. If an email comes from an unauthorized server, it may be flagged as spam or rejected.

DKIM, or DomainKeys Identified Mail is a kind of email "signature." It adds a digital signature to emails, proving that the email hasn't been altered and that it was sent by an authorized sender. This helps verify the authenticity of the email.

Last we have DMARC, or Domain-based Message Authentication, Reporting, and Conformance which acts as the "bouncer" that enforces SPF and D KIM. It lets domain owners tell email providers what to do if an email fails SPF or D KIM checks (for example, block it or send it to spam). D MARC also provides reports to you as the domain owner about fraudulent emails using their domain.

Together these are simple but powerful ways to protect your senders and recipients from phishing attacks, spam, and other types of email fraud. The first link at the bottom of this page will help walk you through the process of setting these up in your environment, and the second is a tool that will help you check to make sure you did it correctly.

Word of caution: Setting this up is pretty straight forward but you need to remember to update it if you make changes to your other mail records. Also, it's not uncommon for smaller health care organizations to not have their SPF, DKIM, or DMARC configured which can flag them as potential spam emails. However, I've found that the benefits of the protection these technologies provide is well worth the minimal work required to have them working for you, and the best part is its free… you just have to set it up.

34

---

Let's move on to Carelessness! While I'll admit this is probably the oddest topic I've ever formally addressed in a forum like this, as we saw from the research it's a big deal. In fact, the DBIR has this stat for us: 68% of all breaches involved a mistake a human made. Let's look at some empirical ways we can address this risk.

35

---

This may feel like it belongs somewhere else, but after years of experience in this field trust me… it doesn't. Even if your organization has fully automated software patching, people will still wait as long as humanly possible before rebooting their computer or re-launching their web browser and chancing losing the 37 tabs they've had open for a week.

Now, this DBIR graphic shows us that not only is this a larger problem for all sectors, its one that the threat actors are actively exploiting. In fact, the number of breaches that started with an unpatched software vulnerability almost tripled from last year to 180%.

So what can we do to reduce the risk of unpatched software vulnerabilities? Some of the answers might surprise you. Of course, we need to make sure that we're patching systems regularly, including third party patches and updates. Some of you might be saying to yourself, I'm great at keeping up with patches on my laptop. But what about your home router? How about your smart TV? Any connected system needs to be patched regularly, including firmware. You also need to make sure that any critical patches are implemented ASAP, even if you have a normal monthly patching cadence. If a patch gets a critical rating, there's a reason and the bad guys are just betting that you won't care.

--- As we discussed a second ago, it's possible to automate much of this. We mentioned Microsoft's Intune earlier in reference to Mobile Application Management, but Intune (part of the Microsoft Configuration Manager) can also be used to help with patch automation and deployment if you own that product. If not, the link below has an evaluation of some other patch automation tools you might consider.

--- The second tip seems simple and common sense, but it's not. You need to make sure your organization has a complete inventory of all devices that need to be patched, and also check that they actually get patched. I will never forget an incident response engagement I had some years ago for a world-leading manufacturing company. They had been hit by malware, but they only had maybe 10% of their systems documented. So while this malicious software was running rampant through their network, literally destroying computers one at a time, our team was trying to figure out how many devices they had and where they were instead of working to contain the outbreak. The net result was a lot of unnecessary damage and time lost for production, and that's a lesson that would be hard to forget.

--- Finally, just because you have an automated patching system doesn't mean it's hands off. You still need to make sure you have a test pool of servers and laptops that you can test some of the more critical or impactful patches before you roll it out to your entire company. Trust me on this one, sometimes you can't reverse the damage that a legitimate and well-intentioned patch can do in a matter of milliseconds.

36

---

At this point you're probably asking why passwords could be careless? In the "you can't make this up" category, here's a real photo I took a few years ago when I went to a regional security conference at one of the member company's headquarters. When I sat down, I realized I was sitting next to the conference room's presentation computer and look at what I found on the keyboard… the username and password. Now, given a little bit I knew about the company I was able to break that password's structure down and when I … ahem… went to the bathroom, I was able to login to every unattended computer I found along the way. Just amazing.

Yet, this is the kind of carelessness we find because let's be honest, people hate passwords. As a result, people tend to pick simple or repetitive passwords (or even write them down on sticky notes). But let's take a look at the next slide where I can prove there's a better way.

37

---

This chart shows how long it takes to break (or crack) a password based on the number of characters and password complexity with modern hardware and software. If you brute force (a hacking method that uses trial and error to crack passwords) an 8 character password that requires numbers, upper and lower case letters, and symbols, that password can be cracked in less than 40 minutes.

--- However, if we take a long pass phrase like "The Hills Are Alive" (yes, I love the Sound of Music too) with no complexity requirements, that password would take 11 trillion years. Now, I'm not the best at math but I can figure out which one is more secure. Not only that, I have no problem remembering the longer 17-character password, but not so much with the complex 8-character one.

In fact, the National Institute of Standards and Technology (NIST), the organization that first gave us the complex 8-character password recommendation in 2003, recently changed its recommendation to drop both password complexity and reset requirements in favor of passwords with a minimum of 15 characters that are only changed if compromised or forgotten (see the linked article for more details).

38

---

Identity has three main components:

- IDENTIFICATION: Finding out who the user is
- AUTHENTICATION: Proving who the user is
- AUTHORIZATION: What resources the user is granted access to

Multi-Factor Authentication (or MFA) brings Identification and Authentication together to fix the password problem. There are four ways to identify who you are for MFA:

- KNOWLEDGE: something you know – for example, a password or PIN.
- POSSESSION: something you have - for example, a proximity card, security certificate, or registered device.
- INHERENCE: something you are - for example, an iris scan or your fingerprint.
- LOCATION: somewhere you are – for example, your physical location or unique IP address.

MFA requires at least two different types, and this makes it much, much more secure than a password. MFA is beyond just being a best practice now, MFA is generally a requirement. Not only should you be using MFA at your company, but you really should implement MFA on all of your personal accounts as well. The one other piece of advice is to stay away from text message based MFA. Text messages are sent by a technology called SMS which stands for "Short Message Service" and it's entirely unencrypted.

39

Our last topic here is Physical Security. Why is that a big deal? Beyond the obvious life safety issues, it's easy to forget in our highly connected and digital world that sensitive or personal data is still sensitive or personal whether its on a server's hard disk drive or on a sheet of paper sitting on the printer. This is usually easier for the medical community to get because there's still so many paper medical records in use (everything from your patient folder to prescription slips).

The first thing we need to do is make sure that your organization has, and enforces, a clean desk policy. All sensitive information should be returned, filed, or locked up as appropriate when employes leave their desk at the end of the day so that unauthorized eyes don't see what they should not.

--- However, even when you are working on something you should make sure that the data isn't viewable by others who are not authorized or don't have a legitimate need to see that data. This is everything from making sure your monitor is turned away from people so they aren't looking over your shoulder (this is called shoulder surfing) to covering documents that you're not currently using.

--- The best rule is this: just be careful and treat the data you have as if it were about you or someone else you care for.

40

---

All right, now we're down to our last action vector, ransomware. Recall our earlier graph from the FBI that last year the healthcare sector was the leader in ransomware attacks, so let's talk about how we can reduce that risk.

41

---

The first thing you need to do to help protect against ransomware is make sure you have good network segmentation. This is harder for many smaller healthcare organizations who don't have the financial or IT resources to do this well. However, there are a number of relatively cheap firewalls that can be used to set up such a system, and we've included some links at the bottom to help you understand how that works. But essentially, you want to separate the three major zones of your network: your data is logically separated from your applications, and your applications are logically separated from the internet (this area is usually called your De-Militarized Zone, or DMZ).

The second point here, zero trust networking (ZTN for short), goes back to the identity model we talked about a few minutes ago during MFA which has three components: Identification, Authentication, and Authorization. If you recall, MFA helps us with the identification and authentication parts, but not authorization. This is another one of those issues that we could do several full-day seminars on, but I recommend that you follow the link for Google's Beyondcorp initiative if you want to learn more about how to implement ZTN.

--- However, the critical control for ransomware is to have great backups. I remember the first ransomware client that I ever helped with an incident response exercise, and one of our first questions was about their backups. Oh, we have great backups of all our critical files they said. However, what they didn't know was that one of the engineers had moved what they thought was an insignificant folder to a location that wasn't being backed up. This ended up being 50 years of mechanical designs that the company had just recently completed a 5-year project to completely digitize so they could produce them in their automated system. Unfortunately, they had not backed those files up for so

long that all copies had been written over and they were unable to recover those files. It was a horrible experience to see them realize the kind of trouble they were in.

As a result, here's some best practices to make sure you have great backups. First of all, you need to have offline backups. That can either be physical copies or tapes of the data that are not connected to the system and stored off-site, or it can be a cloud-based repository that is only connected to the network while backup jobs are running. Next, you need to make sure that you are regularly checking to verify that all the back-ups you think you have been actually running successfully. Finally, you need to periodically, no less than annually, test your ability to restore your systems from those backups. Trust me, you do not want to have to hold your breath for 4 hours during the middle of a business threatening ransomware attack because you don't know for sure your backups are going to work.

--- The last item for ransomware encompasses many of the security fundamentals we've already talked about this afternoon. Training your users to recognize and report phishing emails, keeping your computers and systems patched, good security around your passwords, and awareness around what to do, and making sure that all systems have good and updated anti-virus software are all very important to protecting against ransomware.

42

---

All right everybody, congratulations… we made it through! Let's do a quick review of what we've covered then we can open this up to a little Q&A session.

--- Wait, wrong meme!

Now, because you are all literate adults and because I'm tired of talking (thank you to everyone still paying attention enough to laugh at that), I'm just going to flip through the review…

43

---

…which covers all we discussed about hackers, where they are from, what they're doing, what they want, and how they're using your data as well as …

44

---

the four action vectors: web applications, email, carelessness, and ransomware.

45

---

As promised when we stated, I have also included a set of references for you. The next few pages have key resources for addressing the four action vectors…

46

books & blogs I mentioned along the way (including some additional material in this month's CaseWorthy CSAM blogs that didn't make it to our presentation today)…

47

---

…as well as links to articles I referenced throughout our little talk today.

48

---

And finally, thank you all for attending this webinar and I appreciate ANCOR giving me the opportunity to share with you today.  We will take a few minutes for Q&A.

Please note, because I still can't talk, I'll answer your questions through our Q&A so please open that up if you have not yet done that.  Just in case we do not have time to answer all your questions, I've also put up my contact information.  Feel free to reach out or connect with me even if you just need to know the name of another good book on information security.

49