NCSBN
Leading Regulatory Excellence

2018 International Nurse Regulator Collaborative Symposium - How Will Regulators Respond to Mission Critical Risks? Video Transcript

Event
2018 International Nurse Regulator Collaborative Symposium

More info: www.ncsbn.org/12007.htm

Presenter
Donnie Woodyard, MAML, NRP, COO, National Registry of Emergency Medical Technicians (NREMT)

- [[Donnie]] Good afternoon, I really appreciate the introduction. It's great to be here, I value the partnership that we have with NCSBN and with our colleagues around the world. As stated in the introduction, I have the day job in the role of being the [[00:00:30]] Chief Operations Officer for the National Registry of EMTs. In many ways, we're similar to what you do, except we look at the EMS personnel across the nation, EMTs and paramedics, we have some levels in between that as well. And we do that for both state partnerships, federal, and military across the whole nation. We also have some international partnerships that we work on, we are the credentialing body for emergency medical services personnel. Much like you have an exam, we have an exam. We provide the credential that then is translated to a state license.

So today, I want to talk about responding to mission-critical risk. And, in today's society, one of the key mission-critical risks that we are faced with is the risk of cyber threats. And I want to talk as an executive to [[00:01:30]] an executive to you, I will share some specific examples. I have three case studies we'll work through, all three of the case studies are within the past six months that our organization has dealt with. I hope to, one, raised awareness for you on the types of cyber activity and the risk that brings to your organization. Number two, I hope that I can prompt you to start thinking about your role as a regulator [[00:02:00]] in responding to these risk and how to prepare yourself.

A quote from 2012 which in the words of cyber is decades ago. Okay? But, in 2012, the US House Intelligence Committee Chair said, "There are two types of companies," and I would say there's two types of organizations, "those that have been hacked and those that have been hacked but don't yet know it." [[00:02:30]] I would say that that goes the same and the truth is the same for regulatory bodies, for organizations, for licensure agencies, for governmental entities. There is no differentiation based on if you're a company or not.

As mentioned in my bio, I had the great pleasure of living and working in South Asia for nearly a decade, had a number of rows there [[00:03:00]] helping to bring health systems and work with health systems. The picture here is a picture I took and it's of a tea estate and it's overlooking the Lipton-tea estate in Sri Lanka. Beautiful area, I absolutely loved living and working there. And you see the beautiful tea. I note that we have a tea break, this afternoon, I'm sure that we'll probably enjoy some tea, most likely from this area of Sri Lanka, Ceylon for others may know it as. [[00:03:30]] But I note, up at the top, well, what's the price of tea? And I would suggest the price of tea is a fortune. And let me tell you why. In 1843, Robert Fortune, you may know this story, Robert fortune was a British botanist. And at the charge of a lot of influential people, I'll just leave it like that, he went to China [[00:04:00]] because, at the time, China was the only place that grew tea. So he went to China on a mission and his mission was to identify how you make tea and he knew he needed plants but it was also a process. In 1843, Mr. Fortune went and he stole, not only the tea plans, but the technology and the mechanisms to make tea, exported it out of China, took it into other [[00:04:30]] countries, and started growing it there. That's a well-documented case of corporate espionage.

Now we enjoy tea and I was certainly grateful for tea in Sri Lanka, [[inaudible 00:04:44]] some of the best tea I've ever had there but, in 1843, that happened. Over the next few minutes, I'm going to walk you through a process that's going to look at a very similar activity that's happening in our organizations. And my question is, well, [[00:05:00]] who is looking at your fortune? In 1975, it's estimated that the wealth of an organization, 83% of the wealth of an organization, was determined by tangible assets. So be an organization or company, it was tangible assets. Today, the wealth of an organization, nearly 85%, is that of data. It's intangible assets. We've had a [[00:05:30]] tremendous change in where our wealth is. As a regulatory body, your wealth, your value is largely in the data that you hold. In my current position, we have two million-plus records of personnel who are EMTs, or paramedics, in the United States, and many are around the world. You have similar records in your accounts.

So who is trying to look at this fortune? I want to [[00:06:00]] break this up into four primary groups. One is nation-states. Two is organized crime and hackers. Three is hacktivists. And four is inside threats. And we're going to walk through some of these. So, first off, a case study. Welcome to Our New Executive Director is the name of this case study. Many of you may know, some of you may not, but we had the [[00:06:30]] pleasure of appointing a new executive director to our organization a few months ago. We, like many of you, we put out a press release. You'll see, here's an example of the press release. This actually came out in April...I mean in June of last year, and it's a standard press release. It includes the name, some of the information about who he is, his title, and, at the bottom, you'll see there's a start date. [[00:07:00]] Bill Seifarth, bottom paragraph, [[inaudible 00:07:02]] four executive director responsibilities in August. Okay? Now a pretty standard press release. We should share information. However, for the hackers out there this is the beginning of an opportunity. I'm going to show you how this opportunity develops. I hope, as leaders in your organization, this rings a bell to you.

So August 24th was his first day in the office, [[00:07:30]] we said that in the press release. So August 24th, we did what most organizations do, we updated our website. So we updated our website to say, "Hey, congratulations in our leadership team. He's now the executive director." In addition to this, on our website, we list the other personnel that are in leadership roles in the organization. You probably do the same. We list their name, we list their title, we list what's their background. [[00:08:00]] This is our CFO, we say that she's a CPA, where she went to school. This is a goldmine of information for a hacker.

So let's move forward, September 17th. This is a screenshot from my cell phone, and, on my cell phone, on this morning, it so happens that our new executive director is on travel. So he starts off and he talks about a town-hall meeting and [[00:08:30]] we're trying to organize when we're going to do it. The second email is a draft of the Pulse, the Pulse is an internal newsletter that we have in the organization. Then you see a third email, then the fourth email is "Take two," he made some edits on an attached document. Look at the third email there. Do you see anything, if you were just quickly going through on your cell phone, any thing that sticks out on that? I know he's out of the office, I know he's traveling, [[00:09:00]] and he says, "Hey, I need a couple of physical iTunes gift cards." Okay, see it? And then, I get a follow-up email, "Hey, are you in the office? Thanks." Well, there's a problem. The problem is Bill sent three of those emails, he did not send the fourth. The fourth, if you double-click [[00:09:30]] on the title name, you go in and see that this email is not our standard email but it's from some email called ceomail@scripsnetworks.com It looks like it's from Bill, it was timed for the day he was out of the office on travel customized. This person did not only send these emails to me but they also sent it to our CFO and two other people. [[00:10:00]] And our CFO says, "Hey, this kind of looks weird," multiple people were targeted. Here's the key takeaway, our staff recognized that this was not a legitimate email, they raised the flag, and they stopped this potential attack right when it was trying to happen.

So what type of attack is this? This is something that's very common, I guarantee, if you're in a position of leadership and if your information's out on the web, [[00:10:30]] someone's probably targeted you or they're crafting a campaign very similar to this. And it's a campaign where they do research on your organization. This is not a random email that comes in, someone has researched you, they've researched your organization, they know who report to you, they know what you're responsible for, and they're going to craft a series of emails or messages that look very legitimate that ask you to disclose [[00:11:00]] either information, transfer money, disclose a company's secret. And, in the day and age when we're all connected, it's very easy, as you're going through your emails, to quickly do a response without thinking about it. In the cybersecurity realm, this is called a spear phishing and, specifically, a whaling attack. It's a whaling attack aimed at the wealthy, the powerful, the prominent, the C-suite, [[00:11:30]] the executives, usually with some type of an urgent or time-sensitive message.

Now you may be saying, "You know, I'm not going to go out and buy an iTunes giftcard." Yeah, I didn't, you know, and I was like, "Yeah, that doesn't look right." Okay? However, these type of accounts, these type of attacks happen on a regular basis. We have to be vigilant 100% of the time to prevent an [[00:12:00]] attack. And that's not just you but it's every one of your employees. The attacker just needs one opportunity to get in. This is an estimate from Symantec Corporation, the number of malicious emails a user receives per month, in the C-suite, is estimated somewhere between 10 and 20. And this isn't your everyday spam, these are emails targeted to you.

Okay. So what's the impact? [[00:12:30]] The US FBI issued out a statement that says they estimate that this is accounting for approximately five billion dollars a year [[inaudible 00:12:40]] to organizations. A University, in Canada, had someone receive an email and they wired nearly 12 million dollars as a result of this process. And that's going through a whole series of checks [[00:13:00]] and balances. During this presentation, I'm going to give some examples similar to my own organization and others, not for the purpose of embarrassing anyone, but for purpose of drawing attention. These attacks happened, these attacks continue to happen, they're highly-highly sophisticated, and it's very easy for an attacker to weave through the system. Imagine, in your role as a regulator, [[00:13:30]] maybe they don't ask you to buy an iTunes giftcard but maybe they ask you to send a summary of the latest test resorts, or cognitive exam resorts for licensure? Maybe they ask you to send a list of, "Hey, I need the mailing list of all the nursing directors in the state or in the province." It could be something as simple as that.

Case study number two. I encourage everyone [[00:14:00]] to protect, adamantly protect your credentials. Just by a raise of hands, how many of you know the answer? How many of you have an email account? Obviously. How many of you have a work email account in addition to a home email account? How many of you have access to sensitive information that would be otherwise considered compartmentalized or highly [[00:14:30]] sensitive at your work email? Absolutely. Okay. How many of you have a tough time remembering passwords? Don't raise your hand on this one. How many of you have ever written down a password? Don't raise the hand. Yeah. How many of you have your passwords typed in a text message on your phone? Don't answer it.

In this example, in the first part of the example, I'm going to talk about [[00:15:00]] this picture right here. You know, as a regulator, as an executive, there's a balance that we want to do with public relations communication. You know, I'm responsible for our communication and public relations, and our PR people would love to come and get those action photos in the office, you know, "Hey, let me get an action photo in the office. I don't really know what that means but, you know, can I get a photo of you at your desk or answering the phone [[00:15:30]] or maybe in our customer-service center? Can we get an action photo? Can we get something there? Maybe you are doing something special in your building, you're opening up a new building, or you're [[inaudible 00:15:40]] a new employee."

I encourage you to look very carefully at these photos. In the photo, that you see here, this is a photo of a state employee posing in front of a data system. Now, obviously, there's [[00:16:00]] information shown on the screens, it looks somewhat okay, I mean maybe. You know, there's a video, there's a map, some other things. But apart from that, does anything, on this screen, look out of place for you? It looks like a typical photo someone may take, right? Maybe for some type of a press release or a news release. Let me zoom in a little bit. So, right there on the screen, [[00:16:30]] is a sticky note that has the word password at the top and it has the password below. Now if you look hard, you can read that password, I don't know if they've actually changed this or not, this is not my employee, so I'm not going to say what that password is. But this is a password for a secure system and it's on a sticky [[00:17:00]] note. Okay? Now we may say, "You know, that's not what happened to me." The FBI spends a considerable amount of time working on corporate espionage because there are entire groups of hackers looking at corporate photos, zooming in, looking for credentials, looking for sensitive data.

Let's talk about our experience. [[00:17:30]] I mentioned before, we have a couple million people that we credential. With those couple million people, we, in our organization, have 1.5 million user accounts. So that's 1.5 million individual user accounts, any given time. Some accounts are for individuals, some accounts are for regulators, some accounts are for instructors. All different levels. We had, a few months ago, one [[00:18:00]] credential stolen. The credential was written down on a sheet of paper, in an executives' office, and we believe that, through an employment action, another person was released and the credential disappeared, the sheet of paper disappeared. We were not informed of that, it wasn't known, at the time, until we got a call, a few days later, saying, "I think [[00:18:30]] something's happened because I just got credentialed but I've not taken your exam yet." That's a big deal. So we went through and there's one credential translated in 800 records being accessed. So now, we have an unauthorized superuser that's in the system, they accessed 800 records. Now, we conducted a very thorough investigation, we were able to go through and see exactly what IP address was used, [[00:19:00]] we were able to find out exactly what type of device was used, we were able to geo locate the device that was used, we were able to find exactly what network they were on, we were able to find out that this person was probably sitting on their couch at home, and triangulated it to that. Eight hundred records. Data manipulated. We had the forensic evidence.

That's one example of a breach. [[00:19:30]] It can happen anytime, any day. You might have a super-secure system but you have to have a super-secure system that allows you to get in and do your job. And so, many times, we are the Nexus of that attack. You know, I can have our team create a system that no one could ever get into, but what uses this system if no one can get into it? Okay? I can put in extra requirements, I could have you have a password, [[00:20:00]] plus a two-factor identification, plus a thumbprint, plus a face ID, and, 20 minutes later, you're trying to get in. Would you use it? Maybe not.

If you're hacked, here's a resource that I've used in the past. I have no affiliation with the organization that does this, or the company, but it's a breach-level impact. I have found that this is a very useful tool, I found it to be very accurate. And you can just [[00:20:30]] do a search online for breach-level impact and you can calculate a risk score. So, on this particular impact here, I put in about 900 accounts who were breached. And a breach, by the way, doesn't mean that it's someone just hacking into your system, it could be an unauthorized access by someone who shouldn't have access, like happened here. So about 900 records. Identity theft was a possibility. Social Security numbers, PII, other [[00:21:00]] information is there. Source of the breach is a malicious insider. And how was the information used? Well, action was taken, we know that some people accounts were updated and they had the requirements for credentialing, and they didn't. So this is ranked as a breach-impact score of 5, critical.

As executives and regulators, cyber security is not just the responsibility of your IT [[00:21:30]] team or your CIO or the data department. Cyber security is a responsibility that is shared and it has to be shared amongst everyone in the leadership role. Determining how to make a response to this incident was not isolated to IT. This is an organization-wide impact. If you look over here, on 5.0, it says, "A breach will likely create short to [[00:22:00]] midterm exposure to the business." I'll talk about this actual incident and what it caused. Legal and regulatory impact. Tens of thousands of records sometimes are accessed. Some breach notification and financial loss will happen. Absolutely.

[[inaudible 00:22:20]] what happened with our experience. So this was one regulator in one state that had a credential stolen. [[00:22:30]] Well, unfortunately, it's not limited to one state because we know that we live in a mobile society. People move, people go state to state. And, in this example, those 900 records from one state office actually impacted 26 states. We had to do 26 notifications to the Attorney General's Office based on one breach. It resulted in over [[00:23:00]] 960 total notifications that had to go out. We ended up setting up a dedicated 24-hour seven-day-a-week call center, we offered every single person two years of paid credit monitoring and legal restitution services for the breach. And, by the way, we were lucky. And I say that tongue-in-cheek, who had two people who were under 18 [[00:23:30]] because, in our service line, you can be under 18 [[inaudible 00:23:36]] your education. And if you're under 18 and the cyber breach happens, you get to own responsibility for their entire life. There's no statute of limitation in some states. So we have two people that, if something happens 50 years from now, theoretically, they can come back [[00:24:00]] and link it to us.

So that's an example. Think about this in your organization. Think about the impact. Perhaps you say, "Well, that's okay but I'm a state, or I'm a federal entity." This is where I implore you, you have a joint responsibility with your partners to protect your credentials. It's not something that's just isolated to your organization, it's your organization, [[00:24:30]] the partners you work with, the other state offices that you work with. So here, in the US, many of you probably recognize FOIA, Freedom of Information Act, our organization is not subject to FOIA because we're not a state entity, we're a partner with states. However, the moment we did the notification to the Attorney General's Office, guess what, that now becomes subject to FOIA and is [[inaudible 00:25:00]]. [[00:25:00]] So soon after we did this, notifications went out and now we get to be part of a report that lives forever that says, "Identity Theft Resource report, Data Breach Stats," there we are at the bottom. And now your event is public. So part of cyber security is protecting the information and preparing for the breach and think about the organizational risk and harm associated with that.

[[00:25:30]] As I mentioned before, it's a constant balance between security and usability. A very usable system may be a system with no security controls in it. A system that you can't use is useless. How do you find that middle ground? As regulators, I would say, it's a partnership between you and the organizations you work with, between you and the executive suite, or your leadership role, and the departments or agencies that you work [[00:26:00]] with in and of your own organization.

Let's talk about from a healthcare perspective. This is a memo issued by the FBI, April 8th, 2014, and it reads, "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain." Right now, today, on the dark web... I encourage you not to go there, it is dark... but, on the dark web, [[00:26:30]] a stolen healthcare credential, one of your credential, sells for about $10. A credit card number, and you know the damage that can cause, sells for 25 to 50 cents. Yeah, your credential, your login information is a very high high high priority. It's running 10 to 12 times that of a credit card number. People are looking out for your login information and, [[00:27:00]] as a regulator, you're at the very top of that chain. Because if they can get into your system, then they have hit the jackpot of other credentials. Okay?

Case study number three. I call this one, "Design, prepare, and attack." Any given day, we have, on our website, a functionality that [[00:27:30]] many of you probably have. In fact, by a raise of hands, how many of you have a web portal or something, on your website, where someone can go to and say, "I want to check the credential of someone that you regulate." Show of hands. Yeah, we had that, we still have that. We can't function without it, that's in our charter, that's in who we are, that's in the law, we have to have that. Okay? This map shows, any average day, [[00:28:00]] the number of requests that are coming through our public part of that web site. Okay? And these are rounded by thousands. But you can see that, across the US, we have regular information requests, every day, occasionally, some in Europe or Asia, other parts of the world, that's common, we have people that travel. Okay? However, on one particular Sunday, a few months ago, I started getting alerts on my telephone and the alerts said, "High [[00:28:30]] traffic alert." Now we have our system set up that tells us that. And this is what happened. So let me go back. So that's normal. That's not. Okay? So what's going on? This is an example of another type of cyber activity. Now the good news is our site called it, blocked it. It's good, okay? So no [[00:29:00]] protected information was compromised during this. But an entity, most likely a nation-state, in this particular incident, targeted our website. And they said, "Hey, you have information of people that we would like to have." And they target our website, they wrote very specific code, and they tried, over a series of weeks, months, to break the website. And they finally wrote one piece of [[00:29:30]] code and they said, "Do you know what? We think, if we hit it, we can get in and get out with the data really quick." So they leveraged over 1,000 different access points to hit our server at the same exact time with a piece of code to try to go in and get information. Because, on our website, we already had security running that, if you try to make too many requests, you were shut out, if you try to request us, you know, information [[00:30:00]] that failed because you didn't have the name right, you got shut out. So what they designed is this plan that says, "Hey, we're going to just go from all over the world, attack, and see what we can grab." We use a combination of machine learning and artificial intelligence, combined with a team of really good people, to try to prevent against attacks like this.

So a question is were we the target? [[00:30:30]] Sort of. Maybe. The slide I'm showing you is a declassified slide that's out there through the national partners for cybersecurity. But this slide talks about the anatomy of a modern-day cyber threat upon a regulatory body. And it talks about how these threats happen. Let me walk you through this, this is important to understand. So yes, we were the [[00:31:00]] target of that particular attack, that I showed you on those slides, but we may not be the ultimate target. And let me explain why. On the middle of the bull's eye, is some high-profile entity. In this particular case, that is a component of the federal government. I know that this is an international audience, that could be a component of your government, it doesn't have to be the United States government, the same theory applies. [[00:31:30]] So it's a high-profile that they're trying to get to. What you see, as you move out, is a combination of vendors, service providers, partners, utility companies, etc. And so, the hackers are saying, "I want the information that's highly protected right here. I know that's difficult to get to. So what I want to do is I want to try to attack a partner. And if I can attack a partner, or 1, 2, 3, maybe 10 partners, maybe 20 partners, [[00:32:00]] I want to [[inaudible 00:32:01]] a partner and I want to try to get them because their security is easier to get through. And once I get their lists and their data, I can cross-reference that with another one and cross-reference that with another partner, and maybe I can identify someone who is within that realm that is closer towards the bull's eye. So maybe, you know, I start here and I get down here, down here," and they get closer to that bull's eye. Think about the people you regulate. [[00:32:30]] Think about where you lie within this bull's eye. Do you regulate people who also are, maybe they're a nurse, but maybe they work with the government? Are they a nurse and work within the state or are they a nurse and work within the military or in the police? I know that we have people, in all of those realms, that we regulate and that we credential [[00:33:00]] from the most closest points to the US-government leadership that you can imagine.

So, within this paradigm, your data is extremely valuable, absolutely extremely valuable. So you are a target but you may not be the ultimate target, you may be a vector for someone else. [[00:33:30]] As a regulator, as executive, it's important for you and your team to know your numbers. And what do I mean by that? On the graph, right here, we use a series of dashboards, that our team has created, that we can see what normal is. So we know, on any given day, how our services are functioning. We know how many people are on our website, we know how many emails we get, we know where they're coming from. We know all this. So when we see a spike... And this is an actual screenshot [[00:34:00]] of one of our business analytic methods showing the attack on the map from a couple slides ago. So you can see that it went from baseline here all the way up. And you can see a couple of notches here where they were testing their system.

So it's important for you to know your numbers, number one. Number two, leverage artificial intelligence, machine learning, current technology. And number three, have a rapid-response plan. [[00:34:30]] I'd encourage you to think about, for a moment, what is your response plan in your organization, your office, your entity, if a cyber attack happens? What do you do? Who do you call? Who's the first person you call? Do you have their cell phone number? Okay. Who's the second person?

Who's the team that you're going to assemble around your table? What type of team members are you going to assemble? Is it only [[00:35:00]] IT? I would encourage you think about IT, legal, public relations, many many different people coming together. "Cybersecurity itself is not just a technical issue, it's a business imperative," it's an organizational imperative. This was from the first Chief Information Security Officer of the United States a few years ago. As regulators, as leaders, [[00:35:30]] it's absolutely important. It's not a US issue alone, it's a global issue.

As you see, up here, this is a simple 2-minute search on Google, and that looked at cybersecurity breaches. Now I want to walk through these real quick. In the top right, or your top left, you see a professional hack. So this was a professional hack on the Norwegian health system. [[00:36:00]] Three million patients, a huge impact for the Norwegian health system. Accenture, down here, had a misconfiguration breach. [[00:36:11]] Over here, "Bupa fined 175,000 after staffer tried to sell customer data on the dark web." Okay? So an insider said, "Hey, I have accesses, information. Ten dollars a credential sounds pretty good. I can, you know, have [[00:36:30]] access to," choose your number, "10,000, 5,000, a million records, insider attack." Here in the United States, government security breach, Social Security numbers. Singapore Health, server missed critical updates.

The issue is not isolated, it impacts all of us. This is a sample from IBM, and let me just walk through this. Over on the left-hand side, you see [[00:37:00]] 2015 through January of this year, the key I want to point out here is that attacks are happening for a lot of reasons but the reasons are morphing, shifting, and changing over time. Right now, we're facing a crisis of misconfiguration. A few years ago, in our organization, we made a switch from on-premise servers to [[00:37:30]] the cloud. And I'm not going to try to explain the cloud but we made that switch. And it was the best thing we've ever done, it was great. Okay? But it's a whole new type of technology meaning that the people who used to manage our on-premise servers, all of that knowledge is not immediately transferable to the cloud. It's a different way to manage. And so, in our organizations, and if you're leading an organization, [[00:38:00]] maybe you're at a state office, you know, and you're talking with your state IT personnel and they're like, "Hey, we're going to go to putting our records in the cloud." "Hey, great. A lot of benefits, I am so glad we did it." But, in the back of your mind, if you're around the table, there are questions you can ask. "Hey, how are we changing our approach to cyber security?" you know, "who is leading this? Are we bringing in different people? Are we bringing in the same people? Are they being retrained?" [[00:38:30]] Because, as you see, as we've adopted new technology, the new technology is fantastic but, oftentimes, the people configuring that are not configuring it correctly. And the hackers know that and they can get into the system.

On cyber-risk management. Cyber risk has to be incorporated throughout the organization or throughout the business in a holistic way. [[00:39:00]] It's not the responsibility of one person. If you are a leader, it's empowering every employee. Think back to that first email example I showed you where our CFO raised the flag and said, "Hey, this email doesn't look right." In our organization, our CFO can do that as well as our customer-service agents. Every single person, it doesn't matter what role they're in. [[00:39:30]] You are a vital link, your employees are a vital link, everyone, in your organization, has to be trained, you have to make an investment in them. Cyber exposure should be shared in a quantifiable dollar amount. Think about your budgets, for those of you [[inaudible 00:39:48]] budget authority, think about your budgets. Do you have a budget line item talking about cyber-risk exposure? And if not, I encourage you to think about it. [[00:40:00]] And it's not just rolled up or buried somewhere, it should be a top-of-the-line item in a cyber-response plan. The paradigm on cyber is changing and involves everybody in leadership.

For the last part of the discussion here, for the next 15 minutes or so, I want to talk about a cyber breach. So you've experienced a cyber breach, now what? What are you going to do? [[00:40:30]] Isolate and stop the bleed, from a medical perspective. You have to identify that there was a breach. Rapid internal reporting. Do you have a [[inaudible 00:40:44]] someone, in your organization, could raise their hand and say, "I think I just clicked on a malicious email. I think I just sent a secure file to an inappropriate person. I think I [[00:41:00]] just..." and fill in the blank. If you don't have that [[inaudible 00:41:06]], you will miss critical critical time in the early elements of a breach. You have to build it into your staff that it's okay for them to raise their hand and say, "I think I messed up." Those hours, days, minutes are so vital to the recovery.

Number two, isolate the attack. It may mean that you take all services [[00:41:30]] offline. It may mean that you pull the plug on everything. And that's painful. You know, as states, as regulators, as international bodies, I mean imagine the impact of shutting down a health-record system. Wow. Imagine the impact of shutting down a licensure process. But you have to have the right people that can make those decisions to isolate the attack. Hopefully, you can keep the period short [[00:42:00]] and, sometimes, you might be able to isolate one chunk and not everything. But you have to have the right people that can make the decisions quick.

Number three, protect your data. Absolutely go in. Stop the bleed, protect the data. The moment that we realized that we were a victim of a large cyberattack, most likely from a nation state, you know, we shut down the server, we went black, turned it off, cut all [[00:42:30]] access. Then we went in, reverse engineered how they were attacking, and then put in very specific code to stop those attacks, and then we shared that with our other platforms. Protect your data. And the number three, very important, capture forensic details. Without getting too technical, but if you're in the leadership role, make sure that you're asking these questions to your IT staff, "Hey, do you have a forensic copy [[00:43:00]] of our system and it's a complete forensic copy of everything at that moment in time?" Every log file, if you're taking notes, every log file, every access file, the database. Everything, you need a forensic copy sewed up. That's going to be vital in the prosecution phase and in determining what happened. Most of us have databases that are very live-living organisms, so people are constantly adding, [[00:43:30]] writing, changing records, so you want a copy of that in time.

Client privilege. I noted, when the earlier speaker asked, "How many lawyers were in the room," I'm not going to ask you to raise your hand on that again but I appreciate you in a very real way. We implemented a new approach that leveraged cyber privilege in our response plan. And we have entered [[00:44:00]] into a cyber agreement with a firm that allows us to use them the moment that we sense an attack. And what we do is we cover everything in the attorney-client privilege, related to that attack, and we encapsulate it as much as we can. Even to the point of if we have to work with an HR firm, or a public-relations firm, I'm sorry, [[00:44:30]] a public-relations firm, we have that firm contracted through the attorney. So it's all under attorney-client privilege. Because, in the early days of an attack, you're in, what would be called, the fog of war. You don't know everything that's happened, you don't have all the details. You don't know if this is something that's going to impact one state, or one territory, or is going to impact the whole nation. So start, from day one, thinking about how you're going to encapsulate and protect [[00:45:00]] the information about how you're responding to the attack.

This is a quote, you can see, "The overriding principle of using privilege," and this is attorney-client privilege, "is straightforward, protect your organization's investigation and breach-response efforts from usage by third parties or other regulatory agencies in litigation." Wrap it up under attorney-client privilege if possible. There is a difference between a cyber attack and a cyber [[00:45:30]] breach. I showed you two examples earlier. So a cyber attack is where the globe led up and everyone was attacking and [[inaudible 00:45:40]]. A breach, for example, is where the individual was, you know, individual credentials were used to access records. There was nothing wrong with the system, the system worked as designed, someone got in.

Investigate and prepare for the next steps. [[00:46:00]] Three key components for regulators. Number one is on the cyber side. What's the technology that you need to do to stop the attack and then what forensic evidence you need? Every single case study, I shared with you today, we worked very close in cooperation with the FBI and others to investigate, they're going to want to know the forensic information. Number two, know your regulatory landscape. [[00:46:30]] If you're an organization like us, we work in all states and territories and in countries around the world, every state, in the United States, is different, every country and territory is different that we work in. Know where you're at. And it's not based on where your headquarters is, it's based where the individual lives, where they declare residency of the information that you are protecting.

Mandatory reporting, timelines. We have seen [[00:47:00]] timelines go from undefined and long, in some cases, down to 72 hours. Think about how rapid you got to respond to get a report, regulatory report, issued [[inaudible 00:47:14]] Attorney General's Office in a 72-hour timeline. Contractual obligations. Most modern contracts include a cyber clause. Understand who you have to report, when, how, and what's the process [[00:47:30]] for that. And then the public. Every cyberattack has an impact on your brand, your organization trust. What happens if it hits the news? Are you going to be responsive? Are you going to be defensive? Are you going to be on the offense? How are you going to tell your story? Anticipate the liability. AAnticipate the liability and your response investigation. What's the impact on public trust restitution? I [[00:48:00]] mentioned before, we opened up a call center, we provided credit monitoring. Do you have that budgeted? Where is that going to come from? Do you have a cyber insurance plan? How are you going to mitigate that?

The average cost of a cyber breach for an enterprise, or corporation, and I would say, by definition, everyone in this room would fall into the first category is around 1.3 million dollars. For a very [[00:48:30]] small business or a very small organization it's still over $100,000. At the bottom, you see, on the preventive [[inaudible 00:48:39]] side of it, the cybersecurity budget. US government, on average, spends $959 per governmental employee on cybersecurity. Utility companies are, number one, number two, in the threat matrix, are about $1,344 per employee per year. How much is your organization [[00:49:00]] investing in cyber security, cyber-security infrastructure, hardware, training, personnel training? Where are you at on the spectrum?

The process, as I mentioned before, is holistic. As executive leaders, we have to make sure that we're looking at the whole organization and cyber is no longer a side component of it. We have to look at the human factors, watch our business continuity plan. If we have to shut down part of our digital infrastructure, how do we continue operating? [[00:49:30]] Can we continue operating? As our role as leaders, we have to be looking at that. That's the overview I have, I might have a couple minutes for questions for this. If not, we'll move to the next speaker. I know we have a panel discussion later. But any questions from the audience.

- [[Man 1]] Donnie, you've provided us with a lot of information. [[00:50:00]] And the one thought that started to go through my mind, particularly in those states where there is a degree of centralization of services, the accountabilities for the Board of Nursing versus the central authority makes us even more complex. I'm just wondering if you've got any thoughts or advice or not in terms of how the board holds a centralized service [[00:50:30]] accountable for their valuable data?

- [[Donnie]] Right. That is an extremely important and complicated question. So we approach it on a couple different mechanisms. One is, sure, we do have contractual data signing, data-use agreements, that lay out responsibilities. However, you know, if you take an example, even similar to what I mentioned, [[00:51:00]] you know, are we going to go financially after a state? How does that work? There's challenge is in that precedent, how do you do that? Is the state going to go after for restitution for the individual? You know, in one of the examples I presented, I can't go too much into it because it's still active, but that's one of the things that the insurance company is looking at. So our cyber carrier, although we are not going [[00:51:30]] after the state for financial restitution, the insurance company is in a process to try to figure that out.

I think another key thing though is partnership. And so, this changes...we operate on partnership, the boards, and the states, and the institutions operate on a theory of trust and partnership, that's the same as we operate. And we need to add this new piece into it and it's that [[00:52:00]] new piece of cybersecurity trust and, where possible, I think defining that out in advance of a breach. And these are elements that are new to us in our contractual and partnership negotiations but it's something that we are walking down the road on by saying, "How do we write this out into our agreement so, if a breach happens, we know who to talk to, who's going to face accountabilities, and what does it do to the relationship." It's new areas for us too. Yep. [[00:52:30]]

I will note that one of the things that I am excited about, especially even with NCSBN and other regulators, is we're beginning to have dialogues like this. And, you know, I know that we're having dialogues with NCSBN and another medical regulatory agencies not only to be able to talk about best practices in cybersecurity but talk about our response. And that's why I know that [[inaudible 00:52:59]] [[00:53:00]] doing a great job leading and I really appreciate working with him on that, and others. Any other questions? Thank you so much for the opportunity, I'll be around the rest of the day.