Webinar Transcript: Anatomy of a Breach - Lessons from Real-World Attacks

Video Details

Video URL: Anatomy of a Breach - Lessons from Real-World Attacks (YouTube)

Date Published: May 7, 2025

Presenters in this Video

- Rob Rudloff (RubinBrown)
- David Hendrickson (RubinBrown)

Video Transcript

Sharon Trilk
Good morning and thank you for joining us for our Webinar Wednesday. My name is Sharon, and I'm with SIPA, your Colorado government authority, helping you get more information and services online and offering Colorado governments grant funding. In today's webinar, our guests David Hendrickson and Rob Rudloff with RubinBrown will be sharing more about how cyber attacks occur and how to guard against them. Before we get started, please go ahead and turn on captioning, if you need or desire, and note that during this webinar you are muted. If you have any questions or would like to communicate with the presenters at any point during the webinar, please use the chat or the Q and A function. We will unmute folks at the end after they've raised their hands for any remaining questions. We'll also have some poll questions for you to answer during the presentation and a post-webinar survey, and we hope you'll provide your feedback. Please join me in welcoming Rob and David. Thank you both for your time and for this incredibly timely presentation, as cyber attacks are always on our mind. Also on the call is SIPA sales and marketing director Beth Justice and customer success director Duane Tucker, if you have any questions for us, thank you all again for joining us today, and with that, I will turn it over to our guests.

Rob Rudloff
Great. Thank you, Sharon. Sharon mentioned, I'm Rob Rudloff. I'm from the cyber security practice for RubinBrown, been doing this type of work for over 25 years, so little bit of experience there. And with me today, I've got our lead penetration tester, David Hendrickson, who has been doing pen testing for over 20 years. So as we go through the presentations today, please feel free to ask questions, either

through the chat or save them up until the end. It's really a lot more fun when this is a little interactive. So please feel free to ask questions, and we'll do our best to answer them as we go through.

Rob Rudloff
So today we are going to we're going to just go through some common attacks, recent examples, common factors. What is it these attackers want? And then some ideas on how to protect yourself and your organization. Again, feel free to answer ask questions anytime, or save them for the end. Like I said, we've got a wealth of experience. David's got tons of war stories about everything from physical security and social engineering attacks to technical attacks that you can talk through. So feel free to ask questions.

Rob Rudloff
One of the things we'd like to do is just, you know, why, part of the reason why these things are the type of complaints coming in from this is from IC3, the FBI's internet crime report. And you can just see there's all kinds of complaints that come in. And just realize that these are the complaints. And so there's a lot of these that do not get reported to the FBI for whatever reason. But these are the type of attacks the FBI is responding to and taking in. And you can see everything on there, from, you know, extortion to all kinds of ransomware, fraud attacks, the SIM swaps, which are the, you know, they take over your phone, these type of things. So it's just a reminder that this is prevalent.

Rob Rudloff
There's a lot of attacks going on in the world, so common attacks that we see, the big one everybody's afraid of, of course, is ransomware, because of the business disruption. But there's also business email compromise, things like the email accounts being taken over, wire fraud, which is where they're stealing money, IP and sensitive data breaches. So whether it's personally identifiable information or healthcare information, credit card information or just intellectual property, we still continue to see a lot of fraud against employees, so things like trying to log into your HR portal and changing your account information so your paycheck goes to the wrong place. And as we mentioned before, you know, extortion, and then any combination of the above. A lot of bad guys specialize in one type of attack or another, but occasionally you get a combo attack where they're doing multiple things at once. Just going to ask you, David, what type of attacks do you see, or where are you familiar with both from the pen testing and then just what you've seen in the field?

David Hendrickson
I think one of the big things that, if we look back at the slide before this that showed the different complaints, the number one on there is phishing. It's an easy thing to do. You know, that's probably the biggest thing that most people will be hit with. Sure the bad guys are constantly poking and prodding that external networks all day long and every day. But the phishing is so easy in this day and age, there are plenty of free tools available that even organizations can use themselves to educate users on phishing. But again, these tools are free. There's so many different types of them out there that I think phishing will always be that item that sticks out because it can be done from anywhere. You know, I can buy email addresses left and right. I can get them and send as many emails as I want without worrying about anybody catching me, in a sense. You know, I'm not there physically. You know, robbing banks

and that kind of thing is just not as prevalent as some of this, because it's a lot easier to do. But once we start looking--

Rob Rudloff
Um

David Hendrickson
Go ahead.

David Hendrickson
So once we look past something like phishing, which is so common and you're seeing them daily, a big area that is being hit is a lot of the web application and API attacks. You know, again, those are the type of attacks that there's a lot of complexity when you create a website, especially anything that has a login that allows you to enter in data, to select things, buy things. There's a lot of complexity when it comes to programming those items that it is missed sometimes to put in all of the security around that. So we do still see a lot of what I'll call authorization attacks. You know, from our standpoint, when we're doing a web application, we may be provided a username and password by the client, and we log in with that, and then we look for areas where, when I submit a command or try to gain access to something, it'll show what user is trying to do that, and from there, I can manipulate that command and say I'm someone else, and if it works great now I got an authorization attack, and I have access to things I shouldn't, and this will be the same kind of thing that a bad guy will do, especially on websites that have an auto registration where you can do it yourself. It's not required for an organization to set up that account. You can do it yourself. You know, that gives the bad guys the access in, and now they can start looking for these type of attacks that could provide additional information about other companies, other people, and get that information from them.

David Hendrickson
And then, of course, there will always be misconfigurations, whether that's missing patches on services. Let's face it, from an IT standpoint, you know, being on the IT side, it's easy to look at, is there enough people to do the work? So a lot of times it's, I have to implement something new into an environment. Well, I got to make it work. You know, we paid all this money, so the IT staff just has to make it work, get it out there. We'll come back and add in the security afterwards. Thankfully, a lot of that is changing, but it's still happening, and we will find those errors, whether it's default pages that shouldn't be around, default credentials, weak credentials, you know, those kind of things that we still see out there.

Rob Rudloff
Great. That's a great segue into our next, you know, the next side of those common factors, and you already talked about most of them, things like the controls breakdown, just human error. There have been some pretty notable ones in Colorado, where the attack was made possible by a human error, just a system administrator or somebody made a mistake. Those process issues are more systemic breakdowns where, you know, just didn't have a good change control process. You mentioned that David with his configurations, or somebody just didn't get permission to do something and didn't realize what they were doing. And then technology configurations and, of course, governance, which is, you've

got to have the policies and procedures to give you the authority and authorization to enforce these things.

David Hendrickson
And Rob real quick, you know, I want to touch, you know, we kind of talked about configuration in the tech in this case, you know, the technology configuration. A lot of what we see also, that I didn't mention is there's been a lot of use of like GitHub to put code out there, to allow version control and to be able to share, you know, the different parts of the program or the code. What we're also seeing there is it's not locked down efficiently, and we will find files out there that may contain a username and password because it's hard coded in. So it's that type of, you know, in that case, it's controls, break down, human error. Take that. It's a combination of all of it. So. Uh, that can lead to some serious issues, because we'll find it a lot with databases. You know, you have that application that takes in the data and then writes it to the database in the back end, some of that's hard coded with the username, password, and we can find those configuration files.

Rob Rudloff
You mentioned, GitHub, David. What are you seeing or hearing as far as, what about the how hard is it to what am I trying to ask? How often do you think there is malware or other things in the GitHub software? So instead of accidentally putting, say, username and password, a user did that on purpose, but then loaded to GitHub and just didn't realize it was in there. So it was in there. But the flip side is, because you mentioned free phishing software, like, how do we know that phishing software isn't doing something else?

David Hendrickson
And that'll always be an issue. You know, good thing is there are other controls that help with that, to look for anything malicious, and, you know, scanning, whether it's antivirus, anti-malware, those kind of things, that can pick up that kind of threat. But, yeah, it's definitely always going to be some type of issue with free software out there, if we go deeper into more my world where, you know, there might be an exploit that's available out on the internet, download the code so you can run it, you still have to look through it, because what is it really doing? If it's just posted out there, who posted it? You know, you don't always know who that person is.

Rob Rudloff
Good point. And then at the bottom of that list, I put it in italics, highly sophisticated, attackers, because it just makes me laugh. Most of the time when we see a big high profile breach, you know that the official public service, public announcement is that, you know, they were attacked by a highly sophisticated attackers that did this amazing thing, when, in actuality, somebody just got an email and they clicked on a link, or, you know, in one notable case last year, they called up the help desk and convinced them to change their password, and they weren't really the person who was calling in. So I like to say that the highly sophisticated attacks are very clever. Sometimes they're very basic, because we had a control breakdown somewhere.

Rob Rudloff
So that brings you, you know, the kind of question then is, who's doing this, like, who's doing this? And

we'll get to why in a second. But who's attacking? And so some of the attackers are actually researchers, just trying to investigate. All right? They're looking into things. They're trying to find the zero-days before the bad guys exploit them. You've got hobby hackers out there. Back in the early days of the Internet, that was a fun thing to do is just kind of go around and check things out. It's against federal law now, so probably not a good idea to do that, unless you have permission. You have hacktivists, which are like Anonymous, who take up causes and go after things. There's corporate espionage, although every corporation will deny any of that's going on. But there's always going to be some, you know, competitive analysis going on. Organized crime is really the big one driving most of the major attacks now and then, of course, nation states, with North Korea, you know, Iran, and some of the, you know, China, and some of the other players, being the typical ones that come up. Russia and a lot of China are actually organized around organized crime related to the nation states. They're a little different game there.

Rob Rudloff
But then that, you know, you some of these are doing things for innocent reasons. Some are doing it for, you know, a cause. But the big thing, what they're after most of the time, right, is they want they want money. I'm sure everybody has heard or seen that when you get a ransomware attack, they typically want you to pay in Bitcoin, and that's because it's highly fungible, but hard to track. So one thing to note, just in general with Bitcoin, I always like to remind folks that Bitcoin is anonymous, but it is not private, right? It is a public blockchain, and so every time a payment is made to ransomware and it's reported the FBI. The FBI watches those wallets and tracks the money. And then occasionally -- there's a pretty good Netflix special on it -- occasionally, the FBI will pop one of the bad guys because they make a mistake and, you know, buy a pizza or a Lamborghini or something, and they're able to trace the money through from the original Bitcoin wallets down to the where they took them out and actually used them to convert to cash.

David Hendrickson
I think another part on that, Rob, is, you know, we think about these especially, we look at the organized crime part of it, you know, they're doing their part to get you the pay the ransom, to get the bitcoins from you. And it's not just it's any of these hackers that are compromising and getting this data. They may get something from you up front, but they're also selling it on the back end in, you know, the dark web and those type of areas. So they're making money off of you and making money off of your data, because they're still selling it and it's out there. A lot of these attacks, if we go back to, you know, the hobby, or, you know, not always sophisticated, it can be as easy as buying a compromise or an attack off the dark web and not just finding it yourself. So, you know, a lot of it ends up being services provided by these bad guys at the same time with getting money from you.

Rob Rudloff
Just again, give some figures that just shows you some idea of the dollar amounts involved to business email compromise at 2.7 billion. I always like to joke, sometimes that makes me question my career choices, because that's all that's a lot of money. But you can see there's just a lot of money in this game, and that's why they do it. And the other thing to note, I've already said it, but I'll just mention it again, this is just what's been reported. So this isn't, doesn't include everything not reported, where people just didn't, didn't want to, or were embarrassed, or whatever. You can see ransomware over

there at 12 million, it's been shrinking a little bit as the as the other attacks become more, you know, profitable. So that doesn't seem to compromise in the phishing and spoofing are kind of the big ones. You can see there's a ton of different types of attacks, and these are all things that the bad guys will pick on you if you're an easy target. So if you're in certain groups, other certain types of crimes are more prevalent. So the confidence romance scams, right? They're always going after, ideally, single people, usually single older people. If you're a man, you're almost guaranteed that the picture they show you is going to be a young Asian female. If you're a woman, it's almost always going to be a young Latin man. And that's just, that's just the common path that works for some reason. And of course, there's variations on that by country and by target market and all that.

David Hendrickson
And if we stay on this for just a moment, Rob, if we start looking at some of these actual types and what they are, they're really focused on manipulating and abusing people. And in our environment, from our day to day jobs, there's always a "go, go, go" type of philosophy that, you know, especially business, email compromise is probably one of the biggest ones. The email that comes in, I'm the boss, you need to wire the money. Do it now. Do it now. Otherwise we're going bankrupt. And instead of taking the time to validate, a lot of people are, as you can see, are still falling for that. I'm fearful of losing my job or I don't have time to think, because they need it now, so they just do it, which is very unfortunate. But it is the way these people are, is exploiting human beings and behavior. You know we're using fear, uncertainty, doubt, you know everybody's favorite and the lack of time. You know that we're so used to going fast and getting it done that we don't always think and it leads to a lot of these business email compromises. For anybody in their organizations that do any kind of annual, or however often, simulated phishing attacks. How many people end up clicking on it because, oh, I just didn't have time. I didn't read it through. I just clicked on it because it's something that was there that I was dealing with. So it happens a lot, and these numbers show how bad it can be. And like Rob said, it's big business.

Rob Rudloff
Yeah, I just got the text this morning that said the recruiters had been referred. They got referred to me because they saw several online recruiters mention my name and how good I was and that they want to pay me $1,000 a week for five hours of work, and I assume the next, the next thing would be, you have to put a deposit down and do some other stuff.

David Hendrickson
Right?

Rob Rudloff
I was entertained that I got that one this morning when we were getting ready to do this presentation. And then, you know, like my father in law was a little older, has had the tech support one at least twice now, he's smart to hang up on him. Yeah, the first time he got to the point where he almost gave them access, and then he said, wait a minute. He called me and said, Is this legit? And I said, no, Bob, turn off your computer. I'll be over in a minute. So there's a lot. But like you said, David, this is really going after people, and that fear, uncertainty and doubt, sense of we have to do something or something or something bad is going to happen. All those things. And with the AI, some of the what they the extortion, or what they call virtual kidnapping, we think it's probably going to see an increase. And that's

where, you know, they take a audio, get an audio sample of, say, your kid or your grandkid, they sample it, and then they have the bad guys use AI to play it in the voice of your loved one.

David Hendrickson
And so let's face it, in this day and age, granted, I'm a lot older, so I'm not on all these Tiktok and everything else that has your voice out there. It's going to be easy to find that and get the information to start manipulating,

Rob Rudloff
Yeah, yeah. It's, it's a whole new, whole new world, once we get to the AI and how that, how that does, and we'll talk about that in just a second, maybe as we get into the type of attacks.

Rob Rudloff
So one of the things we want to do is just walk through kind of how, how to think about the attacks and how they're going to look. And so everybody has, kind of your main network that you use in those boxes on there, just kind of your user environment, your main data center, and maybe your primary domain, we call it, where you normally work every day but you've also got, you know, email. So a lot of us are using Office 365 or Google. There's other emails out there, but most of us have moved to the cloud for email, and then we have remote users, which may be on the decline, but a lot of us are still going remote and working remote these days. Then you've also got other networks. So you might have a credit card environment, the PCI, DSS, you might have a private network or isolated network, like if you have SCADA systems or operational technology type things attached to your network, or just other private areas with that Then you might have this external support. So service providers are logging in to provide support, or you've got a managed service provider that does continuous support.

Rob Rudloff
So we, when we talk about this, we start to talk about attack surface and where things can where bad guys can get in and what they can do. And so, you know, we've talked about some of these, but these are all different kinds of attacks that could really come in. And so to kind of go around left to right, the card theft attacks, those could be physical or logical. They could either break in through your network and get to things, like in the case of Target long ago, or it could be their physical-- they're physically modifying devices. Those network attacks, criminal attacks, the network and application ones David talked about before, we'll touch on those again. And then the email phishing social engineering attacks. Those are off to the right. That's where they're attacking those remote users, because we're at home and we're distracted, or maybe not paying quite as much attention as we should. But you're also getting those phishing emails coming in. And then supply chain attacks, which are on the rise. There's a lot more attacks where somebody in your supply chain was compromised. Again, you could point back to that long ago target attack where the HVAC vendor was actually breached, and then they used their access into Target to breach Target. But that means you've got to do some supply chain testing and things like that. Dave, you kind of already talked about this, but when you're especially when you're doing your testing, what, what are common things you're seeing from both, you know, external and internal? And I know, I think you and I have joked that, you know, 10 or 15 years ago, when we were doing external pen testing. We've we won a lot. I mean, we would get in pretty frequently, not every

time, but nowadays it's a lot less. How about just talk through that a little bit on internal versus external, and what you kind of see in the environment?

David Hendrickson
Yeah, exactly. You know, with the always increasing technology, we got new security devices coming out left and right. All of them are helping reduce that footprint. From an external standpoint, and being able to protect our external systems, that it is a lot harder. You know, and if we look at an external test, we have limited on what we can see. It's really only what you allow to be seen from the internet. So that really reduces what we can attack and what our capabilities are. Generally, when we look at an internal pen test, there's a lot more visible. We generally aren't going through a firewall to see all of the network. And you know, you can think about an internal pen test from the standpoint of someone had clicked on a link from your organization and then their computer got compromised. Well, now the bad guys in your network looking at things, and they're going to see a lot more we're going to see a lot more open ports that can be abused, more services available that can be abused. And this is where we start seeing a lot of the internal traffic of some of the insecure protocols that allow us to do more than what we could do from an outside standpoint, because we don't see that traffic. But inside, we do see a lot of it. To this day and age, you know, we are still successful with, for those of you that know LLMNR on an internal network, it's a Microsoft specific protocol that they have on by default. We're still seeing it in a lot of networks, and it is very insecure. Unfortunately, when they made it, they made it to be easy for IT staff to set up and allow people to get access to resources. What it allowed the bad guys to do is make it easier for them to get access to those same resources. And again, we're still seeing it to this day. It's there by default.

Rob Rudloff
On that attack, that's the one where you don't actually have access to the in the clear password, right? That's, you're just manipulating-- we don't want to get too wonky, but there's, there's traffic going back and forth, and you're basically intercepting it?

Rob Rudloff
And then, at least, when you showed me the demo, you showed me like you didn't have access to the actual password. You just the encrypted password, but you were able to log in as if you had the password,

David Hendrickson
Uh huh.

David Hendrickson
Right. So a couple things are going to come out of this. So with that attack -- it's a man in the middle -- so I'm capturing the credential, because this is the biggest fault with that Microsoft protocol. When it's looking for a resource, it sends out a username and an encrypted password. No matter what, it is there if it finds the resource. So you pretend to be the resource, and then you just relay it on to the end devices. And you can do all sorts of things. You can get control that remote computer. You could pull hashes off of that for local accounts or other accounts that have logged in. So there's a wide variety.

But again, it's it's something that's there by default on Windows, easy to fix, but it is there by default and generally not used regularly by most organizations.

David Hendrickson
And that kind of leads into the idea of from an internal standpoint, in this day and age of internet of things, you know, the IoT devices, any of these devices that can be plugged in, bought purchase, plugged into a network. We don't as an IT -- organizations don't always know all that is involved with that device. Even if we think about our printers, that we plug into a network, a lot of them, by default, have certain services enabled automatically, and if you don't know to look for those kind of things, it is there, and it's a default setting, which could lead to a compromise. And that's another thing that we see, is that knowledge of we put a device out in our network, but we know what it does, but we didn't know all the underlying processes that are available with it. And that's where, if you have you know, those regular vulnerability scans or something like that, you'll start seeing those type of services on new devices. Or even if you before you put it out on the network, you can scan it and see that those devices have those services. I don't need them. I need to shut them down.

David Hendrickson
And then, of course, you know, there's missing patches. If we think back to the nation state, you know, this has been a few years, 2017 but we're still seeing it, the MS17-010 exploit. If we think about a nation state, that was developed by the United States, the NSA, who had found the vulnerability and hadn't told anybody. The only reason it came out there was a breach at the NSA. You know. The documents were leaked. And now everybody knew that this existed, but we still see it. You know, those are the kind of things that, unfortunately, we do see. And some of that comes up from, all right, I have a particular application I have on a particular workstation or server. Well, it's old. They no longer support it, but I need that application so I can't upgrade or add new patches to systems. And we see plenty of that out there.

Rob Rudloff
And you talked about the internal pen test or internal attacks. I wonder if you'd just spend a second and go through a little bit on, you know, what's the scenario? Like how would an internal attack occur? And, you know, authenticated and unauthenticated? Maybe just talk through those scenarios like, I mean, do you have to have username and password to log in before you start the attack sequence? Or like that.

David Hendrickson
Yeah. And generally, with an internal pen test, we generally don't have credentials. That's what we're looking for. We're looking for credentials. Domain administrators if you're on a Windows domain, that'd be great, because now I have access to a lot more. But we're looking for that type of information, because then we can utilize it to move into other attacks on other systems. Just because I can, let's say, breach a workstation, that may not be my end goal. That might give me more data, because there's a possibility a domain admin logged on to that computer. Now I can get that credential information, impersonate, and move on to the next one. So I'm hopping them, pivoting to other systems. And that becomes very important. If we look at your chart here, where you have the credit card environment or a private network, it may be segmented off, but if anything is available through, whether it's secured by a firewall or anything like that, if I can get into any type of system, even if that

system contains no data, but I can breach it, now I'm on that network, whether it's the private network or the credit card, and now I'm going to start pivoting. Plenty of tools. Again, all of these are free tools, or most of them are free, that allow me to set up those pivots, and now I can act as if I'm sitting on that network doing all my same tests that had been doing on a less secure side of an internal pen test.

Rob Rudloff
That brings us, I mean, what's one of the things the bad guys are looking for us? We call it lateral movement, or cross network. And to David's point you just made, the bad guys are going to do this. They if they get in through any piece of the network, they're going to try to, as you mentioned, pivot is that they're going to try to cross over to the other parts of the network, because they want the juiciest piece of network to go after if they're going to launch ransomware, or they want the juiciest data they're going to commit fraud or just steal data. You know, we're primarily public sector, I assume when we call or all public sector, because SIPA clients, and then they're also after just damaging your environment or causing mayhem and disruption to local governments.

Rob Rudloff
Almost every 9/11 we get an alert from CISA and from the ISACs saying that there's an increased activity of attacks against US government, entity, state, local and federal, just because they want to cause disruption. So but this lateral movement is really what, that's how again, the Target attack, the Home Depot attack, any of the PCI attacks you've heard of, credit card attacks, even the MGM attack last year, and then some of the public sector ones we had just here in Colorado. This is the same sequence they use. Get in, you know, get your, get your toe hold, and then start to move throughout the network until you got just the right setup, and then you launch your attacks.

David Hendrickson
If you stay on this real quick Rob, you know, that's one of the other things that if we think back to some of those earlier slides where we saw the dollar amounts of the different types of attacks, we saw the number of complaints for some of the different attacks. We just talked about, these, I'll say fairly complex attacks where I'm trying to get into an internal network, move around in that internal network so there may be some type of logging or capabilities of an organization to pick that up and potentially stop it. So it's a lot of work on the bad guys end. Where, if you look at email, the phishing side of things, I just launch an attack, sit back and, you know, enjoy my margarita on the beach because I'm making all this money off of you. It's a lot easier. So you look at, you know, that risk benefit of what do the bad guys want to spend their time doing? You know that internal chart that you have there, if it's corporate espionage, you're darn right, that's where you're going to see a lot of that moving around. If they're looking for specific data, that's where it's going to happen. If it's just to make money, you're going to see it on that phishing, social engineering type of attack, because it is easy. I can send out a million emails, even if I get 10% to click on it, great. I'm happy I just made a lot of money.

Rob Rudloff
Yeah, and a lot of times we've said, especially government entities, not as worried about some of the business email compromise, because, you know, if the elected official or the, you know, the county manager calls and says, hey, wire this money right now, it's urgent. You know, there's bureaucracy. You got to go through administrative requirements. That doesn't happen like it can on the commercial

world, but where we have seen it a lot is in faked invoices, and then also in changing banking information. So one of the things that governments tend to do is build expensive things, like buildings, parks, you know, and oftentimes the contract will put, you know, on the fence, they'll put up, hey, Bob's construction is working on this project. Well, now I know Bob's construction is doing that project. I know he's doing it for the local entity, because I know what the building is. And now I call up the accounts payable and say, Hey, this is Bob from Bob's construction. Can you change my banking information? And the next payment to go out goes to the wrong place. So you have to be vigilant. There are attack methods the bad guys have figured out how to use on every type of entity that exists, and so you just have to be vigilant for those things and have some controls in place. So I thought we'd take you through--

David Hendrickson
Yeah, one last one on that, because, you know, I'm trying not to ramble too much on it, because you and I have been a part of this. You know, the other part that we've seen in in previous jobs was the idea that someone did click on the phishing. They did provide their username and password for the organization they're at, well, now, if I have that, I can potentially log into some type of HR software and potentially start changing banking information for direct deposit. And you know, if there aren't the right controls in place, I change that bank. Payday comes, I get their money.

Rob Rudloff
Yep, and we again, you're right. I remember when that happened. David, I remember, yes, we had to have about with the with the university, reimburse people their paychecks, and it was an interesting time.

David Hendrickson
Yeah.

Rob Rudloff
So if we didn't mention it, David and I used to work the University of Denver. He was the security manager, and I was the, I was a CISO. So we got to watch some of this live. So one thing I thought we'd do, it's kind of interesting, this is, this is kind of a decision tree for the criminals. So it's a little, you know, simplified, but this is what happens when we go through those attacks. And it really fits right in, David, with what you just mentioned with the phishing emails, and how common that is. But it also describes how sometimes they get into the criminals are specialists. So you might have one criminal organization, all they're doing is the phishing and gathering up credentials, and then they sell that. Somebody grabs a credential and validates it, and then says, what is this? Right? Because if it's Rob's personal email, not exciting. There's a lot of spam in there, not much going on. But if it's the email to say, you know, a law firm or a big organization with a lot of money, you know, or a casino or a crypto exchange or whatever, suddenly it gets way more interesting, and they decide, they put a value on that set of credentials.

Rob Rudloff
And so then on that item number three, they really step back and say, okay, what do we got? Do we want to sell this? Or do we want to prepare our attack sequence and go through. And then on the attack

sequence, it could be that they're a fraudster, and they do, mainly, you know, fake invoices. And so the the access to something is to, like, a not for profit, or, you know, a government entity, and they're like, yeah, it's not really my game. So we'll just sell those credentials. Eventually, though, somebody picks up those, these credentials, and you have to imagine, say, like, a deck of cards, a hold of my deck of cards, right? And you're just picking the next card off the deck, and on that card is a set of credentials, and the attack vector. Like, log into this with these credentials, and then you do reconnaissance. And again, you say, what is it? What kind of target do I have? And they may revalue the access, and they're looking at the contents of email, if they can get in. And so again, they're either selling their credentials or they initiate their attack, right? And if they're initiating an attack, they're going after what's my highest yield. And so this is where the bad guys specialize. And not all of them do all types of attacks. Like mostly the ransomware folks just do ransomware. The fraudsters do mainly just fraud. Actually, some of them are not very creative, because only do one type of attack, and we've seen access where, you know, the bad guy had access for 30 days. They looked at 8,000 different emails, and they've only run one attack sequence, which is kind of lazy, if you think about it, but, you know, it helped the client that they didn't have more than that. But they're, they're identifying that highest yield attack, and then they do the attack. If it's fraud, obviously, if it's ransomware, that's a different story, but if it's fraud attack, you know, they execute the transfer, and then they sit back and say, did we get detected? If the alarm bells are going off and people are freaking out, you just put that card to the side, we got our money off this one. We move on to the next card, the next attack. But if they didn't notice, or they responded somehow favorably, even though you took advantage of them, then they'll do it again. We recently had a fraud attack using a fake invoices and wiring that had nine separate wires by the time it was over for over 1.4 million in loss, and it was just because the organization did not detect that these were fraudulent, until, like I said, that ninth one went through, and then, fortunately, between them and the bank on the 10th one, they stopped and said, wait a minute, let's pause and were able to track it down. We put up the polling questions. Go ahead and answer those. Just what type of attacks are is your organization worried about?

Rob Rudloff
Cool. So ransomware is still the biggest one, and then breach of sensitive data. Those are, those are very common. On the fake invoice and the social engineering, so many times we've heard people say, well, that would never happen here. Like, like I'm smart enough not to do that, but remember what David said, you get busy. I call it task mode. You're just knocking out your tasks. Something like that shows up and you think you knocked it out, but you've clicked on the wrong thing or given somebody information that's bad for the organization. So keep those things in mind. And then internal controls, especially on the fraud side. Nothing beats picking up the phone and calling a known phone number for somebody and saying, David, did you really mean to change your bank information just now? Because it seemed weird. But don't call the number on the email, right? Because that's the fraudsters. They'll change the emails, change the numbers, and then don't always believe caller ID, unfortunately, because some of our attacks, and I know, David, you've done this where you use a for lack of a better term, what was it a calling card that changes your source?

David Hendrickson
It's just a service, yeah.

Rob Rudloff
Yeah, and it's not expensive. It's like 10 cents or 15 cents a call or something. I've seen sales people use it, which is really devious on their part. But the bad guys are using all kinds of methods. So just food for thought on those. And then, you know, the impact of these type of attacks. Obviously, there's disruption, operational disruption. There could be reputational damage, which is hard to quantify, because unfortunately, also I think, we've gotten so used to breaches that it no longer really destroys the trust like it used to. You know, the first few times my identity information was leaked or exposed. You know, kind of made me worry. But, like the last, I don't know about you, David, but I probably at any given time, at least one and maybe two or three, you know, identity protection services, because somebody got breached and had to give me the free service again. It's way too common.

Rob Rudloff
And then on the cost side, just multiple layers of impact. Think through, like direct cost of support and response. Especially if you were a ransomwared, and you decide not to pay the ransom, which is what you know we recommend, the FBI recommends, but you're going to have increased insurance costs going forward, and then increased cost to replace and update solutions. The beautiful thing about a major breach, and it's happened a couple like the cities in Colorado, is that you get a whole new infrastructure from the ground up sometimes. The downside is that all that costs money. It has to all be updated and replaced, and it is a painful exercise to go through.

Rob Rudloff
So, I wanted to pivot just a little bit and talk about what we can do about these threats. And so the big three kind of areas you focus on are prevention, detection and response. So prevention is obviously stopping the attacks from ever happening, which is the best, best approach. But then we mentioned that that cross, you know, pivoting across the organization, going from network to network, and that's where we need detection systems out there to see if anything did go bump in the night. Or, you know, the system administrator goes home at 4:30 in the afternoon, and at 6pm they log in from China. And that seems weird, but if you don't have a detection system looking for that anomaly that can go unnoticed, and that actually happened to insurance provider that here in here in Colorado, back in 2015. And then, of course, we have to have a response. So what about the worst case scenario? Worst case scenario occurs. Somebody gets in they do something bad. What's our response? And can we do a systematic, controlled response? It's going to be super stressful, but it's even more stressful if everybody's running around with their hair on fire. So it's really good to do these practices. Most of the folks on this call have a COOP continuity of operations plan, and so the incident response and disaster recovery are really the IT, extension of your COOP and how to engage when something bad happens.

Rob Rudloff
So I thought we talked through just some of those, those attack vectors, and what we can do about it. So if we focus on that vendor and the supply chain, really what we need, what we want to do is, you know, whether it's a cloud solution or a managed service provider or HVAC, you really want to just do a quick vendor risk management approach. Assess the vendor, make sure they're good. If they're a SAAS product, a cloud product, you know you want to ask for their SOC two. You need to read the SOC 2 and make sure it protects the things you're interested in. But, that they have one gives you some comfort that they're doing something to protect your data. That's when I was a CISO, that's what I

wanted. I wanted comfort. In the CPA world, we call it assurance. But then on that external support part of that monitoring, you want that anomaly detection. So again, you know, our HVAC guys log in once a month to do diagnostics and test stuff, and then suddenly we noticed they've been logging in 15 times a day for three days in a row. It may be legit, but it's just something we need to know so we can go investigate.

Rob Rudloff
So when you focus on the users, it's really that security awareness, doing the phishing testing, doing penetration testing, really looking for incremental improvements, just really keeping the security kind of top of mind, so that the users you know are little vigilant. It's okay to be a little vigilant. I will tell you, you'll, you'll, you might get, you might get a giggle or a snicker, but nobody's ever going to complain if you call them up and say, I'm just calling to verify this, because it just the email looked funny, and that's okay, with vendors, with providers, with constituents, with everybody. So just those are kind of that focus on the user community.

Rob Rudloff
If we, if we go to that external protective controls, we used to jokingly refer to this as being hard and crunchy on the outside. And it's really that the basics are, what David mentioned is that change control, configuration, control and quality assurance to make sure it's done, and then doing some NIST refers to it as continuous monitoring, and that really just means doing a periodic test. If any of you have PCI, you know you have to be scanned once per quarter. It's like that, but doing it across your network, just to see, did something show up that's not supposed to be there? Is something misconfigured and needs to be fixed? And then doing those, those two testings, like David mentioned, the external pen testing and then the web application security testing, especially if it's a homegrown web application, or you've highly customized a commercial one, just things to consider.

Sharon Trilk
And we've got the poll question up. Last one. How effective are your organization's preventative detective and recovery controls protecting your environment? Very good, good, pretty good, probably needs work, or not, sure.

Rob Rudloff
And if you don't know, not sure is okay.

Rob Rudloff
These are the type of things we just think through. Most people, I mean, I'd say, David, unless you have a different opinion. Most people are pretty good with the external attacks now, because we just get attacks. If you're connected to the internet, you're constantly under attack.

Rob Rudloff
Good. So we got some very good ones. Nice.

Rob Rudloff
The corollary to these hard and crunchy on the outside is the soft and chewy on the inside, which is

what we see a lot. And this is, so internal prevention detection, again, this is where we're trying to to get that lateral movement, try to prevent it. Ideally never happens. But if it does happen, can we detect it? Do we have systems that let us know what's going on or that we're susceptible to it? And so that that list off to the side, is a combination of things you're going to want to do to harden the environment and to make it harder to to go across the networks, and then also the detection that goes with it. And then you see in that incident response, disaster recovering, that's where we get into that response effort. So something bad does happen, we detect it now we have a systematic way to go through and fix it.

Rob Rudloff
Cool and then I thought we'd we'll get to questions here in a second, or we'll open up for questions here in a second. This is this type of work that RubinBrown does. I saw somebody asked about the slide deck. Yeah, we'll have the slide deck available shortly after the presentation. So RubinBrown does the cyber compliance and frameworks. This is, you know, kind of any, any, any cyber security framework you've ever heard of, all the acronyms, NIST, ISO, HIPA, PCI, DSS for credit cards, CMMC for DOD requirements, tons more anything to do with that. We have a team that does compliance and readiness assessments. We are a qualified security assessor and can do formal assessments for PCI credit. But everything else, we're consultants and advisors.

Rob Rudloff
The technical assessments, and David leads this team doing the technical testing, so penetration testing, the web application security work, vulnerability scans, anything where we're directly interacting with technology, and sometimes people when we're doing social engineering. And so that team, we do all that in house, as a team, I'd like to joke that RubinBrown. at RubinBrown, we have a dedicated team of technical security specialists. We work for the CPAs, but we're not CPAs, so and if any of you wondered that RubinBrown was a law firm, no, it's a CPA and business consulting firm with a dedicated team of technical security specialists.

Rob Rudloff
The third thing we do, and hopefully no one will need this, but we do a lot of this in the collaboration with our litigation support our forensic accountants, is digital investigations, and that's, you know, business email compromise. We've had between one and three of those investigations ongoing for over a year, and so it's pretty constant drum beat of those attacks going on. We also do evidence preservation. That's things that the gentleman who leads that team is a former law enforcement in the St Louis area. Spent his last five years in law enforcement attached to an FBI and Secret Service digital forensic team, and then we, we, we grabbed him and brought him over to the commercial side to help us out.

Rob Rudloff
The fourth primary service area we have is virtual CISO, and this is kind of ongoing advisory support. We come up with an annual plan, and we don't have a-- we have a structure to this, but it's really what we do is wrap around our client. Whatever the client needs for security, we fill in those gaps. And so it's not a highly structured service until we get going, and then it becomes a we set up annual, quarterly, monthly, and if needed, weekly cadence of activity to support the client and their compliance and security requirements on an ongoing basis.

Rob Rudloff
Two of the kind of services I wanted to highlight, the cybersecurity, health check, we call it a packaged service. It's actually a methodology we use for a lot of our services. But the package service is in that $10,000-15,000 area. It's a starter package. Senior people do the work, and then we, we basically, you know, point out, identify where the gaps are, where the high risks are, and then help prioritize for the organization. And the kind of final step in those projects is always for us to step back and say, if I was your CISO, what would I do first? And that's how we prioritize.

Rob Rudloff
And then just as a, you know, we do KnowBe4 security awareness. So one product we actually resell, and it's a pass through for the organizations we really don't make any money on that, that's really a convenience to you all, to the to our clients, so that it's easy to get and they can get it fair price. And these are all services that can be contracted through SIPA and have been contracted through SIPA. So keep those in mind, just a couple of takeaways to remind you just take the time to understand your environment or make sure your IT folks understand the environment from an IT perspective. You know, go through the risk assessments and think about who you're, who's, what are the threats, both physical, logical, people and non-people threats. Regularly assess your environments and then stay vigilant. Just it's okay to be a little paranoid. And if you're in, you know, my world or David's world, sometimes we're a little more than a little paranoid. But, you know, we live in this world, so that's kind of what we do.

Rob Rudloff
So, questions? Did we get any in the in that chat? I didn't.

Sharon Trilk
We have three questions. The first one is, do you have any statistics on attacks specifically for Colorado?

Rob Rudloff
I did not isolate the attacks to Colorado. We can dig that up, I think, but I did not do that as part of the research for this. Sorry.

Sharon Trilk
No worries. The other one is: I had heard once that any time wire transfer instructions include a SWIFT code that means the transfer is international. Is this true, and is it common in wire fraud?

Rob Rudloff
So it's very common in wire fraud. I don't know about the SWIFT code. I'd have to ask my friends in banking to be on that, but I know that. I don't know if you if anybody saw but on one of those the screens with the dollar signs, you know, it mentioned real estate, and that's because of the email attacks that take over email threads between realtors and the closers and the banks and the money gets wired to the wrong place and gets stolen. But yes, anything that indicates an international thing like that or just a change at the very last minute to wiring instructions should always be suspicious and always be validated through, again, don't let them call you. Make sure you call them on a known good

phone number. If you're worried at all, and you're in that position to do it, call the bank and do some sort of verification with them. Bankers can be very helpful if you There we go, Dorothy gave it to us.

Rob Rudloff
All right. In the comments, Dorothy gave us--

Sharon Trilk
A SWIFT code known as a BIC, or bank identifier code is a unique 8 or 11 character identifier that banks and other financial institutions use to identify themselves in international transactions. It's crucial for ensuring that money sent internationally reaches the correct destination. Other question is: what advice, if any, do you have for organizations that allow widespread use of low code, no code, tools, without oversight? I know this pretty broad question, but governance, of course, is important. Any others?

Rob Rudloff
The real thing there is sensitive data. Know where your sensitive data is. If the low code and no code is not touching sensitive data, maybe you can be more relaxed about it. But if it's touching PII, ePHI, credit card data, anything that's considered as sensitive data, then you got to have that governance to make sure it's handled appropriately and controlled appropriately.

Sharon Trilk
And last question: can these emailed wire instructions be modified in transit before delivery?

Rob Rudloff
Typically they're not intercepted, and then, typically they're what they would do is intercept the one you sent, delete it, and then send a new one that looks very similar, but is wrong, is incorrect. So it's not usually can't be intercepted and changed in flight. A nation state, maybe. Like most of the regular attackers, David made the point earlier, they're going after the low hanging fruit. They're not going to work too hard if they don't have to.

Sharon Trilk
All right. Well, thank you everyone for enjoying the presentation. I've seen lots of great comments there. We really appreciate that. Thank you all for joining us. Please don't hesitate to contact any of us with any follow up questions, request to learn more. If you want to quote for any of their services that you would like to get, Please save the date for our next Webinar, Wednesday on May 21 with TEKsystems. And if you haven't heard, our Micro-Grant program is open for applications until noon on May 23rd, so please get your applications in for those as well as registration for our 13th annual User Conference, which will be held on Thursday September 4th at Empower Field at Mile High this year. We're very excited about that. You'll find those links on sipa.colorado.gov, and be sure to subscribe to our monthly newsletter to keep up with any upcoming events and news that we have, find other services that we can help you procure, and useful accessibility and cybersecurity resources. Thanks again, Rob and David, we really appreciate you being here with us and all of you have a wonderful day.