Maurice Fuller

Today I'm with Richard Peters, a senior information security advisor who serves as the leader with UHY's Consulting Technology Risk and compliance group. We'll be diving into cybersecurity and the importance of having a strong cybersecurity defense to protect against breaches, cyber attacks, and ransomware. Richard, welcome and thanks for joining me today.

Richard Peters

Thanks Maurice! Glad to be here, appreciate it.

MF

Awesome. So please tell us about yourself and UHY.

RP

Yeah, you bet. So overall with UHY, we're a global provider of accounting, tax, and consulting all around the world. I'd say everything from that dynamic middle market to fortune 500 companies. There's a large practice around the staffing industry—a big presence in our client base. I fit in that consulting side of that, specifically in cyber security. And generally I kind of compartmentalize it into four buckets.

So the first one of those is we get permission to hack our clients. We call that penetration testing, so any kind of that very technical, nerdy, cybersecurity specific testing falls in that bucket. Specifically for the staffing industry, we do a lot of security assessment. Those are where you know you probably need to do something in security and you know there's limited resources, limited budget for that, so you want to spend those dollars as wisely as you can for those biggest risk areas. So security assessments let us build those roadmaps to help figure that out; so that's the second bucket.

The third is everyone's favorite of compliance. Generally that's around credit card security, pci. We do a lot of that as well as HIPAA security for protected health information. And then the last bucket is the one nobody wants to be in and that's incident response, the forensic side of these. When an incident occurs generally that's when those services come into play.

MF

Okay, got it. So why should staffing firms care about cybersecurity?

RP

Yeah, good question. So that's where all the data is. You know, people say why do you rob banks? That's where all the money is. Well, from a staffing perspective, you guys have the gold mine when it comes to personal information. Identity theft—I mean you guys would be headquarters for that. So there is a ton of juicy data that's there from a bad guy perspective that they would be after. Credit cards are in the news a lot and that's definitely important to protect, but the dollar value that a bad guy gets for an

identity is much, much higher than it is for a specific credit card. So if I'm an entrepreneurial bad guy, I'm definitely going to go after a staffing company for the ability to perhaps steal identities or be able to create identities or to be able to do longer scams around IRS tax returns for these social security numbers and things that I collect. You're a gold mine of data in that industry, so it's definitely best to be aware of that, I think.

MF

Okay, got it. So just how vulnerable are staffing firms?

RP

Yeah, so you are a target and I think that that's probably the first thing to think about. A lot of organizations are like, well, we're small, we're regional, we don't make the news, no one knows who we are. That's changed. The bad guys are looking specifically at different industries and different groups. We've seen some of the large software providers and software as a service cloud-based systems that serve this industry being targeted, and now we're seeing that trickle down to specific staffing firms. These are smaller regional firms that you would not expect that a bad guy would be aware of. They are doing their homework. They are very aware of the industry, and they are very aware of the participants in that industry. So we are seeing targeted attacks specific to the staffing industry. In general the industry is benefited from not being on the radar as much, so I think there's maybe been some lax practices on the security side. The bad guys recognize that they're starting to have some success in the industry, and we expect that to continue to to pick up.

MF

Okay, so if a staffing firm is the victim of a ransomware attack, just how disruptive can that be from a financial perspective and from an operational perspective?

RP

Yeah. So maybe or maybe not you have insurance there, and that will help in some cases, in some pieces. But I think you kind of alluded to where some of those bigger problems are. Specifically we see ransoms that start off in the multi millions of dollars. That's extremely common. That's the starting rate. As you go through the process, there are professional ransomware negotiators now as a profession and they get that price down, but I'd still say those are… I mean, the one we just finished up recently was just under a billion dollars, and that's just specific to the ransom.

So past that you have reputation damage. During the process that that information gets out there, the recovery efforts are extremely expensive. The breach notifications, the disruption of your operations. I mean you are literally down likely for weeks as that process goes through. You have incident responders—something that we do. We're gathering evidence. We have to take systems and turn them off to capture images there. So not only is it the ransomware and the ransom itself can be a huge amount of money. It's really the disruption to the business, that lost revenue, that is a major part of that.

MF

What about cyber insurance? Doesn't that cover me?

RP

So to some extent. There's different, I guess, quality levels I would say in your coverage there. So depending on what you've purchased and which group is providing that, you have different levels of coverage there. We've seen some that do very well. They will pay the ransom on your behalf. They'll even hire the negotiators. During the breach they're generally pretty good about assisting in that process. But as soon as the incident is over, in the recovery efforts, that's where you really need to look at your coverage now because a lot of those coverages don't cover that. It's like, okay, well now we've got to rebuild. Okay, now we need to do a security assessment. Now we need to figure out how it started. Now we need to figure out what tools or products or specialty consultants we need to help shore these things up. All of those things are typically not covered unless you've really called those out.

Then we're seeing another big trend where there's been so many ransomware attacks that even if you've had cyber insurance for long periods of time, you're being pressed to do security assessments and pentests and some of that testing to prove that you're doing those things that are needed to have a good security posture before they'll even renew your insurance. So cyber insurance is a very, very wild area right now.

MF

Alright, got it. So you mentioned some of the security breaches that you've dealt with. I was wondering if you could share with us some of the incidents that you've seen, and also, what does it feel like to be inside an organization as a leader that's been attacked and is subject to a ransomware attack?

RP

Yeah, so our term is the hair on fire moment. If you've done some preparation, you have incident response planning and things that may help you see the light in some of these. But most of the time it's all of a sudden that you're in the thick of it, so we say your hair's on fire. You're panicking. It's your business. It's your customers. It's your data, and you feel a bit helpless. Part of our job when we come in as incident responders is to kind of be that voice of reason and to guide you through that process. Ransomware is probably the biggest problem that we've been fighting, and it seems like it's every week. And it's always on a Friday, and it kind of goes into the weekend, or it occurs over the weekend and Monday morning they come in and everything's locked up.

Ransomware is the biggest problem that we're seeing. We see that continuing forward. It's a bit worse in that not only are they encrypting all of your data and all of your systems, but before they do that they—we say exfiltrate—take or steal some of your data and then to help you pay that ransomware, it's a double extortion. They'll say, hey, not

only are you not going to get your decryption key, but we're going to release this data that we stole to the public unless you pay up, and you better pay up within x amount of time. That's this kind of double extortion to really put the pressure on you to pay that ransom.

The second area especially in the staffing world that we're seeing a lot too is what we call business email compromise. A lot of firms across the world in every industry are going to Office 365 or these cloud hosted email platforms, which are great. I mean I would definitely prefer that over having that in-house. But the problem is those aren't always necessarily set up as best as they could be, and we see these password guessing password spraying attacks where basically someone just logs into your email account. We're seeing those being very targeted as well. Accounts payable, the controllers, the CFOs, right? The money people are being targeted there. Once you log in, you are logging in as a legitimate user so it doesn't tend to raise a lot of alarms. So then bank account numbers are getting changed where deposits are made, and emails are being fired off and then hidden or deleted to say hey, we need to make this change or hey, we need to send some money here. So that's been a huge problem. I'm sure we'll talk about it, but there's some strategies around what I can do to prevent some of that. Business email compromise is probably the second one.

Just to round it out to have three: this world we're in now where people are changing jobs and there's better offers here and there and people are moving around, we have seen a big pickup in intellectual property theft. So before someone leaves a technology company to go to another place, they may download a bunch of data or they may just keep the data they've generated and they've moved to another organization. Through that process, maybe there's some inkling that something's gone wrong. So the forensic side of that has picked up a lot as people are moving and changing positions. The theft of some of that intellectual property, whether that's technology, whether that's a customer list, whether that's the secret sauce for an organization, that's picked up as well. So I'd say those are the big three that we seem to be dealing with again and again and again every single week.

MF

Alright. That makes sense. How about the remote workforce? How has that changed the requirements for cybersecurity?

RP

So we've been seeing it for a long time that the perimeter is dying, and some have been ahead of the curve saying the perimeter is dead, focus on the endpoints and the individual users in an organization. Well, with Covid and just everyone instantly remote, that absolutely killed the perimeters. When we say perimeter, that's the firewalls and the moat you put around the business. Well now almost one hundred percent, almost every organization had remote users immediately. So we saw all kinds of crazy things where now the the business laptop is on the home network where the kids' laptops are at and

the Xboxes and all those things. So we see a pickup of attacks on the endpoints, but really, we just saw targeted attacks against the people. So now you've got people somewhat isolated. I mean, they're communicating via email and phone and that sort of thing, but they're not sitting side-by-side in an office. So we see, especially again for the accounts payable and controllers and CFOs, those who have some control or influence over the money, being targeted in these organizations. They're on a bit of an island so they're targeted and they can't say “hey, did you get that email? That was kind of a weird thing.” The water cooler talk doesn't happen as well.

These targeted attacks have been a bit more successful because of this remote workforce. Then the other thing we've seen a bunch of is that immediately the business has to enable some type of remote access, and some had it in some capacity and some had to shore that up quickly to continue to function as a business. So we've seen lots of attacks against remote access technology. Remote desktop is something that Microsoft provides out of the box. We saw a lot of people enable that and it works great, which is good, but we see tons of attacks where if you just spray it with passwords and usernames and emails and all that stuff that is readily available on the internet, eventually you're likely going to be successful. So we've seen just remote technology that gets hacked just because it was opened up and it's sitting there. The perimeter is dead and be very aware.

MF

I know that as we've moved into the Cloud some companies feel more secure because others are handling their applications, but I wanted to ask you about that aspect of it. How has the Cloud changed what you're seeing in cybersecurity?

RP

Yeah, for sure. The Cloud is, like we say, just somebody else's computer, so there is still risk around those systems. My personal perspective is that the Cloud is probably better than an on-premise solution. I say that because we've seen so many on-premise solutions that the care and feeding of those systems probably aren't as good as they should be, and so they're vulnerable to all kinds of things. You move to the Cloud and some of these large providers generally will do a better job in the patching and the care and feeding of those systems, so that's a good thing. But what we've seen is that there's almost this magic button: it goes into the Cloud, it's saving us some money, and I don't have to patch it anymore. But they forget there is so much complication to the Cloud these days. So what used to be patches and vulnerabilities that come from not being a patch system, they're now going into configuration problems.There's still a ton of exploitation there, but it's just a different type. It's misconfigurations. It's open data. It's shared keys that are out there. So there's still tons of attacks. They're still happening, just the type of attack has changed. Cloud is a good thing. Definitely that is our future and that's where we're at, but we cannot rest on that as perfect cyber. It just changed the types of attacks that we're seeing.

MF

Yep, that makes sense. Okay, what about things that owners should do immediately to improve their security posture, and what cybersecurity readiness actions should owners have in place to protect the future well-being of their company?

RP

Yes, that could be a really long list. I would say that the number one thing I would do is multifactor authentication, sometimes called two-factor authentication. We're using these Cloud systems. We have our emails, we have all the software and things that we use, bank accounts, you name it. Most of the larger ones support this functionality called multifactor authentication. So you have your traditional username and password but then you have a second factor, which is maybe that you have an app on your phone that has a number that changes every 30 seconds and you put that number in, so it's one more additional piece of information you need to successfully authenticate to a service. So when I'm a bad guy, it's not too difficult for me to get your username and password. Your username is probably going to be your email address. That's almost public information these days. Your password—the odds are I could probably guess it or guess somebody's in the organization. But if you add that second factor like a phone with a numeric that changes, then that's very difficult. Now not only do I have to get your password, I have to somehow find you and get your phone or look on your phone or hack your phone. So just by adding that it makes it extremely difficult to log into those services. Anywhere you can enable that, do that.

The second thing I'd say is pay attention to backups. We've seen a big problem in backups where we've solved the backup problem, or it feels like from an IT perspective. Like backups work, they're automated. We've got a large disk. We don't have to worry about storage, and everyone feels that, and I would agree, backups are working very well. The problem we're seeing is those backups, they're kind of your answer to the ransomware. If your backups are working and they're protected, you will have some disruption maybe but you don't have to pay that ransom because your data is safe. But what we're seeing is that those backups are working, they're doing their thing, but they're sitting on the network just like every other device and they get ransomed up like everything else. So they're fully encrypted, you have the backups, but you cannot use the backups because they're encrypted too. Treating those backups almost as if they're as important as your crown jewels is something we're recommending companies look at. Your backups are probably working and doing well hopefully, but start treating those to segment them off or get them off the network or they're copied to a disk that's not physically plugged in so if that event occurs your backups are protected.

Then just the last couple things there is: go in with the expectation that you're going to have an incident, right? It's not if but when, so the more that you can prepare yourself for that… Insert response planning, just thinking through and having a tabletop or gathering the leadership together and saying, what would we do if this event occurred? Who do we call? Do we have legal counsel already on speed dial? What is our insurance, who

would we call for our insurance? Who's our incident responders, or who gives us that information? Just think through those and kind of start writing those down; that incident response planning process is extremely important. Then think about things like logging and audit records. Within IT, there's logging everywhere, and from a responder perspective that's gold for us to help you figure out what happens. A lot of times you've moved to the Cloud and you didn't really enable robust logging, so we look at it and say yeah, it looks like a bad guy logged in from Russia. That's all we could tell you because that's all the logs that were there. So the more you can prepare, get robust logging, get your incident response plans together, the more prepared you'll be for that hair on fire moment.

MF

Alright. That's great information. I was going to say that if you have protections like two-factor authentication in place, that could make it much more difficult for hackers to penetrate your infrastructure, and since they're looking for the path of least resistance, a few things could just point them off to other staffing firms that they might want to hack into instead of yours.

RP

You know, we always say just don't be low hanging fruit, right? If you can make it a little bit more difficult than the next guy, hackers are traditionally lazy, and so if there's just a wide open field of targets out there and well, this one's a little bit too complicated, just move on to the next one… I mean there are plenty of vulnerable sheep out there that the wolf can get. Just don't be the low hanging fruit.

MF

Exactly. And so you sort of answered my next question which was who should you call first if you're hit by a cyber attack, and you started to discuss the importance of having an incident response plan. So if you could, walk us through the preparedness that should be in place.

RP

Yeah. So I'd say the very first call you're probably going to want to make is to legal counsel. If you're large enough to have your internal counsel, then great, that's your first call. If not, as part of that incident response plan you should already be identifying a cyber security breach professional attorney to have on speed dial. Retainers are out there. You could have those. That is probably the very first thing because they've gone through this multiple times, they know the state and federal laws, and you have protection because you're under the council there. That's the very first call you should make.

Then I'd say the second call is to your insurance carrier. They have programs, they have partnerships, they even have maybe preferred vendors that they will pay directly on your behalf. So a lot of times there's maybe some cash flow issues there if you have to shell

out the money to the incident responders or to whatever it is and then you've got to wait on the insurance to pay you back. That could create some cash flow problems. A lot of times the insurance company has on their speed dial different organizations that they will pay direct on your behalf, so that protects your cash flow there. Those are the very first first two calls I would make. Make sure you're under privilege with legal counsel to get their guidance. Your insurance carrier is the very next call you make. Then that should start off that incident response process. There's lots of templates that are out there, and any good cyber security organization or consulting organization can help you build those plans and tabletop exercises where you practice those maybe once a year. You want that hair on fire moment to be less hair on fire, right? It should feel like, okay, I remember this is what we're gonna do, and the calmness through that makes a world of difference.

MF

Alright, excellent. So any final thoughts you want to share with our listeners?

RP

Just being vigilant. We see time and time again where, how did we get to this situation? Were they targeting us? The answer is yes, you're being targeted now. It's being vigilant, it's not being the low-hanging fruit, it's putting some thought into this ahead of time. Cybersecurity is like insurance. I mean none of us really want insurance, we don't want cybersecurity or their expenses. But when you need them, it's the best money you've ever spent. Cybersecurity is kind in that field. If we can prevent things from occurring, the recovery side of this, the lost revenue, the reputation and all, it is money well spent there. It's kind of hard to think through that. But if you think of the ramifications and kind of start planning around that, I think it's just—it's wise money spent, we'll say.

MF

Alright, fantastic. What's the best way to get in touch with you and UHY?

RP

Yeah, you bet. So UHY is easy to find but you always go to uhy-us.com. And myself, Richard Peters, I'm always always glad to answer cybersecurity questions. We love what we do? My email is rpeters@uhy-us.com, or if you still use phones, we have that too: 713-325-8684. Always glad to talk shop.

MF

Alright, fantastic. This has been a highly insightful discussion. Thanks everyone for listening, and we'll look forward to seeing you on the next Staffing Technology podcast.