BARNES DENNIG
Accounting • Tax • Business Insight

Cybersecurity for Construction | Video Transcript

Robert Ramsay, CPA, CISA, CITP, HITRUST CCSFP
Dan Holthaus, CPA, CCIFP

Dan Holthaus:

So Robert, you know we have such a significant amount of construction firms in our practice. What kinds of things do they need to be considering when it comes to cybersecurity?

Robert Ramsay:

Yeah. Thanks Dan. My favorite thing to help them with is winning new work, and putting disaster recovery and continuity planning in a bid can sometimes demonstrate that they are more able to get the job done on time, so that includes disaster recovery planning, details about that their systems are backed up and ready to go, and even a history of availability and consistency with their systems. So it starts with just winning work, which is kind of fun.

Dan Holthaus:

Interesting, interesting. So there's clearly a difference between what happens in their office setting and what happens in their job site setting, so can you talk a little bit about what kind of cybersecurity concerns they have to be dealing with in both of those two areas?

Robert Ramsay:

Yeah, sure. It's not hard enough to just keep your office secure, but they've got to move it on site, all different places over the city, and have the place transformed while they're using it, so yeah, it's a lot harder to have a wireless network on a mobile location and a lot of devices. They've got not just laptops, but tablets and phones coming and going all the time, but the security principles are the same in terms of encrypting them, making sure they're using the proper network, only their network. Some of the same things we tell office workers to be careful of when they go to a coffee shop, that construction workers need to be careful when they're on a job site.

Dan Holthaus:

Interesting.

Robert Ramsay:

Yeah.

Dan Holthaus:

So what kinds of things, from a compliance stance, would you consider that a construction company needs to be worrying about?

Robert Ramsay:

Our smaller residential clients are concerned about payment card industry data security standards. They take credit cards more often, and that encompasses a series of cybersecurity requirements covering encrypting data, ensuring proper access to that data, and then annually training your people and making sure they're aware of these requirement standards, and those have benefits beyond just being compliant. They can lower cybersecurity insurance premiums, and they generally just have a healthier environment when people are more aware and smarter about their security.

Dan Holthaus:

Okay. Can we go off topic with considerations of things that have been happening to some of our construction clients, like, I'm not going to name any names, but we've had clients and prospects have ransomware attacks and malware attacks. What kinds of recommendations would we have for clients around some of that kind of stuff?

Robert Ramsay:

Oh yeah. Well, the construction clients are no different than others in terms of multifactor authentication being the number one kind of prevention, the best tool now available to them, so requiring like we do, where something comes up on your phone when you're logging in on your tablet, that's one of the key security considerations. And then the common concept is the human firewall, so that person who's clicking on a message is the last line of defense, and poor construction workers. They got enough to think about and one more thing is, "Hey, is this message actually a valid, good message from my team?" But anything that can help them do a good job with that, like the training to help them be aware of proper cybersecurity health, is beneficial to them.

Dan Holthaus:

Well, actually, Robert, some of our larger commercial contractors accept payment cards, especially if they have a robust service division.

Robert Ramsay:

That's a good point, Dan. So this payment card data security standards will apply to them too, and it scales nicely, so there's a different set of requirements depending on the size of the organization, how

much activity they have, how many transactions there are, so that's good for them too, even more helpful. That's a good point.

Dan Holthaus:

Great, yeah, because our contractors do have quite a variety of size and so I would certainly not want to have to go through the rigor of compliance if I'm a $10 million contractor similar to maybe a $200 million contractor.

Robert Ramsay:

Yeah, exactly. So for the smaller ones, it's a five page questionnaire and for the large ones, it's a hundred page questionnaire, so it does scale depending on their needs.

Dan Holthaus:

So Robert, we've talked a lot about what a contractor might have to do to keep their own data safe, but what kind of risks are out there for what they might be doing with their customers?

Robert Ramsay:

Yeah, that's a good point. You reminded me the other day how Target, that big breach a few years ago was a contractor and contractors are under a greater scrutiny everywhere because of that and so anything a contractor can do to show that they've got proper data security hygiene, can help them win work. So all of these things we're talking about, whether it's encryption or passwords or multifactor authentication or cyber insurance, can help put their clients at ease that they're not going to cause a breach in their data security posture, especially if they're in a space like healthcare or education or something international where there's a heightened sense of awareness and concern for data security.

Dan Holthaus:

So Robert, you've been working with a lot of our contractors over the years, doing IT audit help as part of our requirements for our audits, but I know you've done some other projects with some of our contractors with respect to their IT internally, so what are some of the things that we could help our clients with?

Robert Ramsay:

Yeah. We have a lot of successful clients that come to us and say, "Hey, what can I do to be more safe, secure, and compliant? What can we do to ensure future positive results and earnings and all that?" They want to reinvest in the business and they're worried about cybersecurity, and so our team often helps with making sure they've got best of class security, policies and procedures and training in place.

Sometimes that means putting more in the cloud and being more robust and agile. Sometimes it means helping with the bid package, as I mentioned before, and trying to present better to win more work, and sometimes it means we just don't know what we don't know. How are we doing compared to others in our industry? That's really fun, being able to help them and hold up a mirror and let them know what they're doing well and where there's opportunities to improve.

Dan Holthaus:

Great. Thank you.

Robert Ramsay:

Yeah.