BARNES DENNIG
Accounting • Tax • Business Insight

The Risks of Ransomware | Ask the Experts Video Transcript

Robert Ramsay, Director & Cybersecurity Practice Leader
Mark Wurtenberger, Senior Manager & Intelligent Process Automation Leader
Kat Jenkins, Marketing Director
November 2020

Kat Jenkins (00:09):

Hi, and welcome to Barnes Dennig Ask the Experts. I'm Kat Jenkins, Marketing Director. And today, we're talking ransomware with Cybersecurity Practice Leader, Robert Ramsay, and Intelligent Process Automation Practice Leader, Mark Wurtenberger. Mark, and Robert. Thanks for joining us.

Robert Ramsay (00:26):

Kat, thanks so much for doing this again. And Mark, thanks for joining us today.

Mark Wurtenberger (00:30):

Yeah, happy to be here. All right, Robert, why don't you start off with, what is ransomware and what are some different ways an attack could occur?

Robert Ramsay (00:39):

Yeah, ransomware is this virus or software or malware that shows up and encrypts data on your local machine and even on your network that can cripple an enterprise. It can stop a business or a hospital from being able to process data. It can slow down all of their systems. And then the criminals who build this and send it and try to get it on your system, then require a ransom. So they want money to give you the key to that encryption, to unencrypt the data and give you your data back. It's very tempting to want to pay them to get that back and solve the problem and get back to operating really fast. And the way it comes is quite often in the form of an email, an innocuous, phishing email that you think it's a free certificate for coffee, and it's really a link to some bad software that starts encrypting your files.

Mark Wurtenberger (01:33):

Thanks. And so given today's working from home environment, what sorts of additional challenges do companies face given the current landscape?

Robert Ramsay (01:44):

Yeah, there's just a lot more stress on the employee, on the security folks or the IT professionals trying to support them. Of course, if you're at home, you probably own a home Wi-Fi that may not be as secure as what you have at work. You may be on a home machine, you may be sharing your machine with family. And you're out of your routine so you may be clicking on things that you wouldn't normally click on, and you may be working with people who are also at home, so that if a fishy email comes in and it's not the same, you might think, "Oh, well, they're not at the office anymore and that's why some of this contact information is different." So there are a lot of stresses on people that are making them more susceptible to these things, especially now.

Mark Wurtenberger (02:27):

So what sorts of things can be done to help companies mitigate these attacks?

Robert Ramsay (02:33):

Yeah, there's three things mostly. One is training, helping your employees to be paranoid, not clicking on things that they're not absolutely certain are meant for them and are good, healthy parts of their email. A second thing is cyber insurance. So the insurance writers now that cover this, an insurance company can step in and either pay the ransom or pay to help clean up all your systems and machines and get back up and running. And then testing backup. So another solution is to delete all the encrypted stuff that the bad guys have made useless, not pay them, and just restore your data from backups and then continue operating. That requires having a lot of confidence in your backups and testing them and making sure that they're fully available, they're complete, and you can get back up and running quickly.

Mark Wurtenberger (03:28):

So what are some ways we can help clients alleviate these concerns they have with ransomware?

Robert Ramsay (03:34):

Yeah, we help in a few ways. On our annual audit visits for our audit clients, we'll go through their control environment and ask them about their network security, about their employee security training, about their cybersecurity insurance, about their backups, and we'll talk through those things with them. We'll share stories. We'll ask them if they're concerned about this kind of thing. Speaking of stories, recently, a company in our town the bad guys got inside the network and convinced them to delete their backups. They sent these phishing emails to the IT folks and said, "Oh, it's time to clean things up. Let's delete those." And then they unleashed the ransomware so that one layer of defense was gone because they were super clever.

Robert Ramsay (04:19):

So sharing that kind of story and telling people, "Hey, even if you get an email that says, 'Delete the backups,' think twice, double check, make sure that's not really what you need. So that's the kind of thing we help, by just sharing information and sharing support with others. We also help with special projects or internal audit efforts. We'll test backups, or we'll help with the training to make sure the training is consistent and complete and what people need. There's different types of training depending on if HIPAA applies, if they're in healthcare or other sectors. So we'll help with training, we'll help with backups, and that kind of thing. So that's what we help people with.

Mark Wurtenberger (04:59):

Good to know. And then so a lot of this information is new to folks out there. What resources do you recommend for the non-technology people to get up to speed in this area?

Robert Ramsay (05:11):

Yeah, it's funny. There's information coming at us from all over, and I know IT people, we've got our own favorite feeds and industry sources, but for leaders or executives or just people that are non-technical, I like to, especially if they're readers or get audio books, I like if they can find a story or something that's interesting that also weaves in some technology information. And there's two that are related to this. One is called Ghost in the Wires. It's a Kevin Mitnick memoir. He was an older, super hacker that the FBI was chasing. It was back when you paid for long distance, so he was trying to hack for free long distance and he got into the FBI's phone system and they were in phone system and they were hacking each other's voicemails.

Robert Ramsay (06:00):

He knew when they were coming and he left a plate of donuts on the table, and then he left his apartment and they came in. And so there's all kinds of funny stories woven in, but you learn to be really paranoid, because what he was very good at was convincing people of this fishing concept, that he was a good guy on their side and to give him their information, confidential information. And I learned from reading that, that as paranoid as I am, and I do this for a living, I could fall for that. There could be a system where if he spent months connecting with my peers or people I'm connected with, and then he made an ask of me to do something and I confirmed with someone else that he had already talked to, that he'd convinced them that he was trusted, that it's possible. So that's one that I like. It's amusing, it's got a little spy versus spy to it, and then it does remind you what the bad guys think of and how they plan before they do this kind of thing.

Robert Ramsay (06:54):

The other one is a little nerdier. It's called Countdown to Zero Day. It's about the virus, the Stuxnet Virus, that the U.S. Special Services agencies and Israel unleashed on Iran in the Iranian nuclear facilities. And it's a virus, but it caused their facilities to blow up. It sabotaged their uranium enrichment and it's written by a reporter from the angle of evidence that's coming to the general public from this virus showing up at anti-virus places. So McAfee, they see this virus, but it doesn't hurt a laptop or a regular machine. And so they're investigating. And so the story, it's a true story, of them trying to figure out what it does and realizing that, "Hey, this is million dollar software. Who would have done this and why?" And then at the same time, weird things are going on in Iran's nuclear energy facilities.

Robert Ramsay (07:47):

The International Atomic Energy Agency is there and seeing things go awry and they don't know why. And so I think it's an interesting story if you're interested in any of that stuff, the technology or the international relations, and then it explains a little bit how the virus works, how anti-virus detects it, and what vulnerabilities there are in our systems. So those are a couple of things that I like to share.

Kat Jenkins (08:13):

All right, Robert and Mark, fantastic. There's some great information there. We know that this is a rapidly growing risk. If you have questions or would like to learn more about ransomware or would like to talk to one of our professionals, visit barnesdennig.com. You can set up a conversation or reach out via email. We're always happy to help, and we'll see you next time on Ask The Experts.