# Transcript: Ep 50 - Cyber Series - Ransomware Round Table

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker #1 (Narrator):

WGU's IT Audio Series. Flexible, portable, profound.

Speaker #2 (Dave Huff):

Hey, folks. Dave Huff Here with another episode of the IT Audio Series. Today we're going to be talking about ransomware. We've got a panel of program chairs at Western Governors whocombined they have over 100 years of experiencein the Information Security and Cloud computing area. We've got some real good experts that I'd like to introduce you to. We'll talk about ransomware, what it is, how you can protect your company from it. Get some perspectives on that and some of the current events. We'll also talk about how WGU can help preparestudents and folks in the industry to protect their companies in their ransomware space. I'd like to introduce you guys, Dan Mahler who oversees our Cloud Program, Mike Morris, who is the program chair and overseesour undergraduate cyber and Lane Melton who oversees the graduate cyber programs. Welcome, gentlemen. Appreciate you-all taking time to join us today. Yeah, let's start right off with the top. Any of you guys, in the news right now there's a lot of talk about ransomware attacks and ransomware. What is a ransomware attack?

Speaker #3 (Mike Morris):

Ransomware itself is a form of malware. It's a class of malware that's ever changing. It allows the user of the malware to basically encryptdata as well as propagate throughout a network like a worm. There's multiple types, there's 30, 40, 50 different variants right now. They even have ransomware as a service. You do not have to be a technical powerhouse to be able to use ransomware. You can go on the dark web and pay a price and use a whole series of bots to launch it.

Speaker #2 (Dave Huff):

Why is it called ransomware? What's the story there?

Speaker #3 (Mike Morris):

Well, ransomware is used to do two things. One, it will encrypt a victim's data. For instance say that you're a large university like WGU, and it gets into your network and they encryptall of our data so that we can no longer access our data. Then if we haven't run our business the way we should andwe don't have sufficient backups or up-to-date back-ups, we can't access that data. Our students won't able to access their data, won't be able to access their courses. That's part 1. Part 2 is once the data is encrypted, if you don't pay the price, you won't get your data back. The second thing that they're doing now is using it, say, "Hey, if you don't pay us money not only are we not going to encrypt your data, but we're going to put it out on the Internet.” When you have personally identifiable informationout there now being leaked to the Internet, that's a problem.

Speaker #2 (Dave Huff):

Can ransomware attacks be prevented?If so, what are the best practices there to keep control of the data?

Speaker #3 (Mike Morris):

Yeah, absolutely. It's like anything. Ransomware can be prevented. It gets down to people processes, policy and governance, and having a clean house. I'm not sure which one you want to start delving down, I can start talking about people as an example. People by far are the weakest link. The reason they're the weakest link is because people receive a phishing email, that could be the way that the malware comes into the organization. They could be socially engineered. They can get a phone call. For instance, if you have a LinkedIn page and it says, "Hey, Dave you are the Program Chair for WGU and Network Operations. " You can receive a phone call. "Hi, I'm Company X and I like to start partnership with WGU, I want to shoot you over an email with that. " Then they go and they set up a fake company. You can go in and set up your own name and IP, let's say five bucks in less than five minutes, you get an email in, it's now malware, you click on it, open it up, then launches. Another thing that our users don't do currently, all users have a tough time password management. Being able to have strong passwords and maintain and manage those strong passwords. It's tough to have 50 different accounts and try to keep up with us. Last but not least, VPNs. We have a lot of people now working from home because of COVID, and so the working from home, or they may go to a coffee shop, or maybe they're traveling and they're working on that hotel network. Well if they don't have a VPN in place, they're not using it, then bad guys can see exactly what you're doing. I can set up a wireless site inside Starbucks and call it Starbucks 2, if I see the first one called Starbucks 1, you log into it and then you go out to the Internet and I capture all your credentials. Now I can gain access into your company network.

Speaker #2 (Dave Huff):

Sounds like on the people side, there's some education but there's also some technology that we need toput in place to close that gap and to try to control that vulnerability.

Speaker #3 (Mike Morris):

Absolutely, training is key. Being able to train your employees to know what phishing, know what social engineering is, and how to try to keep their own environments safe and clean.

Speaker #2 (Dave Huff):

Let me turn it over to Dan because Mike, you mentioned something about policy. Dan what's your take on that?

Speaker #4 (Dan):

There's something pretty common among a lot ofcompanies that have successful ransomware attacks. That's, they didn't have a defined policy. Either there's a lot of regulation or an industry standard that's not being adhered to. Just about everything has got one of those three or more things that you should do. Most of the industry standards like ISO or others, are things that you want to do minimum standards for securing your data, securing your networks or training. Because of that lack of policy and lack of policy enforcement, when you go and you do a third party security audit, you'll come up with deficiencies. If you don't address those deficiencies and youend up in what's problems with due diligence. You end up not meeting any standard, and people don't get trained, and you don't follow a legal or regulatory or industry standard process, you're more susceptible, in my opinion to ransomware, or just hacking in general. Really this boils down to governance, how you would approach governance, and how you would do your due diligence.

Speaker #2 (Dave Huff):

You made an interesting point too about the audit not following up on it because thatwas some of the findings in the Colonial Pipeline situation, right?

Speaker #4 (Dan):

Yeah, you'll find it's also with Department of Health Services in England. You also found that was with the city of Snohomish here in Washington State. They all had an audit or findings that said you need to do a thing and they didn't, so they didn't do the governance that they needed to do.

Speaker #2 (Dave Huff):

Okay. You know both of you guys have mentioned governance, and Lane, the program that you oversee asa program chairs or masters in information security and insurance, that program is geared toward governance, right? Focus on executive leadership practices. Would having executive and good leadership practices, would that have helped, in the case of Colonial, would it help to prevent their attack? Do they even have security leadership at the top?

Speaker #5 (Lane Melton):

Absolutely Dave, it makes a tremendous difference. You've not only got to have the technical expertise with your boots on the ground, your employees have to be trained, you have to have the governance, but you've got to have the leadershipin common technology domains. They know what these domains consist of, what they entail, and they know how to address the security issues within those common domains. It's absolutely necessary to understandthe common security domains that apply to ransomware, and that's what we focus here at WGU. We try to make sure that we're covering at least 10 domains of security that are going to cover ransomware along with regular, data security, telecommunications security and that type of thing. Governance is absolutely crucial. There's other organizations out there like NIST, the National Institute of Standards and Technology. They have various guidelines that they'veestablished to be able to protect information systems, to certify and accredit technological base information systems. If you secure these based on standards that are hard to establish, tried and true, then you're going to have a better chance at fending offransomware and people hacking your network in the first place.

Speaker #2 (Dave Huff):

We've talked about people, policy, and governance as three keystones. What happens then if your company is attacked? What can you do to minimize the impact or what are your options if youlost control of your data and the bad actors come looking for some ransom to release it? What can a company do at that point?

Speaker #3 (Mike Morris):

Dave, there's a couple of things that hopefully the company has done ahead of time. Then we'll go from there. Let me back up a step. We're talking about JBL. JBL was just attacked. It was dear to my heart because they obviously produce beef.

Speaker # (Dave Huff):

They're going to wake a sleeping giant there, aren't they?

Speaker #3 (Mike Morris):

That's right. They recently paid $11 million in ransom. What's interesting there is they spent over $200 million, that's their IT budget. For 2021 it was $200 million. They have 850 IT professionals in there yet they had ransomware come in. They paid the money. Why did they pay the money? Because they didn't want corporate information getting out on the Internet. That was a big concern. Now, what could they have done to prepare themselves for something like that? This is what some companies could do. I'm not going to talk about fixing systems. I have a list of 10 thou should do's that maybe we'll get to in a minute. But from a government standpoint, companies should absolutely have an up-to-date incident response plan, a business continuity and disaster recovery plan. They should practice these. They should have tabletops. They should practice these things yearly. They should involve all the stakeholders, including law enforcement, includingall the people that would be called if they had an incident. Another thing that could consider is possibly shifting some of the risks that they're exposed to by having cyber security and business interruption insurance. That is what several companies have done. It was to where they actually have insurance to help them offset the cost. Another thing that they could do is establish a corporate policy, make sure they have it reviewed by legal for the payment of ransom as an option. Make sure you're talking with Council as well as your insurance carrier. The reason why is because if you're paying ransom to a country that is on the government's watch list, you could be breaking federal law by paying the ransom.

Speaker #2 (Dave Huff):

Right. Yes. There's a lot to it, let options. Go ahead, Mike. You had more?

Speaker #3 (Mike Morris):

Yeah, I had two more and then I'll be quiet. Let's see. The other thing economists should be able to do is define the particulars of when, how, and under what conditions the decision to pay or not pay would be made. You know, this could also be an executive tabletop-type exercise. Last, the thing that the companies really need to consider, what are the disclosure requirementsfor breach notification in the states that they're in? Currently, 48 states across the United States have breach notification laws in place. Two of those are very interesting. New Jersey and Connecticut require that you disclose that you've been breached only if somebody has gotten inside your network. If they get inside your network, you have to disclose that if you're in New Jersey or Connecticut. That could have a big impact on your customer base. If your business is say, protecting somebody else's corporate network, consultant or whatever, and you get hacked, that could be a death nail to your business plan.

Speaker #2 (Dave Huff):

Yeah. I know and very few businesses are just in one state anymore. Dan, this operating in the Cloud, does that make organizations more vulnerable, or does it give them more protection options? What do you think there?

Speaker #4 (Dan):

A number of things, especially feeding into what Mike was saying, is that that disaster recovery business continuity plan should be in the Cloud, period. There's no reason not to be able toheartbeat between one data center and another data center now. Costs are equal, you can be running concurrent data centers, boom, done, call it good. But the other thing that's interesting about the Cloud and how security works in the shared responsibility model that you would have witha Microsoft or with an Amazon is that you can abstract your security better. You can separate out the responsibilities that are strictly your provider, whether those are Amazon or Microsoft, and actually turn those over. That allows you to free up resources from having to secure physical data centers from having to do physical other things and focus on code, focus on accounts, and focus on communications. You can actually set it up so that your databases can only talk to certain head units, you can't just access them from anywhere. You have to talk very securely between two different databases. Databases can replicate seamlessly across the board between data centers that can be geographically dispersed. Yeah, there's no reason why the Cloud can't help you, especially on abstracting security better, but it will also give you that opportunity to do that disaster recovery plan becauseone common threat to everyone that's had unpaid ransom is that their backups didn't work.

Speaker #2 (Dave Huff):

Isn't a good backup the antidote here?

Speaker #4 (Dan):

It is, it just depends on how you want to do it and how you want to test for it. You know, Mike was saying, do it as a tabletop. Mine is flip one data center off in the Cloud, see if you can failover to the other data center in the Cloud, and make sure you're running the health checks. You can do this in real-time back and forth and not skip a beat;not miss one second of business operations if you're in the Cloud by doing it that way.

Speaker # (Mike Morris ):

Hey, Dave, I want to add. Obviously, you can always do a long list of things to help protect your company, but I have eight that, real quick, I just want to bring up that companies should consider doing.

Speaker #2 (Dave Huff):

Sure.

Speaker # (Mike Morris):

The first one is a freebie. The first one doesn't cost a company a dime. 99. 9 companies could do it today with their existing infrastructure, with their existing software that they have currently. That is, on e-mail, make sure that they have bannering turned on so that when you get an external email, it comes up in a banner. First thing, the highlight of your e-mail, you'll see where it says this came from outside your organization. It doesn't cost a dime to turn that on, and it really helps your employees understand that. They'll start questioning and be like, well, why did the company president send mean outside e-mail asking me to send $100, 000 somewhere? I'm not really sure why he would do that. Bannering is a great free one that many companies don't do, but they should be doing. Another one is, know your assets. By that I mean data. As Dan mentioned, up to the Cloud. Know exactly where all your data is. Where is your data located? What are your networks? What are your devices? If you have a good picture of what you own and where it's located, then you can start protecting it. But the second thing is backing up your crown jewel data often in a crypt. As Dan mentioned, a Cloud would be perfect in that you could have it in multiple locations, do the failover test and see, does site A equal site B? Yes. That is awesome. Crypt your data. If it's your crown jewels, if it's that five percent, 10 percent of your business, the heart of your business, encrypt it. Decrypt it when needed. Keep your system patch and segregate it where appropriate. Easy thing, but people don't do it. Do vulnerability scans. You name a company, there's multiple companies out there that provide all different types of functionality and vulnerability scanning, but go through and do it. Follow up on those vulnerabilities. Do threat analysis. Make sure there are multiple threat feeds that are out there. You get the threat feeds, you can feed it into your next-gen firewalls and have them automatically block IP addresses, sites that are known bad. Do whitelist. Whitelist your applications. Those applications that should be running on your systems, allow them to. Those that don't, won't. Then blacklist your non-business site. If folks should not be going to ransomware.com, well, make sure you block that in your firewalls. Last but not least, as much automation as you canbring into your log analysis would be great. It would really help your security teams to be able to, if you can automate your log analysis from both network and systems, all your devices so that you can see when you have an event. You can see something come into your network, you can see it move laterally across inside your network, and then you can react to that. That's my list.

Speaker #2 (Dave Huff):

Lane, from the top-down, how do you effect these type of policies? How does the governance plan leadership, executive support, how does that drive these type of things?

Speaker #5 (Lane Melton):

Well, again, you've got to have the leadership in place from the get-go. In the case of this particular pipeline incident, they did not have top-level management from a technical perspective, and you need that. Another keen aspect of this is that our national laws andregulations have not necessarily caught up to the latest, "hacking techniques". The pipeline industry is not subject, like the utilities company, to various regulations and reporting requirements. They've recently just changed that. President Biden has asked for changes in regulation to the reporting requirements for pipeline-type industries, and also the people that they have in place from a management perspective, and how they're running their network. All these regulations are coming down the pipe, and you're going to have to have strong leadership that know these new requirements and are able to technically implement them within the company itself. You're going to need management, you're going to need people that know these regulations, you're going to need people that have the managementand the technical capability to make this happen, and that's exactly what we do in our Cyber Program at WGU.

Speaker #2 (Dave Huff):

Lane, thank you for that. Hey, before we sign off, let me go around the table really quickly and ask you guys about your programs, and about how WGU helps to prepare students to be successful in these fields. Dan, what is it about your Cloud programthat's going to turn out the best graduates that we have?

Speaker #4 (Dan):

The thing I like about this program is that we're Cloud computing framework certified. Which means you're getting the Cloud computing security, practitioner from ISC squared, you're getting CISA, you're getting Pen Test, plus you're getting the developer or the architecture, the sysops, the foundational certs, all this stuff is going to tie together, so you can just plug in and go wherever you land in the Cloud.

Speaker #2 (Dave Huff):

Right on. How about you, Mike, what defines your program?

Speaker #3 (Mike Morris):

In our program, our students will get 14 certs by the time they complete our program. As far as skill sets, vulnerability analysis, incident response, forensics, pen testing, that will enable them to be able to hit the ground running. This certs will prepare them to be able torespond to an incident within their organization.

Speaker #2 (Dave Huff):

Okay. Lane, what about you? What defines your program?

Speaker #5 (Lane Melton):

When the student comes into our program, they're going to leave with two certifications. One's going to be the Certified Ethical Hacker, and the second one is going to be the Computer Hacking Forensics Investigator. These are two timely certifications that'sreally going to technically prepare the studentto the hacking and attackingdemands that are on our network and information systems today. We're also going to prepare them from a managerial perspective. In other words, they're going to know the national laws that have to be followed, they're going know the common bodies of knowledge in the cyber warfare world, the domains that are applicable to that. They're going to know how to go in and approach things from a technical perspective, but also lead a technical team and have the managerial skills to be able to facilitate people workingfor them for the betterment of all the companies out there.

Speaker #2 (Dave Huff):

Right on. Not to be left out of the discussion, I talk about our network operations andsecurity degree program that culminates in the CCNA. We have a great suite of certifications all wrapped in with other courses. Not everything's a certification at WGU. I think it's important to also point out, gentlemen, that because we're competency-based, we don't really have semesters on timelines, so students can progress as quickly as they can throughthe programs so that they're out in the industry applying what they learned. They don't have to wait four years for an undergrad or two years for a graduate degree. As quickly as they can move through the program, pass tests, earn certifications, they can find themselves out in the workforce. Folks, thank you for this great discussion. I appreciate your expertise. As I mentioned when we started, there's over 100 years of security expertise on this call, and it was clear listening to you guys that you know what you're talking about. Thank you so much. Thank you everybody for listeningto this episode of the IT Audio Series.

Speaker #1 (Narrator):

WGU, a new kind of you.