Ransomware Defense Playbook: Practical Steps That Work | Transcript

Regina Akrong & Griffin Dickerson

July 2026

Regina Akrong:

Hey Griffin, good to see you.

Griffin Dickerson:

You as well.

Regina Akrong:

Today we want to talk a bit about ransomware, and I know it affects a lot of companies. I mean it just strikes and everybody is kind of not ready. Some people are. But I think it would be good to know a little bit about it, and you can start by telling us why we are still talking about it.

Griffin Dickerson:

Yeah. So ransomware, it's still one of the biggest risks that organizations face today. Like any cyber attack, the methodology, the attack point, and the technology involved is rapidly evolving far faster than any defense. Defense is always playing catch up. And it directly impacts businesses and business leaders, and IT folks and cybersecurity folks have to be on the defense at all times for it.

Regina Akrong:

So what does ransomware look like today? I know in the past, maybe in the 2000, early 2000s, so whenever I started, it would be they would start to encrypt, and then you see this screen that tells you that you have to pay. But what does it look like now?

Griffin Dickerson:

Yeah. So now it's not just availability. It's not just encryption. It's far more often social engineering based. And it's not just, you don't have encrypted files, that thing pops up and now suddenly you're in some kind of ransomware situation. It's more often unauthorized access, data theft. And the pressure comes from different angles too. Things like downtime, data exposure. Those are a lot of the stressors that we see now, whereas before the main factor was data theft and data loss. When now even, just being down for a certain amount of time, is going to affect your income and your value as an organization.

Regina Akrong:

How do these attacks usually start?

Griffin Dickerson:

Yeah. So like I said before, big point here is phishing and stolen credentials obviously. And then any unpatched or exposed internet-facing systems. And those are the main attack points there. So phishing, like we said before, is a huge one. That's why it's important to have that base level layer of training for your employees, for anyone across the organization that's going to be interacting with sensitive data, or any data at all really that you don't want exposed. Encryption now is kind of the final stage. So that's your last layer of defense if they're in your system. And it's not just the first one where folks are just coming in and taking things, that you don't have encryption. Most companies do. They have to find more creative ways around that.

Regina Akrong:

So how would you say this has changed compared to the past?

Griffin Dickerson:

Yeah. So there's a bigger shift to multi-extortion. So multiple points of pressure on an organization that could cause them to want to pay the ransom or entertain paying the ransom. And then they're also using data theft plus the ransom. So they might have control of your data, be in your system. You pay the ransom, they take your data anyway. So that's something to be aware of. And then now we're seeing more legal and compliance issues with ransomware. It can affect your reputation going forward. And your compliance, that once you thought was intact and in good shape, is suddenly exposed publicly.

Regina Akrong:

So how would you say the hybrid work since COVID and cloud, how would you say that has affected the risk?

Griffin Dickerson:

Yeah. I think overall it's just a larger attack vector.

Regina Akrong:

So how can organizations reduce the ransom risk?

Griffin Dickerson:

Yeah. Like I said before, I think step one is the phishing and social engineering training. Being aware that those things can happen and keeping an eye out for them. But then also just reduced entry points, patching, making sure your patches are up to date, making sure your software is up to date, your defenses are up to date, configured correctly. And then access controls obviously as well. Regular access

reviews, making sure that the folks that do have access to sensitive information systems, sensitive software systems, are the ones that are supposed to. And then the ability to detect any suspicious activity early on I think is huge too. That kind of prevents the attacker from moving laterally across your network. The faster you can isolate them and identify them the better.

Regina Akrong:

So some people would say, "Well, we have backups so we are not worried." What would you say to that?

Griffin Dickerson:

You know, that's not the only attack objective anymore, just taking the information, or deleting the information. Pardon me. I think now stealing the information or exposing the information online is also a huge issue. So just having a backup that saves you from the data being deleted is only one kind of avenue that attackers could take to affect their network.

Regina Akrong:

So what if you pay the ransom, they what? Do they still post your data out there?

Griffin Dickerson:

I mean, they certainly could. They certainly could.

Regina Akrong:

Yeah, you can't trust them.

Griffin Dickerson:

Yeah. No, I would not do that.

Regina Akrong:

So what do regulators expect when this happens, ransomware incident happens?

Griffin Dickerson:

Yeah, that's a good question. I think just like any other incident response procedure, you really want clear and quick, effective communication, identifying, "Hey, this is what happened. This is where we are. This is how we responded. And I mean, obviously customers and business partners want to see that you've effectively identified it and communicated it. But I think regulators want to know where specifically the attack is taking place, how it affected your system, and then what you did from there to remediate it.

Regina Akrong:

So I'm sure a lot of organizations may say that, "Well, we are ready. We can take it." I mean, what advice would you give to those who feel they need to learn effective ways of handling ransomware when it happens? How do they prepare for it?

Griffin Dickerson:

Yeah. I think we've touched on some of it already, but I think evaluating security training, access controls, the ability to have effective and up-to-date recovery processes are all the basics. I would say I think now with the evolution and the more advanced phishing and social engineering mechanisms, I think that baseline training for employees across the board is probably one of the most important ones. But then also the ability to identify it once it's in the system too.

Regina Akrong:

And to add to it, having a regular phishing test for the employees to be able to identify some of these emails and not click on links is very good to keep them kind of reminded every day.

Griffin Dickerson:

Right. Yeah. And I think also keeping employees up to date with things. So when new attacks are coming out or new types of attacks that happen, keeping everyone informed, "Hey, this is a thing that can happen now."

Regina Akrong:

Showing them examples of what it looks like.

Griffin Dickerson:

Yeah, exactly.

Regina Akrong:

Yeah. Okay. And then having a policy on ransomware would be I think as to whether you want to pay or not pay. It would be a good way to prepare because you don't want it to strike, and then you're now deciding what to do. It's like, "Oh no, should we pay? Should we not pay?" Having that policy on file.

Griffin Dickerson:

Yeah. And then that can also go into the documentation aspect of it too afterward. How do we document this properly to make sure that we're doing all the correct things in a legal sense as well?

Regina Akrong:

So what would you say to the leaders of these organization?

Griffin Dickerson:

Yeah. I think overall it's a business responsibility. It's not just a technical responsibility. We've mentioned the phishing training, the social engineering, and the risk that it puts your business in, not only with your own data and with your money, but legally as well I would say, when you're using customer data and sensitive customer data. But I think resilience kind of depends on the actual prevention, the detection, like we stated before, and then obviously the recovery if it comes to that. And then lastly, I think planning has to include clear communication, and then some form of legal advisory in response to that.