Laura PAVIN: Hey there, it’s Laura Pavin. Before we start, this is part two of our cybersecurity conversation with former NSA director Mike Rogers. So if you haven’t already, I’d recommend you listen to part one first. This one will make a lot more sense if you do. Okay! Back to the show.

…

PAVIN: It’s day two of my conversation with Mike Rogers, a retired four-star admiral…as well as a senior fellow and adjunct professor at Kellogg. Last time, we talked about why cybersecurity is a leadership issue as much as anything else, because it’s all about managing risk. We also discussed how to protect yourself and your workforce against cyber attacks…and how to gauge your readiness for a real attack.

[music]

But what do you do when all of your defensive tactics have failed…and the enemy is already inside the building? This episode, Rogers makes the case for acting quickly…even if you don’t know a whole lot about the extent of the cyber attack. He wants you to think twice about paying that ransom…even if it feels like the easiest exit. And he wants you to seriously consider going public about being breached…because we can’t understand cyber criminals if we don’t talk about them.

“Easier said than done!” you might be thinking.

Don’t worry…Rogers VERY MUCH walks the walk.

Mike ROGERS: I have had networks penetrated and, um, that's never a pleasant conversation in the white house situation room. Yeah. Yes, Mr. President has really happened. Um…

PAVIN: Luckily you won’t have to do THAT.

We get into all of it next.

…

After you realize you’ve been breached, Rogers says your top priority is to act quickly. Even before you completely understand what’s happening.

ROGERS: You can't just wait to say, “well, I'm just going to wait until I have perfect knowledge or until I have a high level of confidence.” In the middle of a cyber crisis, look, you are going to have to get used to the idea that you're going to have to make decisions with incomplete and often conflicting information.

[music]

PAVIN: A lot of times, Rogers says, it’ll be really obvious that you’ve been breached because…cyber criminals will send you an email saying that they’ve breached your network…and that you may have noticed you can’t access your network…and oh by the way… we’re going to include some of the data we’ve extracted so you know this is real!

Other times, it won’t be as obvious, but you’ll notice your network is acting wonky or slower than normal. Or your employees start having trouble logging in. Or there’s a bunch of unrecognized login requests. The point is, suspicious activities are happening, so assume the threat is real…and act quickly to lock down what you can and fix any other vulnerabilities so that the criminals can’t do even more damage.

WHAT should you lock down? Rogers says that you should think about which systems have the greatest impact on your organization’s ability to execute its mission or its key function. If you’re a car manufacturer, maybe it’s a production component. Or maybe it’s data elements you need to produce certain things. Whatever it is, lock it down.

Only once you’ve done all this should you take the time to figure out what you’re dealing with and build a strategy around it. But as you strategize a path forward, be mindful of your communication…because the criminal will probably be paying close attention to your plans.

ROGERS: Remember the adversary very well has a high probability of still being in your network. So what does that mean? So as you are sending emails, as you are using the same network to coordinate with your response, to educate your workforce about, “okay, we're dealing with the cybersecurity incident,” the adversary, in most cases, is actually reading your emails.

PAVIN: That’s right! Which can make a breach feel even more troublesome…because how can you coordinate an effective plan of action with your company…if the enemy is reading all of your emails?

[music]

Rogers says you may have to revert to good old phone calls. Or app-based communication…on a platform like WhatsApp. Or maybe even paper-based communication with couriers and everything. No joke, Rogers has seen this done before. Though it IS extreme.

Essentially, you’re going to have to think outside the box. And that’s the throughline in all of this. Rogers had to do this in 2015…when he realized that hackers that were believed to be associated with the Russian government had penetrated the Department of Defense’s unclassified Pentagon networks.

ROGERS: Sure enough, these things always happen on a Friday.

PAVIN: And he ended up having to take a pretty drastic measure.

ROGERS: And I literally tell the team, “we're going to isolate the Pentagon.”

PAVIN: That meant officials could use the Pentagon’s network structure to talk internally, but not externally…to the rest of the Department of Defense…which, of course, has bases around the world.

But this came with a problem.

ROGERS: I just can't tell the chairman of the Joint Chiefs of Staff and the secretary of defense, “sir, ou're just going to be isolated for a while. It'll take us a few days, but don't worry.” That's not going to work.

PAVIN: So Rogers pivots and decides to create a whole new alternative network structure for some of these most important users. He had that in place by the weekend.

Yes, this is a VERY extreme example of how to troubleshoot communication issues on your feet. But it showcases what Rogers says was the result of planning. Not planning for this exact situation…because things never really happen the way you expect. But the act of planning, itself…and doing those practice simulations we talked about in our previous episode, does serve a valuable purpose here.

ROGERS: Because we had done the planning, I understood the nature of the adversary. I understood the nature of my systems. I understood the capacities that we had. And so as the actual event unfolded, I would be thinking to myself, "you know, when we were planning, remember that capacity we had in the following area? Hey, we could use that for this particular scenario."

[music]

PAVIN: So step one: Act fast and lock down what you can so the problem doesn't get worse. Step two: Be careful how you communicate. And in all of this, you may find yourself leaning on your cyber planning and training to think on your feet…because your adversary will be doing the same.

…

PAVIN: Now, a cyber attack can happen for a number of reasons…sometimes it's to steal identities, or infrastructure…and sometimes hackers hack just because they can. But a growing problem has to do with ransomware attacks. This is where hackers hold your data hostage until you pay them a certain amount to get it back.

If you find yourself facing a ransomware attack, at some point you'll have to decide whether or not to pay this ransom.

ROGERS: My view is, look, the default should not be "well, we're going to pay unless there's some reason not to." the default to me should be, "I will not pay unless there is some compelling, unique reason." And I do see some scenarios where there potentially are some reasonable scenarios in which you might pay.

PAVIN: Under what scenarios…should people maybe pay?

[music]

ROGERS: Oh, for example, if we're talking about disruption as potential life and death impacts. "Hey, I'm a healthcare provider. I'm a vaccine manufacturer in the middle of a pandemic."

PAVIN: So, for Rogers, organizations should pay for only the most serious of reasons. The reasons that he DOESN'T think are worth paying for? Doing it so you can get quicker access to your network…rather than waiting the couple of days it would take to get it under control yourself. He also takes issue with another reason companies give for paying ransom.

ROGERS: I tend not to believe that a valid reason is, “well, we should pay because we need to regain control quickly for reputational purposes.” I do acknowledge many general councils have very legitimate concerns about liability. You know, “hey, look, if by publicly acknowledging this, are we also potentially publicly accepting responsibility? And if we're publicly accepting responsibility, does that imply that if we are sued, we're now assuming liability?” So I understand the concerns, but my view would be look in the long run, we're just incentivizing these actors to engage in more aggressive activities, and I don’t think that’s good for us.

PAVIN: Yes, this is a bigger, macro-level, greater-good kind of way to look at this. Which honestly…may not be enough to convince you, especially if you realize it’s cheaper to just pay the ransom than to be without your network for a stretch of time. But Rogers says that, if more organizations stand their ground, everyone benefits.

And that dovetails into Roger’s final point: You should publicly acknowledge that you’ve been breached. Not only to your employees…who will need to be aware of why they can’t do certain things on your network suddenly…not only to the people within your supply chain…who could be the criminals’ end-target anyway. But you should also tell the federal government…who can actually help.

ROGERS: Within the federal government is an agency…CISA. The Cyber and Infrastructure Security Agency has overall responsibility for ensuring federal government support and responsibility within the cybersecurity arena can potentially help you catch these guys.

PAVIN: Rogers points to a breach that happened last year to Colonial Pipeline — the largest fuel pipeline in the U.S. You might remember it. It led to fuel shortages across the East Coast.

[music]

What happened was…extortionists accessed its data and held it hostage until Colonial paid a ransom. Though Colonial DID pay the ransom, it worked with the government…and the government did something kind of cool.

ROGERS: The federal government used its resources to ensure that a significant portion of the cryptocurrency that Colonial had used to pay the ransom…they actually forestalled the criminal's ability to access the payment. So in essence, you paid the money, but it never got to the criminal. Again, the government was able to do that. That's not something that an individual company is going to do, but that's a unique kind of capability the federal government has.

PAVIN: Beyond leveraging the government’s unique capabilities to beat cybercriminals at their own game…organizations should go public about their breaches because we can then all learn from each other’s mistakes. Right now, says Rogers, organizations are too tight-lipped about security lapses for others to learn from them.

At some point, if this continues, the government might have to intervene, he says, and require some level of transparency, like it did in aviation.

ROGERS: Think about the approach we take with aviation safety when an airplane crashes, or there is an accident: government steps in, we do a mandatory investigation. And at the conclusion of that investigation, we not only identify the source of the accident—"why”— but we then mandate a series of follow-up actions designed to ensure it doesn't happen again. We change aircraft manufacturing. We change aircraft maintenance policies. We change training for flight crews. We mandate changes to the software configurations on airplanes. We don't do any of that in cyber intrusions.

PAVIN: If it were up to Rogers, the government WOULD step in and do all of these things to ensure the

same vulnerabilities don’t keep getting exploited again and again. Only then will cybercriminals have any incentive to change their own behavior.

[music]

To sum it all up here: The way you communicate with both internal and external parties about a data breach…and the speed of your response…can make a huge difference in terms of the damage done. So plan ahead, and use what you’ve learned from those plans to think on your feet when the cybercriminals surprise you.

You’d also be wise to think hard about whether the ransom you pay is worth it…because unless it’s a life-or-death scenario, it’s better that companies keep fighting. Collectively, this will discourage ransom demands, overall. For the same reason, consider acknowledging that you’ve been breached. All of this will help businesses, organizations…and governments…across the country and the world…understand what works and what doesn’t, when it comes to protecting their networks.

[CREDITS]

This episode of The Insightful Leader was produced by Jessica Love, Emily Stone, Fred Schmalz, Maja Kos, and Laura Pavin. It was written by Laura Pavin and mixed by Andrew Meriwether. Special thanks to Mike Rogers. As a reminder, you can find us on iTunes, Google Play, Spotify, or our website. If you like this show, please leave us a review or rating. That helps new listeners find us. And visit us at insight.kellogg.northwestern.edu. We’ll be back in a couple weeks with another episode of The Insightful Leader podcast.