Laura PAVIN: These days, it doesn't feel like there's a lot that people can agree on. But here's one thing.

[News clips] A security breach at LinkedIn turns out to be much bigger than first thought…..the Federal Trade Commission has opened a probe into Equifax's historic data hack ….Marriott just revealing a massive data breach involving a guest reservation database…

[music]

PAVIN: Cyberattacks. They're a problem for organizations…governments…heck, even school districts…everywhere. Big and small.

Globally, some measures show that businesses saw 50 percent more cyberattack attempts per week in 2021…compared to 2020.

It's a problem. So I called up Mike Rogers for advice on how organizations can get a better handle on the situation. He's a cybersecurity expert and senior fellow at Kellogg. He also helps companies manage their cybersecurity woes...but he had this other, past life.

[New York Congresswoman Elise Stefanik] I would like to welcome our witness today, Admiral Mike Rogers who serves as the Commander of U.S. Cyber Command and the Director of the National Security Agency.

Yep, he headed up the NSA and the U.S. Cyber Command, and worked under both the Obama and Trump administrations. And what you just heard was audio from 2017, when Rogers was asked to testify before Congress about the state of cybersecurity in the U.S. and internationally.

[Rogers at hearing] - Hardly a day has gone by during my tenure at Cyber Command that we have not seen at least one significant cybersecurity event occurring somewhere in the world…this has consequences for our military and our nation, at large… [fades out]

PAVIN: So, this is a special episode for us. Or two, I should say. Because there's a lot to discuss around how companies can protect their networks and work through a cyberattack. The stakes are really high.

[music]

In 2020 alone, cybercrime cost both consumers and businesses almost a *trillion dollars*…according to the Center for Strategic and International Studies. That's almost double what it was in 2018.

And here's something you might not have considered. If you lead a small business, your business could be *extra* attractive to cyber criminals. And that's because, on average, small businesses *don't* tend to have the security infrastructure that larger businesses have. But it doesn't have to be that way. Feel intimidated? Don't! Because Rogers says that you *do* have what it takes to make these big cybersecurity decisions.

Mike ROGERS: The amount of times I have heard board members say, 'I don't have an IT background. I don't do cyber.' My attitude is, look, you need to think about cybersecurity through the prism of risk. As a senior, as a decision maker in the path you have taken to become the leader of an organization, to become a member of a board of directors. You have dealt with risk your entire adult business life. And while cyber is specialized and has some particular aspects to, it in the end, my argument is that cyber is just one element of the broader dimensions of risk that, as an organization, we deal with every day.

PAVIN: You, as a leader, should absolutely be helping to make decisions around cyber. So, in our first episode, we'll talk to Rogers about how companies — big and small — can deal with the ubiquitous threat of a cybercrime. Next week, we'll learn what to do when the enemy is already inside the castle.

That's after the break.

…

PAVIN: My first meeting with Rogers was…very on-brand.

[music]

Basically, the building I work at requires this special key to get in. So I told Rogers to call me when he was close so I could let him in. I waited…he was a few minutes late. When I finally got the call, he told me that he had surveyed the building for keyless entry points…and failed. So our building is, in fact, secure.

I did ask him, "why did you do that?"

ROGERS: Telling me what I can and can't do, I never particularly liked.

PAVIN: Said like a guy who used to penetrate foreign networks for a living.

Anyway, when we started talking, Rogers made it pretty clear to me that cybercrime is something that A *ton* of companies are dealing with right now...and have been for some time. Rogers said the COVID-19 pandemic likely made the situation worse. Because something happened in 2020 that made companies pretty vulnerable: Many of their employees started working from home.

ROGERS: And when we're working remotely, we're using the same computer system, the same home router system that our children are using for education…our children are using for gaming….our spouses and partners were using to also work. So that

means that, in the past where most organizations had a well-defined perimeter with a central security stack, and everybody worked within that and we controlled access in and out…now we find ourselves in a world where companies, organizations have had to blow that up, expand the perimeter to include our personal devices at home. So we've had this, what we call “proliferation of end points.”

PAVIN: Think about your workforce’s laptops, their smart printers, their routers. These are all devices that someone, like a cyber criminal, can remotely tap into. And when you’re an organization with people working in dozens or hundreds or thousands of places…sharing wifi and devices with their families…there are a lot more ways for someone to slither their way into your network.

Which leads us to our single most-important piece of advice for guarding yourself against a cyberattack: Keep up your basic cyber hygiene.

ROGERS*:* Strong encryption, good virus protection, strong password-changing policy, not giving administrative-level access to too many people.

PAVIN: All of these tips are pretty basic. I’d be surprised if you hadn’t heard of at least most of them before. But maybe *because* they’re so basic, they’re also easy to ignore or push off for later—and that’s pretty great for cyber criminals. Because here’s what they’re looking for.

[music]

ROGERS*:* You look, basically, for poor construction or poor practices…default passwords like “password,” security openings that quite frankly come when you buy something that were set to default and they never changed them, or their anti-virus is old and it doesn't account for current viruses.

PAVIN: So encrypt your data. Update your virus protection constantly. And make sure everyone is updating their passwords regularly…or you can implement two-step verification.

If you don’t have someone like a chief security officer doing all this for you, you can also buy enterprise-level software that can do a pretty solid job of it.

But let’s linger a bit on the administrative access part that Rogers was talking about.

ROGERS: Administrative access, for example, allows you to grant an individual access to almost every part of your network. Why? Because they have a role where that's required. They're involved in repair, they're involved in maintenance. They’re involved in the operation of the network. And a lot of organizations, quite frankly, give way too much access to way too many people beyond what they really need to do their jobs. So, in many cases—in my experience—well-meaning employees will bypass security in the

name of speed and efficiency, or they will create connectivity, remote access that you are unaware of that helps them in their job, but presents a greater risk.

PAVIN: It's understandable that employees want easy access to every part of the network…particularly during an abrupt shift to remote work.

But at this point, it might be worth reassessing who does and doesn't actually need administrative access. Because it gives criminals more possible doors to enter your network…and to swim upstream from there.

ROGERS: Think about supply chain. Think about suppliers. For example, we used to watch nation states in my previous life go after law firms. And we kept thinking, "what makes law firms so attractive?" I can remember my general counsel, who I had hired from the outside says to me, "well, a lot of organizations use outside counsel to do their intellectual property, or think about patents, trademark with the government. So quite frankly, to do that, the company provides the law firm the intellectual property associated with the patent or the trademark or the copyright." I'm going, "oh, that's why these are so attractive. If you can't get into the company itself? Yeah, find out who else has access to their data."

[music]

PAVIN: Yeah, everyone that you work with, contract with…and share some kind of sensitive data with…is a possible target for a criminal…and if and when that criminal does breach that other entity's network? Well, you could very well be a victim too. Or maybe you were the intended target to begin with.

…

PAVIN: Listen, all of these steps…like requiring more password changes and tighter controls around administrative access…are probably going to be annoying for your employees. And you're going to have think carefully about how to get them on board.

ROGERS: I've said this to a president one time, you know, "sir, we can have the greatest technology in the world. We can have the greatest investment in cybersecurity in the world. But if we have a user community that doesn't understand what we're doing, that makes poor choices, that engages in poor security practices…it undermines everything we're doing." So, I urge every organization out there, never forget that. As you're creating this cybersecurity strategy, educate and train your workforce. Why are we asking you to do this? Help them understand, "hey, here's what happens when you don't do this."

PAVIN: Make it too hard for people to do something basic at work, and they're going to find ways around it. So help them understand *why* these measures are in place. But if you REALLY want your employees' buy-in, consider making compliance more…enticing.

ROGERS: ***We have got to incentivize and reward positive behavior. So, for example, most organizations today are routinely doing tests of employees for spear phishing.***

[music]

PAVIN: Spear phishing is when you get an email from an address that looks like it's from someone you know…and they try to get you to click a link or reveal sensitive information. Your IT department might send out emails that look like this to test you…with the idea of training the behavior out of you.

ROGERS: ***And in many cases, when the individual clicks on the link, they get a nasty note from IT. I said, for example, "when they don't click on the link, why aren't we, for example, recognizing them? Putting out a nice email that says, "hey, the following 10 employees did perfect on the last update test for software that we did." "Hey, we're going to do a drawing this week, and out of the 100 people that we did a spear phishing test with, we're going to do two gift cards for a restaurant or some service."***

PAVIN: I mean, it certainly makes me feel more motivated! And think about it this way, what's spent on a gift card is a drop in the bucket compared to the expense of a breach.

[music]

To recap, good cyber hygiene isn't rocket science. But it can do a *lot* to fend off a cyber attack. So make an effort, today, to get on top of things. Just make sure that what you're asking your employees to do isn't overly onerous, because if you don't have their buy-in, you're going to have trouble protecting your network from a breach. And if onerous is the way it has to be, explain *why* that's the case–and consider dangling a carrot or two.

…

PAVIN: But is all of this *really* enough to keep the cyber criminals out? Rogers says there are a couple of things you can do to find out. One is called "red teaming."

ROGERS: You pretend you're an outside entity, you're a criminal or a nation state, and you actually try to attack your own network. And they call it red teaming. Some organizations do this themselves. Larger ones, sometimes, will do it themselves.

PAVIN: Pretend you're the enemy. And do as the enemies do. If you fall into the small business camp, and you just don't have the resources to do this yourself, you can hire someone to do this for you. And if you want to get even more granular on where your network defenses stand? That's where a second option comes in. Get yourself graded.

ROGERS: There's a market out there where several companies are involved in remotely grading or assessing networks. And they'll actually provide a written product that says, “hey, here's a letter grade or a numerical grade, one to one hundred. We'll also, for example, tell you how that relates to companies your size. We'll tell you how that relates to the average in your industry or business sector.” So there are entities out there—business entities—that are doing this as a way to make money.

PAVIN: You might, at this point, be thinking to yourself, “all these cybersecurity measures…this is gonna cost me some dough.” And sure, none of this comes cheap. But, again, it’s almost certain to be cheaper than what a criminal will demand you pay once they’re holding your data hostage. And if you think you *won’t* pay, the odds are that you will, according to Rogers.

ROGERS: Probably 60-to-70 percent of the entities that have to deal with this end up paying. And that's a little better than it was. If you go back two years ago, I would've said the number was closer to 80-to-90 percent were paying. Most companies don't want to disclose this. Most governments don't want to disclose it.

PAVIN: And that’s why Rogers wants you to consider this: In the event of a breach, you should tell the world that it happened.

[music]

But we’ll get to that in the next episode…*and* we’ll get a real boots-on-the-ground account from Rogers…about his first-hand experience with breaches.

ROGERS: I have had networks penetrated and, um, that's never a pleasant conversation in the white house situation room. “Yes, Mr. President, this really happened.”

PAVIN: Join us next week for part two of our conversation with Rogers.

[CREDITS]

PAVIN: 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 next week with part two of our cybersecurity series.