Martin Hinton (00:03)

Hi, and welcome to the next episode of the

Insurance News and Information Podcast.

your host and the executive editor of Cyber Insurance News, Martin Hinton. And today we're joined by William Altman, who is the head of cyber threat intelligence at CyberCube. Now, what does all that mean? I guess I could tell you what Williams told me, but the best thing to do is just get right to the expert himself. And William, first, thanks so much for joining us. Please tell us a little about what it is you do, what CyberCube does, and how you came to this moment in your career.

William Altman (00:32)

Yeah, thank you, Martin. Really appreciate you having me here today and sharing your audience with me. I hope I can share some insightful information about cybersecurity and cyber insurance. hopefully there's a lot of follow-up. And if folks have questions, they can always get in touch with you or me. Really looking forward to engaging with the audience today. Myself, I have a background in cybersecurity.

have worked for CyberCube now for five years. So I don't know if I can say I don't come from the insurance industry anymore, but I don't have a background working for an insurance company. I've worked for Fortune 500 companies, for CISOs at those companies. I've also worked as a contractor for the US government for a period of time and really built my cybersecurity expertise doing a mix of hands-on work and certifications and coursework. And then also,

here at CyberCube on the job, working on the different products and data sets that we have that really helped me understand what's happening out there in the world of cybersecurity, cyber defense and threats that we can really make sense of using our products and services. So that's a little bit about me and how I got here. CyberCube itself is the world's leading analytics provider for cyber insurance around, you know,

how you can price the risk from both a single loss perspective on one company to assessing risk and exposure across thousands of businesses in a portfolio. We have solutions for brokers, for underwriters, for reinsurers and cap modelers. We're increasingly applying our services to critical infrastructure organizations and the public sector. And we not only are in this to really build the...

bottom line of our own business and help our clients succeed. But we have a social mission here at CyberCube. We're in it to help improve the resilience of organizations and society by realigning insurance incentives and helping companies protect themselves and get the insurance they need to cover losses when they do get attacked. So it's a little bit about CyberCube and also why I'm here and what motivates me to do this work. And looking forward to talking with you today about some of the recent work we've done around

small businesses and the cyber insurance protection gap in that space. But really love talking to folks about cybersecurity and

topics related to cybersecurity and threat intelligence.

Martin Hinton (02:54)

done. Your transition is great because one of the

Martin Hinton AI (02:56)

Well done, your transition is great because on of the...

Martin Hinton (02:59)

last

that we worked on here at Cyber Insurance was about your global threat briefing, which is one of the reports that you guys put out. it covered specifically the element that was interesting to me was the small business part. So I'm just going to look at a few of my notes

here and tell you a few things. If I get any of these numbers wrong, because we know how numbers and statistics work, you let me know. But.

You just touched on it, the protection gap for small businesses. And I've said recently to a few people, there's a bit of a mindset I've encountered where it's a bit of the teenager mentality. Like, it won't happen to me, it won't happen to me. And the statistics in this report that you guys put out, they betray that feeling. 75 % of ransomware cases targeted businesses with 11 to 1,000 employees. And small businesses often lack the robust cybersecurity measures.

So I guess I'm wondering, what is it about small businesses that makes them attractive targets to cyber criminals?

William Altman (03:54)

Yeah, this is a great question. think small businesses oftentimes don't perceive themselves as targets. Once upon a time, this might have been true. It's certainly not the case today. When I say small business, I'm actually referring to a revenue band of $10 million a year to $250 million a year.

So you start to think there's quite a difference between those companies at either end of the spectrum. And certainly a company making $250 million a year in recurring revenue is going to be a cyber target. And so I think we have to define that revenue band to really understand what we're talking about. And once we do, it's pretty clear that threat actors would like to go after companies that make this amount of money. Now, these companies oftentimes have thinner margins than say companies

that medium size or large, so over 250 million in year in revenue or over a billion. Smaller companies just don't spend as much on cybersecurity. They just can't, their margins are thinner. And so they have to make budget cuts and prioritize things and...

look at where they can cut to make operational efficiencies. And this tends to amount to a cybersecurity program that works, but is not impenetrable. No cybersecurity program is,

but those that under invest are obviously a little bit more risky. so threat actors know this. They look to small businesses for low-hanging fruit, kind of an easier payday because they can find misconfigurations, software vulnerabilities, end-of-life products.

all these things deployed on the public internet that are easily findable and accessible. Today, there's no secret that artificial intelligence is changing the game for both attackers and defenders. know, while I don't think 2025 is the year that AI really significantly changes the calculus between threat actors and defenders, you know, we're not likely to see threat actors use AI in a way that puts defenders on the back.

foot for a significant period of time this year. We are likely to see threat actors gain some efficiency using AI, specifically the threat actor class that targets small businesses are going to be able to more easily find these businesses and their assets and their credentials and their login portals online using AI. And they're also going to be able to break in and bypass those login portals and MFA solutions using things, pardon the

the technical terms, things like credential stuffing or brute forcing you might hear, know, use this is using AI to break into a login portal by either trying previously leaked credentials that could be reused or creating whole new email and password combos to break in. These are the types of things that threat actors are doing today that will impact small businesses going forward.

So we do think that there's a reason to be concerned if you are a small business.

Martin Hinton (06:46)

You touched on the AI part

of

you just said there for a second, because there's a bigger topic there about how real the threat is now and how quickly technology will make that a bigger threat. You touched on the

financial realities that a lot of small businesses have. If you're a small business owner now listening to this, what's something that you might do in the short term to make yourself more secure against these kinds of vulnerabilities or less vulnerable to these kinds of threats, I should say?

you can always buy something, right? We're always adding to make things better. Is there anything that you can do that is within the domain of a company that might have 15 or 20 employees? And I'm thinking about very basic things like, you know, having, again, there's a lot of resources that are free, multi-factor authentication or, you know, updating software. What are some things that you can do that maybe they're doing already, but they just need to dial up

the sort of...

idea that for them and their employees that these things matter and they are akin to we turn the lights off when we leave the office, we lock the door, we don't leave the fireplace on, know, the basic things you do to protect your business.

William Altman (07:54)

Yeah, this is a great question, Martin. I'm glad you asked it. Really gets to the heart of how to take action given the threats that we've talked about. So if I'm a small business today, you nailed it. It's MFA. I really think multi-factor authentication is going to impose enough cost on a threat actor that if they are faced with the

Option to choose a company that has MFA and one that doesn't it will go with the one that doesn't every time So you are making yourself a less attractive target right off the bat by having MFA solutions deployed Especially on key resources if you have any remote access tools an RDP port open or if you have any virtual private network resources that you're using MFA should be used on these login portals

If you are administering some part of your own network, whoever that local administrator is on that network should also be challenged with proper MFA challenges at the right times.

This is not going to prevent every single cyber attack. Threat actors are increasingly capable of bypassing MFA solutions. We saw this in 2023, I think it was September when MGM was breached by the group Scattered Spider.

They were able to use social engineering to trick call center employees into resetting MFA credentials. So not even exploiting the technology itself, but rather the processes around the technology. So MFA is not a foolproof solution, but it is really one of the best defenses we have today, especially for small companies where even the small things matter greatly because threat actors again are looking.

for those

hanging fruit.

Martin Hinton (09:34)

I was going to say,

William Altman (09:35)

So MFA, really big deal.

Martin Hinton (09:35)

I mean, what you talk about

And the bad guy will go to the easier target, right? And again, you hear this in homes, right? Is there an alarm sign in the front yard of one house and not the other? Like a very basic message to be said, listen, it's going to take you slightly longer. And we know time creates great vulnerability. If it takes you longer to break in.

William Altman (09:45)

Right.

Martin Hinton (09:58)

It's a more complex process, then there's more likelihood that you'll be discovered in the process or the breaking will be alert alert, you know, the right quote unquote authorities. Is that something to sort of, you know, to put it in terms like and I, I asked companies are doing this already. They're already thinking about particularly if you're a physical place, like a warehouse where you store goods, right? You're doing a lot of this already. And the important thing is to take this idea and place it into a digital sphere. So a lock on a door.

The second lock is MFA, right? That's the idea. If there's two locks to break, then it's twice as many locks to break on a physical door. And MFA for digital environments is similar in that sense. Is that a fair way to put it? I don't want to make it too simple.

William Altman (10:43)

It is. Yeah, it is. Yeah. I love the comparison to physical security in this context. It absolutely works. I think MFA is just one more lock that you can put in place that threat actors have to spend time, as you said, breaking into. And they will go to lower hanging fruit, especially for small businesses. When it comes to large organizations, just because they have MFA in place doesn't mean a threat actor won't spend the time and energy to bypass it because the

potential payday at the end of that crime is much larger and potentially pays off. Whereas a small business, know, they really have to make that economic calculation between time and money. So you're trying to impose those costs as a small business on these threat actors, make it so they would take more time to breach organization. MFA is a great way to do that. I think the second biggest thing you can do today is to understand your identity and access management infrastructure and exposure.

to really make sure that because we're working in these remote work first world and we're looking at perimeter lists networks for the most part, we need to know who's entering and exiting the network. The same thing would be true of your warehouse. Just as you're putting

the lock there, you also want some record of who's coming and going. in our digital sense, this is management of login credentials, making sure people have.

access to the right data at the right time when they need it, no more, no less. This is called privileged access management. These are the types of things that can be done to also greatly reduce threat actors capabilities today, especially when it comes to using credentials that are breached in past attacks. Just asking your employees and mandating that they reset credentials and don't reuse passwords for work on the same accounts they use for shopping, for example.

You know, that ensures that one breach doesn't potentially create a vulnerability in your company infrastructure. So these types of credential and

management ~ procedures are really important today. I think the third one.

Martin Hinton (12:41)

Is this in the realm of like a zero trust kind of environment where you have to prove you're supposed

to be there?

William Altman (12:49)

very similar, very similar. That Yeah, very similar concept. I think zero trust is probably more applicable to a medium or large size organization where there's layered parts of the network that are segmented and no one gets to go anywhere without proving who they are. There's an element to that. For small businesses, though it may not be as expansive, you your small businesses today, like you said, it could be 15 people that log into

Google and Amazon and Microsoft resources in order to collaborate. I still think rotating those credentials is very important and having that identity management space be secure

is important because you may not have threat actors break into a core software build environment, but they might break into your email.

your

Martin Hinton (13:35)

Yeah.

William Altman (13:35)

people to wire money places. And this happens all the time.

Martin Hinton (13:35)

Yeah. So you, I mean, again, the idea

we're talking about is

if you've got a warehouse with electronics in it and you've got an office building down the road where the sale distribution and management of the movement of that product is to people who buy it and the delivery of it from who the supplier you get it from. your, I don't know what your accountant, in-house accountant is in the warehouse every Friday night from 10 to midnight.

That would be an alarm bell. So that's why you're there. What are you

in this space? Again, in the digital environment, it's a similar scenario where, you know, if someone who's involved in bookkeeping is reading contracts for that aren't signed yet, or in the legal part of

if you will, digital world of the office, that's a red flag. And the simplest thing to do is to restrict that access. And if there's some reason that comes along that someone might need that access, they have a privilege that's a temporary privilege, right? That doesn't...

this vulnerability that drags on and on and on like the one for all the people who get to live in that space regularly? that a sim... is that any kind of remotely good way to put it?

William Altman (14:40)

Yeah, absolutely. That checks out. I would agree. It's a good way to simplify it and kind of make it an accessible idea. The third thing that companies can do is, as you've also pointed out, software vulnerability patching and management of software vulnerabilities. I think we're likely to see this year that threat actors do less software vulnerability exploitation, especially against smaller organizations, because they can more easily breach those groups through

leaked credentials and using artificial intelligence to do so at scale. Software vulnerability exploitation tends to be really specialized. You have to be a software engineer for the most part. There's just fewer people who can do that. And so I think that is an attack vector will always be important. Companies should be patching software as often as possible.

the number one attack vector facing small businesses in 2025. I think we're far more likely to see.

Martin Hinton (15:27)

Do you think that's a reflection of the fact that, if you will, what it takes to be a cyber criminal has been democratized

William Altman (15:34)

Absolutely, Martin. That's exactly what we're saying. Yeah. It's easier to conduct a credential stuffing or brute force attack on a small businesses login portal for its VPN

connection that it is to identify the VPN solution, figure out there's a software vulnerability there and exploit the vulnerability if you will.

Martin Hinton (15:50)

Yeah. All right, so I want to move on. Sorry, pardon me. Go ahead. No, no. OK,

William Altman (15:56)

please. No, I know you're.

Martin Hinton (15:55)

the next bit I wanted to talk about from

report is one that we've done some work on. And I did an op-ed piece that I think I shared, but it doesn't matter if I did. But the premise I raised in this piece was that when we look at critical infrastructure, we think about it's a pretty broad spectrum. I don't know if it's like 12 or 16 or so industries that fall into that category.

But education isn't one of them. And in the thinking in my mind, as minor as it is, the K-12 environment, because of the role it plays, if you will, in taking care of not just the next generation of employees and educating them, but also making them safe and secure while the current generation of employees goes off to work. And when schools shut down or they're the subject of a cyber attack, there can be a significant data loss because they carry a lot of sensitive data.

but they're also incredibly vulnerable as a function of the same sort of thing that small businesses are underfunding. And I just wonder whether or not you could touch on that a little bit for me and where you see that as a part of the concern in this space.

William Altman (16:57)

Absolutely. Well, let's just start by recognizing that education is one of the most attacked sectors around the world.

They kind of check all those boxes that your threat actors that are financially motivated are looking for today. You've got an industry that holds a tremendous amount of sensitive and highly regulated data, especially when it comes to schools that are holding data on minors. It's a whole separate package of regulations there. So those organizations are often willing to pay to get that data back. We also have organizations that are operating on thin margins, as you pointed out, schools.

They oftentimes under invest in cybersecurity or treat it just like it's normal IT work. so, you the IT guys got it. That doesn't cut it anymore. And they can also not afford downtime.

This is an interesting angle for education because it's not like manufacturing where manufacturing also can't afford downtime. If you shut down the line, every second something's not coming off the line, they're losing money. That's not the case for education. So it creates an interesting dynamic for insurance companies because when the school shuts down, they're probably still receiving tuition money.

that doesn't end the tuition payments that they've got. So there's not a lot of lost revenue associated with the downtime, but there's a tremendous impact on society and on communities that I think insurance companies ought to recognize and still factor in. Maybe not in terms of payout, but at least understand that this is happening. When schools go down, students can't get care that they need. They don't get meals. There's no childcare.

As you pointed out, it has an impact on parents as well.

These schools oftentimes want to get back up and running, even though there's no revenue loss. They need to get back up and running. So they're oftentimes willing to pay. So that combination of sensitive data, limited cybersecurity budgets, and low tolerance for downtime place education squarely in the crosshairs of threat actors today. We see attacks

all over the world, all the time on education. There's a little bit of a reporting bias because schools especially have to announce that they've been

Martin Hinton (18:56)

You, you.

William Altman (19:10)

attacked, they have to tell people and they put it on their website and they tell parents and stuff. So we hear about it. So it's a little bit of a reporting bias, but you know, if you visit a website called the cone briefing, KON, and you can just see a list of recurring attacks that happen in different sectors, it's astounding how many education firms get attacked today.

Martin Hinton (19:27)

You touched on this, there's a bias

to, that's one of the issues in the space, isn't there, the reporting element at all. An article I read recently was about how there was a report out of the UK about banks under reporting cyber events. And all I thought was, that struck me as startling and it was fairly well, mean, it was a research report, so it wasn't speculation or groundbreaking journalism, this has happened.

That idea that we, it's like, is it called frequency syndrome? When you see something a lot, you think that's where it always happens. That is the phenomenon of education. You touched on this with education though. And this is a concept again, like I think with small businesses and maybe parents at home, they're like, why would anyone want to hack the school? You said the word sensitive data. And I think what people, at least as I understand it, when you get to the university level, when you say sensitive data, you mean some of the...

William Altman (19:55)

Mm-hmm.

Martin Hinton (20:20)

groundbreaking tech that's being developed on at the highest level of education in the world. Stuff that's going to be in the next this or that that's going to make a billion dollar company. That's what we're talking about,

William Altman (20:30)

I think it's both. think your high-end research institutions, Stanford, MIT, they're certainly doing cutting-edge government research there that governments around the world would love to get their hands on. Some of the first cybersecurity programs were developed at universities that were trying to secure intellectual property. For a long time, that was the forefront of the battleground.

was how do we protect university IP? Those days are long gone. Now you have a lot wider of a threat landscape, but that's certainly a factor for those big research institutions. They want to protect their intellectual property. I think those threat actors that are trying to steal that IP tend not to be financially motivated in the true sense. They're geopolitically motivated. They're ideologically motivated, tend to be aligned with governments.

The financially motivated threat actors are in it for extortion. And they're going to use data on students and faculty to achieve their aims. And this could occur at high-end research institutions. It could occur in liberal arts colleges, vocational schools, K through 12, anywhere where there's sensitive data. And the truth is the most sensitive data is K through 12, minors data.

We saw this actually earlier this year when there was a breach on a company called Power School. Power School is a student information system management platform. It's holding everything from mental health records to medication procedures, lots of sensitive stuff that stays with a child their whole life. You can't change that like a credit card number. And so this is very valuable for threat actors.

today in terms of extorting schools and extorting Power School itself, but then also a long tail of fraud and abuse is likely to occur on the students and faculty who had their information missing. Just for context, Power Schools is a technology that we classify as a single point of failure. They hold information on 18,000 institutions globally. When the threat actors made out with data in this attack,

they still date on 60 million students around the world. So we're looking here at just the start of something where threat actors have realized that there are these clearing houses of data and education that

a lot of institutions vulnerable to their extortion tactics.

Martin Hinton (22:53)

You touched on it, you used the phrase that, you know, because sometimes it's

But you used the phrase, the

tail. And one of the things that I've been talking to a few people lately about is this idea that once the data is in the world, your secret's out, if you will.

And I don't like that phrase because it makes it sound like this shouldn't be private. It's not a secret. It's isn't like, you know, something you don't want the world to know about you because it's a bad thing. This is just private data. sometimes the language I think portrays what we're talking about. But you said long tail, the idea that if, you know, 60 million student records in the case of power school are out there in the world, they are going to be the same forever. The information about these people is going to be the same as it is now forever. It's their history in some respects.

And the length of time that that could be used to monetize, if you will, cybercrime is significant. Do you think that's something that is talked about enough? the long term, you

the idea that 20 years later you might have something pop up that becomes an issue for you? Is that what we're talking about? Is that a realistic way to think about it?

William Altman (23:52)

It is. Yeah, absolutely. think this data will live in leaked databases forever. May not be immediately usable, but if threat actors are trying to compromise you as an individual later on in life or fraud or some kind of other abuse, they will certainly have access to leaked databases. Perhaps they'll have the leaked database that shows that you needed mental health counseling when you were in ninth grade, you know?

And that's in that power school breach for a lot of people. So I just feel like it is talked about, but it's probably not addressed enough. Today, we pretty much just say the organization responsible has to pay for credit card and fraud monitoring in perpetuity for these individuals. So we cover the financial angle, but we oftentimes don't cover other types of abuse that could result from this

Certainly we're not nowhere on this, but there's some progress to be made.

Martin Hinton (24:45)

All right, well, we're to move on. We're going to touch on now

next element of the report that I want to mention is the financial sector. it's probably because they've got the money, a bit of a mixed bag. And one of the statistics out of it was that 65 % of small financial institutions have above average security and 35 % remain highly vulnerable, is the phrase I've got in front of me. Is that an accurate characterization? And what puts them in a class of being more resilient to these cyber threats?

William Altman (25:13)

Yeah, absolutely. So what we're doing is we're looking at security in organizations that are considered small financials. So 10 million to 250 million in revenue across the world. We looked at a portfolio of 10,000 small financials across the world and we looked at them for

their security and their exposure metrics. These are two different scores that are offered by CyberCube to help summarize a company's cyber risk posture.

What we found was that the majority of small financials in this portfolio are above average security, but 35 % of them are below average security. That's not an insignificant number. So what does that mean? It means that underwriters approaching this space have to do so with great care and appreciation for the nuance of writing financials. And that that's what's necessary for really being able to identify those highly secure

entities in the financial services industry. There's a number of things that firms that are high security do well, that firms that are low security don't do well. I think one of the big ones that we saw was actually the implementation of multi-factor authentication. CyberCube can see from the outside looking in whether or not a company is using multi-factor authentication technology. And so we found that highly secure financial institutions use it, those that are less secure don't.

Martin Hinton (26:38)

So the

insurance part of this, there is the ability to really customize coverage for the particular risks that exist, right? The question I have is what's the interconnectivity of these organizations like and how does that, because obviously they have a lot of information flowing in and out of themselves. Is that something that a cyber criminal will see and it becomes a nice target?

William Altman (27:00)

Absolutely. We know that even secure entities in financials, education, any industry really, but we'll look at financials. Even the most secure organizations are still at risk of losses due to sector wide reliance on common technology and cyber events that would impact those common technologies. So when I looked at common technologies used by small financials globally, we saw that Bloomberg was highly used, heavily leveraged.

This is not very surprising anyone in financials probably logs into a Bloomberg terminal every day for something I'd originally thought this was just for Looking at some data and maybe chatting with other traders. It turns out it's a regulated platform that there is a lot of transactional information flowing through and if it goes down There's no easy replacement. So all of the activity and transactions flowing through the terminal cease to a halt

And so that could greatly impact a lot of small and medium and even large sized financial institutions that use the Bloomberg terminal. We found other ones like Factset, FIS Global, and a number of other technologies that create that common single point of failure across financials. We did the same analysis for education.

Martin Hinton (28:14)

You

touch on the... I don't wanna take too much time off your time, but so I wanna move on now and come back to what we touched on a little bit is, and it's everywhere. And I read probably like you more than a few reports on cybersecurity and various sectors and domains and all that sort of thing. And the hero and the villain.

Right? There's a comic book coming, right? And it's artificial intelligence or AI. The idea that it is this, and the analogy I think I've used in the past is it's the car. It can be used by a bank robber to get away or the police officer to chase. And whether or not one's more effective than the other depends on way more than the car's quality. So I wonder whether you might just dive into that topic now of AI and maybe start with an example, because I think a lot of people

While I use it a lot, a lot of people don't quite appreciate how it can do things like make you more efficient. So what's an example of how AI is currently being used to commit these kinds of crimes?

William Altman (29:18)

Yeah, I mean, you're right. It's being used on both the attacker side and the defender side today. I think that's partly why we're not likely to see attackers use it in a way that puts defenders on the back foot in a significant way this year. There's still a balance and an ebb and flow to the advancement and the use cases for this stuff. When it comes to threat actors using AI, I think today I'm mostly looking at the

reconnaissance and target selection stages, the delivery stage as well of the kill chain, meaning threat actors are more easily able to find the right credentials, login portals and companies to target. And then they can rank those companies based on the probability of success for an attack using artificial intelligence that recon and target selection phase is getting a lot easier for them.

Just the ability to collect and synthesize tons of data is now easier with a large language model. So you can sift through tons of employee records, leaked data, LinkedIn profiles to kind of find those targets that you want to go after. And you can do it in a more automated way.

Next is the delivery phase. You've got to get some kind of payload into your target's network in order to do some damage. So this is often done through phishing, email-based phishing being really popular. You try to get your victims to click on a link or download some attachment. This is a primary way threat actors break into a network today. Phishing the right employee and getting their password can be just as good as exploiting the right software vulnerability.

So today we're seeing artificial intelligence enable threat actors to spin up real world, lifelike fishing lures in real time. So things that are directly targeted at Martin Hinton and your lifestyle and the things you like and everything from your social media accounts. And it's all put together in a nice email and sent to you at the time, which will generate the most potential urgency or when you're most distracted, you know, this is

This isn't happening today at scale at that level, but we're getting there. We're starting to see that threat actors used to send out phishing lures to get people to click on emails. They

would A-B test, just like marketers. And then whoever was clicking on the email they liked, they would alter the campaign to be more like that email. It used to take...

days for threat actors to alter these campaigns. And that was a long enough period of time for defenders to respond. Today, threat actors can use AI to alter and spin up new campaigns on the fly way faster than defenders can share intelligence and stop those things. So we're kind of at a point where the defenders that are using cutting edge technologies like abnormal, proof point, mimecast, and can afford that stuff

can still catch these phishing lures. Those who are not able to afford those technologies are likely to get caught in the crosshairs. So that's a big one we're following today is just how is AI supercharging social engineering? You've probably heard about deep fakes, these fake videos that can be spun up with AI. There's already been evidence of a CFO sending millions of dollars to a fake CEO, deep fake fraud. So this is still in early days, but it's coming. Yeah.

And then I mentioned credential stuffing and brute forcing earlier, two techniques that are also being enabled by AI today.

Martin Hinton (32:51)

Now, one of the things that I come back to all the time

is

But you touched on the way you put it earlier, the efficiency it creates with the pace with which the product being delivered to fish with, if you will, is altered faster. And I can't help but think, you know, we started with a car analogy. There's almost an assembly line process that's been created here where the...

the efficiency and the speed with which you can create the end product and even change it by changing an element of the assembly line and retooling one part of it to make the wheel

hub different or whatever it might be. This is where we are with this. the pace with which this is going to change is one of the big challenges for people on the Defender side, right? This tool is now, because it's open source in most respects, is available to everyone to use as they like. So I guess...

you know, a hammer can drive a nail home and misused it could break your thumb. Is that something that, you know, we need to keep the audience and people and small business owners and corporate executives and really everybody in the mindset that this is, there's no quick fix to this. There's going to be what works today. And then like you keep using the phrase this year, this year, meaning that what we see now is perishable. It will change. And we need to be.

consistently on guard for the latest trick, the latest tool. Is that the mindset that as burdensome as it might be, people need to take on individually and then also leaders need to present to the staff and the workforce within their control.

William Altman (34:24)

Yes, but I want to caveat this idea that the threat landscape is so dynamic and shifting and that I think we do need to see things in quarters even, or maybe even in smaller increments of time. It is a shifting landscape, but the truth is threat actors have been good at attacking companies successfully for years without artificial intelligence. AI is coming to make them more efficient.

and it's going to help initially a very specific subset of threat actors that are going after smaller targets for smaller ransoms. So I don't think we're going to meaningfully see AI really change the threat landscape very soon because it's already so bad and threat actors frankly don't need it. I think in time we'll see that it expands that specific threat actor class and we could see...

more attritional and large losses, especially in the insurance ecosystem as a result, I would say in the next five to 10 years. There is also the possibility that the technology will brought to all expectations and we end up with what's called artificial general intelligence much

sooner than we think. And that is a truly unpredictable environment. So to kind of pick up on your thread, Martin.

the audience should be aware of artificial intelligence advancements and the fact that it's an unpredictable space. So while we're doing our best to understand future outcomes, we have to also develop our tolerance, our resilience, and our resoluteness for ambiguity around future impacts of artificial intelligence, as uncomfortable as that might be.

Martin Hinton (36:01)

Yeah, listen, I again, I think that one of the

things as we move to wrapping up, I wonder whether or not, because this report's global, there are parts of the world or regions of, say, America or parts of Europe.

that are doing better than some others and others that aren't doing as well and what you attribute that to as we sit here today.

William Altman (36:21)

You know, it's difficult to throw a blanket over large swaths of the world and say they're more secure than others. Like that is a difficult exercise. There's data within cyber cubes, global insurance exposure databases that can help us prove out these different thesis. But just sort of speaking off the cuff, I'll say in my experience, more heavily regulated places tend to have more secure companies.

Places like New York, California, where a lot of the financial or data regulations were developed, they tend to have more secure organizations that work there, say, have to stay compliant. That also goes for different industries. tend to see banking, energy utilities, these types of heavily regulated sectors tend to be more secure than, say, like retail.

construction that haven't had as much digital regulation imposed on them in the past. So fairly.

Martin Hinton (37:16)

And there could be a bit of a misconception that could be created there because a lot of those

So then there's information for a journalist to put on the television or in a newspaper. And that makes you think, it's always them. It's always them. When in fact, there are lots of places that don't have that obligation because the regulations don't exist. I go back to data sets and creating risk analysis. that

William Altman (37:30)

you

Martin Hinton (37:37)

you think is a fair way to put it?

William Altman (37:38)

Absolutely.

I think it's absolutely a fair way to put it. It's a challenge that cybersecurity professionals, journalists in this space have faced for a long time, which is this reporting bias, the lack of accurate data about how many attacks actually occur, when they occur and on whom. We do the best with the data we have knowing it's still an incomplete picture and the number of attacks is much higher than what's actually reported.

Martin Hinton (38:01)

So bringing it back around to the beginning, I want to

The small business owner out there, right? They hear about MGM, they hear about change, they hear about colonial pipeline. Maybe if they're reading European press, they hear about the NHS and they see North Korea this and Russia that and China in the phone system. That all sounds like it's not their problem.

And the truth is, it is potentially their problem. I just want you to touch on again, of the perspective, setting aside the financial threshold you might have to meet to find exactly what you should for today's dilemma. What are the small business owners should they do? We talked about multi-factor authentication. Run me through a couple of things as we wrap up that small business owners should double check, ask themselves. Maybe they don't know.

William Altman (38:47)

Yeah, it's a great, great way to wrap up. I think it has to be said that a lot of small businesses are relying on managed service providers and

security service providers for a lot of the things we're talking about. So if I go to a small business owner and I say put MFA in place on all your systems, they're like, okay, but we rely on an MSP for all of our network and security. So I actually just have to go talk to them. It creates a challenge for an insurance company to really know the true security of an

I think small businesses can reexamine those relationships with their managed service providers to ensure that those managed service providers are not single points of failure leading to extortion at many organizations. We know from past history specifically an attack on a group, I think it was called

I think this was, was this Kaseya VSA attack where threat actors broke into an MSP and they were attempting to ransom and extort the MSP because they'd locked up all the clients data. So they're still only staging that extortion on the MSP provider.

the ransoms paid by the MSP, but the impact occurs on all the customers environments in their data, because they then put pressure on that MSP to pay up. So we know that threat actors are interested in this type of an attack vector. So it creates an issue for some small businesses that may otherwise think that outsourcing to an MSP is just foolproof. It's not. So think re-examining those relationships, ensuring that the MSP has a

downtime and disaster recovery plan that you're a part of is going to be really important going forward. would say that's my number one advice other than looking at those baseline kind of bedrock cybersecurity measures. If you need a reminder on what those are, I would just go back to the NIST cybersecurity framework and look at the key controls for identifying, detecting, protecting, responding, and recovering from cyber attacks.

and see if you're in line with those, the checklist. not, contact an MSP, some kind of outsourced solution that can help you. If you're interested in how this might affect your insurance policy and you're small business, get in touch with CyberCube. We'd love to hear from

Martin Hinton (41:03)

Outstanding. You touched on the NIST. There

are a lot of public resources out there that are, you know, what you could put simply as a checklist that you could run down as a business owner and say, I don't have three of these or two of these and that sort of thing, at least to give yourself a sense of the environment you're in now. And then you have some ability to go that someone like CyberCube can ask questions about things. Is that a way to put it?

William Altman (41:27)

Absolutely. Yeah. I would recommend the NIST framework, the CIS controls. You could also look at things like the ISO certifications and whether or not you align with those. These are common frameworks and regulations that organizations have to comply with to prove they're secure. So think starting there is going to help you from both a security perspective, but also a commercial perspective.

Martin Hinton (41:50)

We'll put links to all those spots in the show notes. So if you're watching

and

So as we wrap up, William, is there anything that we haven't covered or you'd like to go over again, anything I didn't ask or anything you thought we were going to talk about that we didn't touch on that you want to bring up?

William Altman (42:04)

I think I'll just reiterate that when it comes to threats facing small businesses this year, we're encouraging small businesses to also re-examine those virtual private network connections, remote desktop protocol, remote access connections. It's something we explored in the report and just wanted to make sure that small businesses were aware that that's one of your primary initial attack vectors this year, given what we've seen from threat actors so far.

Be on the lookout, stay vigilant, and good luck.

Martin Hinton (42:32)

Good luck, I love it. William Altman, Head

of Threat Intelligence Services at CyberCube. Thank you so much for your time. It was really, really interesting. if you're watching and you've got a question, like William said at the beginning, put it in the comments. We'll get back to you. And if I don't know the answer, which is a high likelihood of if it's got anything technical to say, I'll touch base with William and we'll do our best to get you a reliable answer.

William Altman (42:45)

Thank you, Gordon.

Martin Hinton (42:58)

I'm Martin Hinton. is the Cyber Insurance News and Information Podcast. Thank you so much for watching. If you liked it, please share it. If you got any comments outside of the subject matter we touched today, we'd love to hear from you. Again, enjoy the rest of your day. Take care.