Cybersecurity for Small & Mid-Sized Companies

Fri, 10/29 8:20AM 58:22

SUMMARY KEYWORDS

security, people, cybersecurity, company, attack, tools, grant, tyler, customers, vendor, address, understand, question, breach, supply chain, focus, talking, ransomware attack, important, share

SPEAKERS

Grant Walsh, Justin Bourgeois, Tyler Collins, Tom Utley, Aaron Bock, Matt Larson, Stephen Kowski

A Aaron Bock 00:00

All right, I think let's get started. We've got a good number of people on the line already, we've got some attendees filing in, but we want to be mindful of your time today. Welcome, everyone, on this webinar. Welcome. Hope you guys are having a wonderful day. Good morning, or good afternoon, depending on where you're joining from. We are excited to have you as part of the Opkalla Webinar Series. Today we'll be talking about cybersecurity success for small and mid sized companies. My name is Aaron Bock. I'm a managing partner here at Opkalla. For those of you who are not familiar with Opkalla, we are a trusted advisor. We consult anywhere from the small and mid-market to enterprise companies across infrastructure, cybersecurity, telecom, and other operational areas within IT. We work with a lot of these different companies with different scenarios we're going to be talking about today. And in today's webinar, we're going to be talking specifically about cybersecurity success. How small and mid-market companies deal with that. And we have seen a lot of these situations with our customers. And so we're going to make this as conversational as possible and hope you get something out of it. But we're going to be hearing from some of the highest rated vendors in this space, along with one of our customers, CPI security, who also has a very large focus on security, both physical and cyber. So today, we're excited to have you, please put your questions in the chat. Elizabeth will be moderating, and we'll get to those throughout. So before we get started to introduce all of our panelists today, I wanted to share a couple of stats with you guys. So I'm gonna pause my screen sharing. So a couple of stats today that I think are relevant for this conversation. So this is actually from one of our our panelists today, Mimecast. And Justin Bourgeois, who's on this, who's going to be speaking a little bit. So more than 6 in 10 companies suffered a ransomware attack in the year 2020. More than 60% of companies suffered a ransomware attack. That's a really high number, a lot higher than previous years. There was also 64% increase in email threats. I think we'll have Mimecast and IRONSCALES and others speak to that today. 79% of organizations were hurt by their lack of cyber preparedness. We're going to talk a lot about that with everyone here. And then 85% of all breaches involve some sort of human element. So with those stats, we're going to be talking about this in a conversational format. I would like to introduce our panelists, and I'd like to introduce the vendors here to talk a little bit about some of these stats and what they're seeing. So today, and let me make sure I'm sharing here. Can you guys see my screen? Okay, okay, good. I guess we can stop the share for a second. So with us today, we have got from CPI, we've got Grant Walsh and Tyler Collins. Welcome Grant and Tyler.

Grant Walsh 03:20

Morning.

Tyler Collins 03:21

Thank you.

Aaron Bock 03:23

I will let you guys go first here in a second. But from Arctic Wolf, we've got Tom Utley.

Tom Utley 03:30

Everybody.

Aaron Bock 03:32

From IRONSCALES, we've got Steven Kowski.

Stephen Kowski 03:36

Everybody, thanks for having me.

Aaron Bock 03:38

Thanks for coming, Stephen. From Mimecast. We've got Justin Bourgeois.

Justin Bourgeois 03:43

Good morning, everyone.

Aaron Bock 03:45

And from SentinelOne all the way from the West Coast, we've got Matt Larsen.

Matt Larson 03:49

Morning.

Aaron Bock 03:51

So what I'm going to ask you guys to do first is, if you guys can, let's go in the order that we started. So Tom, if you want to introduce yourself a little bit more, talk a little bit about Arctic Wolf briefly, share a little background, and we'll we'll go to the next one.

Tom Utley 04:06

Yeah, sure thing. So my name is Tom Utley. I live in the Charlotte area, been in networking and security for probably about 20 years now. And you know, I work for Arctic Wolf here in the Carolinas. We basically are a security operations company. We're focused on basically providing the services of a security operations center to small to midsize businesses. So, you know, you might not have the amount of resources to build a team of 12 or 15 security engineers. And so we basically provide that at scale to our customers. And we do services like managed detection response, which is 24/7 monitoring. We do manage risk, which is helping with vulnerability management, and we do managed awareness, which is basically a fully managed training program for all of your employees.

Aaron Bock 04:59

Awesome. Thank you, Tom. And it's awesome to see the success and growth of Arctic Wolf over the last year. Up next, Stephen, if you want to tell everyone a little bit about yourself and IRONSCALES, you're up next.

Stephen Kowski 05:13

Yeah, I'm Steve Kowski. I'm the Global Director of Sales Engineering, help our customers with proof of value exercises and kind of the technical side of our tool. Who IRONSCALES is, we run an anti-phishing platform that has a unique combination of both simulated phishing training and active threat mitigation based on AI and machine learning, Behavioral Anomaly Detection to catch BEC and social engineering. And we originated out of the Israeli Defense Force and fighting real world kind of threat actors at a nation state level and moved into the commercial space.

Aaron Bock 05:56

Awesome. Thank you for sharing Stephen. Justin, let's go to you.

Justin Bourgeois 06:00

Sure. My name is Justin Bourgeois. I am a Sales Engineer here with Mimecast. Been with Mimecast for four years coming from an implementation, network admin, security admin sort of jack of all trades background for the past 15. Mimecast is a security vendor that approaches security in three major zones. (1) Where we exist outside your perimeter, (2) your perimeter, or maybe the castle walls you might like to think about, and then (3) how we take actions inside the perimeter to circumvent and stop attacks throughout the entire mitre attack team.

Aaron Bock 06:33

Very good. Thank you for sharing. Thank you for being here, Justin. And last but not least, Matt, let's go to you.

Matt Larson 06:39

Hey gang, Matt Larson here. I'm a SentinelOne Account Manager in the Carolinas. I'm here in Eugene, Oregon. I've been in cybersecurity for a little over 10 years now. First half of I spent with Symantec. So started with the legacy AV signature based and moved to SentinelOne now almost three years ago. And SentinelOne is a next-gen and endpoint protection provider. So we focus mainly on the endpoint using AI, layering AI engines, along with adding in for the first time, automation for not just on execution, but full remediation. So we tie together with the rest of the panel here, we focus though mainly on that endpoint. And the way we try to keep you safe is by integrating with many of these other, you know, best-in-breed solutions.

Aaron Bock 07:34

Awesome. Thank you for being here, Matt. And thank you for being up a little bit earlier than the rest of us. So without further ado, our guests, we've got Grant Walsh and Tyler Collins, they are in the same room today. So I will go to them. Grant, Tyler if you guys can introduce yourself. And then if you guys can, I'll let you guys pick who's doing it. But if you guys can tell the crowd a little bit about CPI, what does CPI do? Give a little bit of background on how large, etc., and then we'll kind of get into the meat of the webinar.

Grant Walsh 08:06

Sure, so it's Grant Walsh. It's good to be here. Appreciate you guys having us on the panel. Been in IT roughly 20 years, primarily on the infrastructure side, a lot more focused on security. Last several years, this thing's ramped up and put more focus on that for the corporations I've been with. I'll let Tyler introduce himself as well.

Tyler Collins 08:25

Tyler Collins, thanks for having me. I've been in the IT industry for over 10 years, kind of across the the tech stack. So I would say Jack of All Trades as well. I'm happy to be here. And hopefully I can provide some good insight for the conversations.

Aaron Bock 08:44

And also, Grant, Tyler - can you guys give us a little background just because not everyone's from the North Carolina area. Tell us a little bit more about CPI, size, etc. What do you guys do?

Grant Walsh 08:54

So CPI Security is the leading security company for residential and commercial security systems in the Carolinas. So we have a footprint in North Carolina, South Carolina, Tennessee, Georgia, Virginia. Now we're a typical mid-size company. But we've primarily focused in this area. You know, I'd say we are, the overall ring ranking wise, we're number eight in the country when it comes to security companies. Just to give you an idea of scale wise. But we're a typical mid-sized company ranging in that, you know, that 1000 employee area.

Aaron Bock 09:26

Awesome. And and we're gonna kind of get into this. So it's kind of ironic, we have a customer who focuses on physical security, kind of as they started. So with CPI, Grant and Tyler, you know, Grant, you said in your intro, in the last couple years, you've been more focused on cybersecurity. So we're talking today about cybersecurity and mid-market companies, developing a plan. What's changing? So maybe just explain a little bit more to the audience, like why is cybersecurity becoming such a focus of your job even though infrastructure was it previously?

Grant Walsh 10:00

Well, I think I mentioned earlier in your stats, just kind of like the attacks have ramped up year over year. I think I even saw this morning that for 2020 to 2021, ransomware is up 148%, from 2020 to 2021. So, those attacks are happening more often, the phishing campaigns are happening more often. And I think in a mid-market company, a mid-size company, a small company, it's kind of that sweet spot. We've talked about it as part of our team. Large organizations usually have dedicated security teams, they have dedicated budgets, they've got CISOs, they've got everybody applied to it. And they've got a lot of data where that quote, unquote treasure for the attackers to get to and sometimes it's not worth the effort. And there's a lot of script kiddies and low, low hanging fruit that they can't get to. We on the other hand, mid-size company, not speaking for us directly, but just overall in general tendencies for a mid-size company, you don't have that dedicated team, a dedicated budget, a CISO, people just focus on that primarily. So you're wearing a lot of different hats. So as we've seen, in even where I was at before, companies our size are seeing more of these attacks, because we don't have that, didn't have that, couldn't have that focus on security, didn't have the budget allocated to it. So we've just been more, over the last couple years for myself, just speaking for me personally, we've had more of a focus to get to be aware of what's going on in security, because things just didn't, we didn't see this, probably 5, 10 years ago. While they were always out there, the conversation was there about being security-minded. It wasn't something we were laser focused on each and every day when you came in. I mean it wasn't something you just kind a thought of. Yeah, you had your best practices for Microsoft, you took your certs, things like that. But it's becoming more and more upfront. The media covers it more, we're seeing more high-level attacks, we're seeing more nation state attacks, we're seeing phishing campaigns on the rise, I think some of the tools for the guys today, you know, using Mimecast, or, you know, understand what IRONSCALES is bringing out, you have the awareness there of those types of attacks. Tyler, would you add anything that?

T Tyler Collins 11:48

Yeah, I think another thing is a lot of small to midsize companies, I think have this misconception that because they're a smaller company, that they can fly under the radar for some of these these malicious actors, and that's the exact opposite of the approach that you want to take. So I think that's another reason why Grant and I have also started making a really large effort into diving deeper into the cybersecurity space.

A Aaron Bock 12:17

Yeah, and I would add to that, you know, I know we'll get into a little bit more there. But I want to kind of build on what Tyler just said. For everyone listening, we work with a lot of customers all different sizes. And the number of times in the past year I've heard someone in the mid-market or small space say, "No, we're not that important. You know, we're only 300 employees. They're never gonna come after us." That is just not true anymore. It's changing. They don't really care how big or small you are. It's 'Do you have a weakness? And can they exploit it? And for how much money can they get out of you?' And I think we'll talk about that. Definitely, I'm seeing people smile on the panel, because I know that's a conversation that they're all having every day. I guess, Grant, Tyler, asked another way, and maybe Tyler, you take this one to start. So we're also talking about, you know, alright, now that we understand cybersecurity is important from all of the stats, and from just what's happening in the space and what you see on the news. How do you guys, and I know you're doing it right now, but how do you guys go about creating a cybersecurity plan? How do you decide, well, what are we going to do ourselves? What are we going to do in-house? Or what are we going to do externally? And what are we going to do with a third party? How do you guys go about developing that plan, executing that plan? Where do you see challenges in the small, mid-market, for really delivering a strong cybersecurity plan?

T Tyler Collins 13:40

I think we have to start with visibility. You have to know what you've got going on in your environment. I think that's kind of where it starts, internally and externally, what you're exposing. And you run into, I think, similar challenges. But at smaller scales than larger companies. You have the cost challenges, smaller budgets, so finding the right solutions to fit into your budget and working with partners that are aware of your budget constraints and bringing the right solutions to the table. And you've got complexity. So you've got on-prem, you've got cloud, you've got hybrid, you've got all these different, you know, models that add layers of complexity to security and figuring out how to navigate those on limited budgets and on, like Grant was mentioning, different sized teams that may not be a 100 person security team. And that's offensive and defensive. You know, we're trying to protect against people who have large teams doing offensive and defensive reconnaissance. Well, you know, we're trying to defend against these and they're trying, they've got teams working to to figure out how we're doing that. And so those are things that we're trying to battle and navigate. And again, I go back to the visibility, because in the end, if you don't know what's going on, then you can't protect it.

Aaron Bock 15:08

Grant, anything you'd like to add to that?

Grant Walsh 15:10

No, I think what he said, you know, understanding the strengths and weaknesses of your people, understanding the availability. I mean, most mid-size companies have small teams who can't work 24/7. Well, you could, you burn your people out and you have that rotation of people because you work them 24/7. You have to be aware 24/7. But that's what we kind of look at, that "Do we do it in house? Do we flex out?" You know, "Are there companies that can help us? Are there partners that come alongside us and can be a partner, not just selling us some tool?" That's the latest and greatest, with asking a partner to take the time to understand who we are, what we're trying to do, what we're trying to defend. Understand that, hey, you guys only have X number of people, here's how we can help augment that at a cost that's beneficial to you, you know, for you to stay ahead of the attackers.

Aaron Bock 15:51

Yeah, and one last - this might seem like a very cliche - question. Like, "Why are you asking?" Of course, it's important. But Grant, Tyler, I'll ask - why is cybersecurity so important to CPI? Why does it matter?

Grant Walsh 16:07

Why does it matter? We are CPI Security. We can't have CPI Security and a security issue. So there's brand damage, there's issues with customer data. Every company has the same thing, you know. When you're trying to get support - because to do all this, you need to have leadership support - you got to get the buy in to do any sort of stuff, have a program, understand the importance of it, somebody to sign the check at the end of the day. So that same thing is, "Why do we do this?" Well, not just because we want to because it's a cool IT thing to do, but there's a benefit to the company. "What's the cost of doing it?" versus "What's the cost of not doing it?" And "What's that brand damage look like?" You know, "We had an issue? What does it do to our customers if we have that type of issue? What does it do if we're on the TV? What does it mean, in terms of, even if it's small, what's does the cleanup effort look like in terms of resources I have to apply to it? Insurance costs, all those type of things?" So, why do we do it? At the end of the day, to protect the company, protect the brand, protect our customers. But also, just overall, to save money. I mean, yes, it costs money upfront to put it in place, but long term, those costs are much higher. We try to remediate or recover from an incident.

Tyler Collins 17:13

I think adding on to that is also bringing awareness to the employees and how important it is that they stay diligent and learning and continuing with our awareness training and understanding that they could potentially impact the entire business. And that does affect them. And so bringing that awareness to everyone is important, from the top to the bottom.

Aaron Bock 17:38

Yeah, I couldn't agree with you guys more. And I think what you said, Grant, about it being a monetary issue, but also a brand, a reputational issue, it could be even bigger than that. And I can't remember the stat exactly, but it was over 50% of companies, especially in the small and mid-market, when they were hit with a ransom attack, they were closed within two years, because they didn't have the plan and they didn't have the ability to recover, not only from the damage from data loss, or from a monetary issue, but from the brand damage that it caused. So thank you guys for sharing. So I also want to give some of these folks that have joined us on the panel a chance to share. We heard what their companies are doing. And I know they're partnering with a lot of our customers and people we're running into. But let's start with Matt. What are you guys seeing at SentinelOne? Maybe trends in cybersecurity? What are some of the newer things that are coming up in late 2021? We'll say post-COVID or sort of at the end of COVID, hopefully. What are you seeing from a trend? And then what are some of the challenges you're seeing with people being able to address security issues?

Matt Larson 18:57

Yeah, thanks, Aaron. And Grant and Tyler, that was great. It hit on, to me, the fundamental issue that I see. I talk with people looking to get a stronger stance and security every day. That's what I do. And the common thread of the people that I see that are dealing with breaches is that there is no ownership of security within their organization. So, Grant and Tyler, obviously you guys work deep in security and you understand it. Anybody on the call here watching this today, I would encourage you to make sure you have a champion for cybersecurity in your organization because it starts there. I want to back up. Way before any tools, you have to understand just how important it is, and then have somebody own that. Many of the calls I get on, even post-breach, the breach isn't really anyone's fault because maybe it's in IT. You know, an admin, that's really easy, just infrastructure. This is a side gig and he pays attention a little bit, but I would just start there. Like Grant grab a champion, make sure, because that, outside of tools, is the common thread of the people that I see suffering from ransomware over the last two years. So let's start there. Make sure you get a real champion inside your organization. And then as everyone knows, just the frequency of attacks has gotten to the point where for many organizations, doing this on your own is not possible. So I would say the, you know, the Arctic Wolves to the world that are watching, you know, 24/7, we have a vigilance offering, but people augmenting your team I think is the wave of the future. We have great tools, but in, you know, in the hands of someone that's not paying attention all the time, still, there are gaps.

Aaron Bock 20:52

Awesome. Thank you for sharing, Matt. Let's go to Justin. So Justin, same kind of question. You know, what are you guys seeing from a trend perspective? What are you seeing as a challenge, either for people procuring technology, or trying to address the cyber flaws in small and mid-market companies? And how are you seeing them either be successful or they're not getting what they want, they're not able to address the concern.

J Justin Bourgeois 21:15

Oftentimes in the conversations I'm having, budgetary concerns, and just simply, like mentioned earlier, just not having that champion in leadership that understands just how fundamental cybersecurity is to the general health of an organization. One thing I do like to note and kind of call out specifically is not just a rise in ransomware attacks and spear phishing, but also in supply chain effects. This is something that is on the rise globally. And yes, you may be the kind of lowest hanging fruit in the attack chain that they're trying to work up. Granted, I can get access to your account. Let's say I'm now looking through your email. If I see the suddenly you have a partnership with this other higher market vendor, partner, whatever it might be, that's a goldmine to me, because now not only can I use your information to get money out of you, I can use your relationship to this giant client, customer, whatever it might be, and now turn them into payday. So I think focusing on the supply chain, understanding that no one person does this alone, and it has to start from the ground up. Get buy-in from leadership, understand that they need to be made aware that cybersecurity isn't just a professional problem. It's a personal problem. Using the same password on Facebook as you are for your domain credentials, that's a huge risk in both directions.

A Aaron Bock 22:45

Yep, so you're saying don't put your child's name and the year you graduated as your password?

J Justin Bourgeois 22:51

Pet names is a particular favorite. Snowball718 is not a great password.

A Aaron Bock 22:56

Yeah, no, but you're right. And I think you hit on a couple things that are, you know, not only trends I think in cyber, but like the supply chain issues. There's some coming from COVID, things like that. But there's also a lot that are coming from cybersecurity breaches. It's shutting down an entire supply chain. And we're seeing that lead up, we're upcoming on the holidays, you know, people saying, well, things aren't gonna come in time. It's because the supply chain is being attacked. And you're right, people are going down market, they're going up market. And that's where I go back to the question of, "Why me?" We're talking, you know, a lot today about small and mid-market. It can affect the people you're working with.

J Justin Bourgeois 23:34

You may not be the end goal. That's kind of the point. You're just the first step into hitting that big fish I'm after.

Aaron Bock 23:41

Yep. Absolutely. Stephen, let's go to you. So same question. What trends are you all seeing at IRONSCALES? And then what are you seeing as far as addressing those cybersecurity issues within a small, mid-market? What are you seeing as challenges, maybe creative ways that people are addressing it, etc?

Stephen Kowski 24:00

I think that just to build on, you know, what Justin was saying, I agree. This supply chain attack, anybody, you know, any vendor impacted by like, SolarWinds, or something like this, you know, it's a real concern, right, we need to be, you know, focused on that. But also, I think I heard something earlier about the kind of limitations from a human standpoint, right? The resource challenges. You need tools that, you know, you're not getting this kind of death by dashboard that will scale along with the threat, because it's growing every single year. It's not going away, it's not getting better, right? So you need something that is going to grow in scale and with your organization and actually be a force multiplier at the SMB market level, because, like we said, there's just only so many folks. And then I want to go back to Matt's statement. I loved it. You know, you do need that mouthpiece and you do need that champion, but also, I think it's even beyond that, you need every single person, like we've been hearing here, to understand that this is not a technology problem. This is a business risk problem. Security is a risk management function, first and foremost. It's not just a group of technologists. The business has to understand that. And then also each individual employee that may have to understand that the business may survive, and your role in it may not, right? So if everybody has a personable, actionable interest in it, and needs to, you know, really take account. But for us, when we look in the messaging space, most of our focus on that, you know, you look at median impact of any given phishing attack - $260,000 - but 10% of them, you know, I think are up in the world, up around $10 million, right? And what we're seeing is hyper personalization, social engineering. If you look at the latest Verizon DVIR, it is increased from, I think, 11% to 22% over the last year. And when you see the things like, OpenAI, GPT-3, you see phishing as a service economy growing, it's dirt cheap to send an email, right? That's why you're seeing this growth. It's because it's just so easy to do. Anyone can do it, and we can buy a rootkit. It's very, very simple. So I mean, we certainly see trends around holidays and COVID, and these types of things. We're gonna see that missed package FedEx wanting you to click and put in your information. We certainly see that. But I think the bigger thing that we're really kind of looking at is that we're targeting the users. This is becoming a social thing. The user has become the new endpoint, right? All the statistics are showing that. So we need to really focus our energy deeply in making sure that they're aware of the threat, their role in the threat and how to take action against that threat.

Aaron Bock 27:00

Absolutely. Yeah, some of the stats that you just shared, and what we were talking about with the human element of it, they are real. And some of them I don't even know if we're quantifying them correctly. But a human is a weak spot. And you know, the attack vectors are getting larger, they're getting bigger, they're getting wider. And it's "How do you address those up front?" And what's interesting is you come back to, you said email messaging, where you guys focus, that's still the predominant area, but it's getting more creative every day.

S Stephen Kowski 27:30

Number one ingress point of every attack, you know. While we're worried about the internal, the ransomware, that's already inside the house. We need to, you know, not miss sight of the front door and putting a lock on there and putting some alarms on there. As important as ransomware is, I don't mean to discount it, but I totally agree with you.

A Aaron Bock 27:50

Amen.

T Tyler Collins 27:52

Another part of the end user perspective is helping empower them to be able to communicate that something seems off or not that they're going to get in trouble for recording something or, "Oh, I clicked on this," and then just letting it go without recording it or without giving them some type of medium for communicating that. I think that's another big challenge and a big ask that we have is communicate and how can we help you feel like it's not a "This isn't to say you're not gonna get in trouble, this is something we need to be aware of." So I think that's another big challenge that a lot of companies really have to focus on.

G Grant Walsh 28:32

At that point, you know, if you've been in IT long enough, there's hopefully a shift from legacy IT where the shame game was strong. "Shame on you for clicking on that." No, I'm not shaming you when you don't know, you have a gazillion emails coming in and you're trying to do your job. You know what, our job is to help educate, up-train. It's "Thank you for bringing that to our attention - here's why it's important that you brought that to our attention. You know, here's how we can make sure. Here are the tools we can put in place to help block that." To an extent you can't block it all. And then we kind of explain we can't block everything. But the main thing for us is, these are our customers, have some empathy. Understand, they don't know everything that we obviously look at from an IT side. They don't understand this is the sophistication in terms of the attack threats coming in from email. So just having some empathy with people and not shaming them. Because back in the day you would shame them for every little thing they did. In a blue screen, you shame them. It's their fault the PC crashed, or do you know, you shame people. Well the same thing now, you've got to have empathy, and that helps buy support. They understand you're not going to come down on them because they have suspicions about email. And they're more likely to come to you with some other issue that comes up.

T Tyler Collins 29:36

And they're kind of your line of defense. I mean, you've got to have them on board and then you introduce new tools. They're gonna buy in if they feel like they're included in their understanding of what you're trying to do. You're not just "Oh, another tool. Oh, another this. Oh, another process. Oh, another ...." You know, if they feel like they're included and they understand why you're doing these things and how it can impact them, as well as the business, then you really are marching in the right direction.

A Aaron Bock 30:04

Yeah. And I mean, I think you guys all hit it on the head. But I mean, we're talking, we're hearing from some of the people that have these tools that help make this easier, but it's not ever going to be 100%. It's just not. It's hard to secure 100% because there's always a new attack vector that's coming in. And so I think, to your guys' point, empower your users, give the culture to embrace security, allow people to have a method, whether it's via tool, or they can come to you and say, "Hey, I've got something that I don't really know what I'm doing, it looks suspicious." Have that culture so that you guys can deal with it. And hopefully, you can add in tools, you can add in services that allow you to address those easier. I think that's what we're seeing in a successful organization versus like, you guys just said, click on something, well, you're fired. I mean, that's not a culture we want because just the reality is that I think the execs are some of the worst people at some of the companies as far as who are being targeted, and do they follow the security protocols. So yeah, Grant, Tyler, thank you for sharing. Tom, let's go to you. So let's wrap up the question of cybersecurity trends you're seeing. And then I want to ask another question, want to go to Grant and Tyler after this. But a few times, it's been brought up, one of the hardest things about cybersecurity and getting the right cybersecurity approach is addressing with leadership, having an executive sponsor, making sure that your leadership team is on board. So I would ask you, what are the trends? And then how do you help leadership - folks that are maybe not as familiar with IT or security - how do you help them understand the risk and the value, even though its cost they haven't seen before? How do you do that?

T Tom Utley 31:52

Yeah, those are great questions. And I just want to echo what the other folks have said about the trends. I mean, user awareness and supply side attacks, or supply chain attacks are definitely, you know, the two biggest things that we're noticing. I mean, just to go back a little bit with the SolarWinds incident, imagine, you know, you've got this environment, you've got your tools, you're managing your environment the best you can. You wake up one day, and you're completely owned by an attacker. And this is not something that you did wrong, it came in as a part of the software for one of your trusted tools. So there's really no way to prevent that from happening. So, you know, the only thing you can do is detect that and respond to it. And so, yes, like, why would a small company be worried about that? Well, you might not even be the target, you might just be collateral damage. You know, supply chain attacks have introduced this concept into security that they're going to attack the entire ecosystem and try to get the large companies, but at the same time, your network is also being owned. And so I think, you know, it's about to be Halloween, I think that's pretty scary when it comes to the supply chain attacks. On the user awareness side, I think it's something like 85% of attacks begin with a user error, like clicking on a phishing link or downloading the wrong file. And I think it's important to have the right attitude about it. So instead of just saying, "Okay, we got to do this once a year, hour-long training session, so check the box and make sure that you attend," that's not the right approach. I think that you need to keep up with the latest trends, the latest attack methods, and keep that training continuous, you know, once once a week, once every other week. Small bite-sized pieces of training, to make sure that your folks are aware of what people are doing right now. And then when it comes to trying to communicate the reason that you need to have a security program, you need to have a strong security posture - obviously, with IT, our job is to increase productivity, to make the company better so that the company can make more money. And you start talking about cybersecurity, and it's kind of a different conversation. You're not going to put in place cybersecurity tools and make more money. But what you're going to try to do is put in place cybersecurity tools to reduce your risk and to prevent you from losing money. And so I think the important thing there is to communicate a total cost of ownership based on the potential costs with a cybersecurity attack. So it'd be realistic, you know. Go from, you know, an account compromised, that leads to maybe business email compromised where you pay the wrong account. And then go all the way up to a large-scale ransomware attack where they're asking for millions of dollars. And just explain all the different costs that are effective with that, not only IT costs, but also just business downtime and those types of factors, such as brand reputation. Once you put that in place and give sort of a range of costs, it becomes really easy to show, you know, "Now here's the cybersecurity budget." So this is a very high amount of savings compared to what could happen.

Aaron Bock 35:12

Awesome. Yeah, Tom, thank you for sharing. And I agree, I think it's about telling the story, about the "why". And I want to kind of punt this over to Grant and Tyler. So, you know, obviously, CPI has security in the name. And so I think there is a focus on security for you guys inherently. But I would imagine you guys still are seeing new maybe cyber risks, and there's new cybersecurity prevention tools, etc, that are coming out where not everyone in leadership would understand that. How do you guys help create, like what Tom said, how do you create that story around "this is why we need it, this is the risk"? How do you evaluate the different vendors and options that are out there? And how do you, you know, really address these risks from a third-party vendor versus internal perspective?

Grant Walsh 36:04

That was a very deep question.

Aaron Bock 36:05

It is a deep question, so think hard.

Grant Walsh 36:06

Multi-layer there, for sure. I mean, when it comes to leadership, it's just awareness. Using real life, real world examples of what's going on out there. So they're aware of, "Hey, this happened to Company A, what would that look like if it happened to us?" You know, just kind of play that to Company A, what would that look like if it happened to us?" You know, just kind of play that scenario through, so they can understand what that impact would be. "Here's the solutions we have in place, and here's how we could or could not have stopped something like that at our level." Allowing them to understand, not so much deep in the weeds, what the technical aspect of the tools do, or what we're looking at doing. But, "Here's the data that we have that we're trying to protect, and if that type of attack happened to us, here's where we could have stopped it, here's maybe where we would have missed. This is why this tool, or this solution would help us." And as we kind of grow, and you know, companies expand from on-prem to, as Tyler mentioned, on-prem hybrid or in the cloud, now data's sitting over here. Now if that same type of attack was a supply chain attack, "How does that affect our data sitting there? How does that tool that we're using, how are they secured to keep our information secure internally? But overall, when it's speaking to leadership, it's what we said over and over again today. It's really the cost of doing it versus the cost of not doing it. Yeah you're going to invest as much that may stretch over two to three to four years depending on that investment. But one attack or one breach or one incident could easily wipe that cost out when it comes to the remediation and recovering from it or, like you said, if small to mid-size companies don't recover after two weeks, they shut down. That's a massive loss. So it's just for us from a leadership standpoint, it's communicating to the ownership, executive team on a regular basis, not just doing it at budget time. You know, it's once a year you get your budgets. "Hey, now we're done talking about security for next year." That's an ongoing thing every week, every month. Have that slide, that point in the executive communication of, "Hey, here's what we're doing. Here's how your tools are working." So after you've got the tools in place, "Here's how your investment is paying it back. Here's how your investment is working every single month, every single week. Here's how your fishing tools are working. Here's how your endpoint tools are working. Here are the things we're catching." So that builds that confidence every week over and over again. That "Okay, the money I spent as an owner, or the executive team that we spent on the company, is paying back. I'm getting bang for my buck."

T Tyler Collins 36:09

Yeah, I think to add again, it's the constant awareness. It's the ongoing awareness of what the threat landscape looks like, to the business internally and externally and other companies similar. It's the constant. This is something that's happening every day. It's changing all the time. And I think historically, a lot of companies just had no awareness of how frequent these types of attacks and incidents are. And it's got to change. That's got to be a constant conversation.

G Grant Walsh 38:54

It's never ending, unfortunately. "Did you talk to ownership? Okay, so now we bought this, we're secure?" "No, we're secured for now. We're good against this particular threat today or this second. Tomorrow it can change quickly." An attacker changes direction just like anything else. So it's a, you know, to be cliche, it's a cyber war. You are constantly on the defense, and you're having to constantly change your tactics, techniques to stay ahead. So that's the same thing. If you continually remind your leadership and help them understand this thing is going on. And every time it hits the news, "Hey, here's another one. Let me share this with you. This one was on the news today, you probably saw it." We all saw the Cloner pipeline ones or the Kaseya ones, or the other instances out there in the world that happened. So "Hey, this happened. Here's how that could have impacted us." Just having those conversations. And that's, you know, let them know that it's not an ending project, you know, where you hit a certain date and you're done. It's the constantly evolving and trying to stay ahead of those attackers.

Tyler Collins 39:46

And your fighting - these have become businesses. If you're fighting against businesses that have, you know, their goals are to figure out the way they can get in, all they need is one. I mean you're you're trying to protect against everything you can. All they need is 1 - one zero day. One something. And so it's, you know, again, it's the awareness. This is new. This is only going to get worse.

Aaron Bock 40:10

And to that point, for those of you who are monitoring the chat, Tom had shared, we brought up the SolarWinds attack, I think multiple people did. He shared a link. If you take a look at that afterwards, but you see, we talk about the threat landscape changes. And this is why we have to always be prepared prepared. The same group that attacked SolarWinds is now attacking the customers. And so they're changing their attack vector. They're changing the way that they're going after people. So thanks for sharing that, Tom. We actually had a question come in, and I want to direct this - let's go to Steven first. And then Justin, second, because you guys kind of both brought this up. So question is, what advice do you have for assessing the security level of a third-party provider? Because you guys both mentioned third-party providers in the supply chain attack? How do you assess the security landscape inside of one of your vendors, whether it's cybersecurity or other? And then how do you guys specifically share - I mean, you guys are security companies, so that's what you guys do, but how do you share how secure you guys are? And how your supply chain is tight or protected? Steven, let's go to you first.

Stephen Kowski 41:15

Absolutely. Yeah. Great, great question. I'll talk about how we share, first and foremost, is through accreditations and third-party audits, internal pentesting is what we're doing all the time. And how we share those reports under NDA is some our SOC 2 report, right, ISO certifications, and our regular continuous audits of our own environment. That's how we share that and how we secure it. We're a security company first and foremost. And if we kind of fail in that respect, we've really missed the ball. As far as other clients and vendors, don't have a ton of subprocessors. Those that we do, we try to make ensure that they are having similar controls put in place, they are having pen tests being done, they have similar audit requirements. And frankly, if we can limit it to just as minimal data as possible that we transmit, we don't want to give them anything more than they absolutely need to give us data back. I don't want to give out an entire email. If I just can give out an MD5 hash to a vendor, that's really all I want to do. Right? And so it's, "How do I minimize the amount of information that we're giving out ongoing, and then making sure that they are establishing these minimums and they're maintaining those, and allowing us to do independent audits as well?"

Aaron Bock 42:52

Yeah, that's a great answer. And so Justin, going to you, similar question. But, you know, how do you guys address the third party supplier, and then maybe give your recommendation to those who are listening. How should they go about also addressing their third party suppliers, whether it's an IT or other.

J Justin Bourgeois 43:09

Certificates and applications, ISO certs and SOC 2, type two, whatever it may be, those are a great place to start. As a security professional, though, as the IT manager, whatever the position may be, you're probably going to get some sort of pushback, some sort of request from an end user, maybe even someone in the C-suite, that this vendor needs to be treated differently, this needs an exemption from this rule, this needs this, this needs a custom something. Fight that. Fight that hard. Don't carve out explicit whitelist exemptions for those vendors, because let's be honest - sometimes as security vendors, we need to play our cards a little close to the chest. I don't want to tell you what kind of firewall I'm using. I don't want to tell you what endpoint solution I'm using. Because yes, we may be partners, but it's kind of not your business. So I would say beyond, especially for the smallest side of the of the businesses, that the affectations and the certificates, those can be quite onerous to achieve for some startup. And maybe they do some sort of niche thing that is fantastic, great partnership to have the accompany. But at the same time, that's a company of 10 people. They're not going to go out and get Soc 2 certified anytime soon. And so understand that the rules you put in place as a security team and your assumed higher security ecosystem are there to protect the ecosystem. Carving out exemptions is just a general bad idea. And I would recommend you fight that regardless of who, whether they have a C in their title or not, requests that kind of exemption.

A Aaron Bock 45:00

Yep. Steven and Justin, thank you for sharing. We actually had another question come in. I want to go to Matt because Matt sees it from the account side. And I think more of the dealing with the decision-making side a little bit more. And I know you guys were brought in a lot of times when, you know, shit has already hit the fan, excuse my French. So Matt, maybe share from your perspective. What are some of the horror stories, in light of Halloween coming up. What are some of the horror stories you've seen? How bad can it get? What are you guys seeing? And then maybe share with with the customers who maybe have been lucky enough not to have been hit with a breach or a ransomware attack or, you know, maybe they've had a scare. Why is it so important to do that before the scare happens and before it actually works? So that was a lot there. But you know, feel free to dissect as you wish.

M Matt Larson 45:54

I'll do it for Halloween. Yeah. So it is part of my job. I guess I started just a couple of years ago. I got together with some of the public sector IT managers at NCLGISA. And I threw out an invite. "Call me anytime." I knew some of them had dealt with breaches in the past. They put together a strike force. So a bunch of people fighting together tried to, for the common good, for the public sector in the Carolinas. And it wasn't much more than a week later, I received a call at about 2:30 in the morning my time here from a frantic IT director and they were locked up, a neighboring county was locked up and had no real tools. You know, I think they were calling law enforcement, they had a whole team of people, they probably should have called before me. But I at least pointed them in the right direction. And I guess the horror story is that this was exactly - they were getting together, finally putting together a strike force and focusing on this collaboratively - but before that day, no one owned this. These were IT people, not security people. So it really drove that home to me, as I watched over the next couple of years, this happen. And again, the the common thread there, they were dealing with antiquated systems and the thought that someone would go after them hadn't even crossed their mind. "Why would someone? We have no money." You know, and we saw that kick off a string. So I think the supply chain attacks have really put to bed the idea that, well, "You're not going to be a focus." You may not be the end target, as Justin and Steven have said, but that doesn't mean you're not going to be part of that. So I've watched, I guess, some 55 of them over the last couple of years that had called me and said, "I wish I had talked to you six months earlier." But it's not just endpoint security. I mean, this is going to go for anyone here on the panel. Get somebody to really own this and put your processes in place. And like you said, stick to them, as Justin said, because it can get ugly, at 2:30 in the morning, thinking that you're not the target. It really is irrelevant. There is a lot of collateral damage.

A Aaron Bock 48:34

Yeah. And to that point, you know, we've talked - and thank you for sharing that, and for the sake of Halloween, obviously. But, you know, we've talked a lot about all these things you can do, and it's better to be doing it earlier, rather than once things have already kind of hit the fan. So I want to go to Tom and then Grant and Tyler. So, Tom, you guys specifically deal with customers who may not have the resources on the security side to really even come up with a plan and really kind of move that along because they don't really know where to start? What is, you know, obviously, with the mid-market and small, IT resources is always a challenge. How do you guys go about it - and what would you suggest for a company that doesn't have the staffing to really address the cybersecurity properly? How do you start? Where would you advise someone to begin? How do they end? And then let's go over to Grant and Tyler afterwards to maybe get your customer perspective.

T Tom Utley 49:33

Yeah, so I mean, I would start with a framework and making sure that the leadership at my company is agreeing with me that we need to fill out this framework. Basically have a solution for each component of the framework. And there's several different ones. The NIST framework is probably, you know, the most popular, but it basically gives everyone a reference point. You know, here's what we're talking about when we say we need to detect issues. Here are the different components of that. Once you have that in place, you need to figure out "Okay, what should we address?" And obviously, Arctic Wolf can help out a lot in terms of addressing those different components because we monitor environments 24/7. And we provide a concierge security team, which are security experts that are focused on your individual account to work with you and shore up your environment over time. So that's a part of our service is to have that team of experts that you can reach out to, and that can help you build your security posture. So even if you don't go with Arctic Wolf, I think it's extremely important to have security expertise that you can leverage, whether it's in your company, or a consultant, or a service like ours, so that you can assess, "Here's where we are. How do we get to a good state from right here?" That's really the most important thing.

Aaron Bock 50:54

Awesome, yeah. And I guess let's kick over to Grant and Tyler. So from your side, you know, even at a mid-market company, and it depends, I guess, on what your classification of 'mid' is, but you guys I know, have dealt with staffing challenges. I think we all have, especially in the last year and a half with COVID. So you know, staffing being an issue, finding people to fill roles that you really desperately need, how do you know, that list of "Okay, hey, we've got a lot of things we need to secure." It might be broad, you know. It might be everything in some some people's eyes at the company, which is fair. How do you start? How do you start with that list? And how do you start checking those boxes off?

Tyler Collins 51:33

Yeah, I mean, I think this kind of goes back to what Tom said. I think you get the visibility. First you figure out kind of what framework. You do a risk assessment or pen test, or kind of identify the potential exposures that you have. You do your research and find "Is the primary attack vector, which, you know, we're seeing a ton of email. Okay, is that a place we should start from? Let's ensure that we're securing our environment from the email side first." but I think it still goes back to working with a partner. And doing your research internally, and figuring out, you know, "What's the most likely vector that we are going to be compromised?" And start going from there. And that's, still, a part of that is working with a vendor and getting that visibility. And then just start checking them off.

Aaron Bock 52:31

Awesome. Well, we've got five minutes left. There's a question here in the chat. I'm going to leave this as a rapid fire for all of you guys. But it's kind of a funny question. So, "Who are these bad actors that that hack into the orgs? They're obviously smart. Why can't we use those smarts for good?" I'll let, let's see, let's go to Justin first. Why can't we get these people to work for the good guys?

Justin Bourgeois 53:00

Because it pays too well. It pays too well. I mean, if I send out an email campaign, and let's say it's bottom of the barrel, no sophistication, I'm expecting maybe a point 1% success rate there? Well, I send that to 2000 people. That's two people. And 2000 people, that's basically all of Mimecast. Okay, so now I send it again to nine other companies? It's just simply too lucrative.

Aaron Bock 53:27

Awesome. Steven, let's go to you. Quick question. Rapid fire. What is the maybe the largest ransomware amount you guys have seen? You don't have to disclose the customer, obviously ransomware amount you guys have seen? You don't have to disclose the customer, obviously. But what's the largest ransomware account? Or - in the sake of Halloween horror stories - what is the highest click rate of emails, bad emails and training, you guys have seen in an organization? What percentage of people click a bad email?

S Stephen Kowski 53:56

Percentage click rate? Yeah, when we're doing these trainings, I've seen as high as in the 90's. You know, in some extreme cases. I think you can always drive it down. You could drive it down to, you know, maybe 10 or 15%. But because we're trying to paint a moving train here, you're not gonna get it with just templates alone and that kind of thing. So, you know, with the customization and the hyper-personalization, it becomes very, very challenging to drive it down much, much further than that. So, I don't know if that answers it.

A Aaron Bock 54:33

No, 90% - if I'm the CFO, CEO, I'm the IT manager of that organization, I am very worried. I saw 68% in a 2000-person organization last year. That was the highest I'd seen. So 90 is very scary. Thank you for sharing. Tom, one last question for you. So I guess from what you guys see commonly, what is the biggest challenge from a cost perspective when it comes to addressing a security need? And I could kind of tell this story probably for you. But what do you guys see people try to do to address something, and then it doesn't work and so they go a different route?

T Tom Utley 55:13

Well, I mean, so there's two things. On the technology side, there's a tool called a SIM, which a lot of people try to install and manage themselves. And you quickly find out that you can't just purchase a SIM, you also need all of these various add-ons. And getting all that configured and tuned is a very long-term project. You have to hire people - not just one person, but people - to manage that tool full-time. And then you have to start hiring people who are forensics experts and can dig into security issues. And so then we get to the second problem, which is people. And the cybersecurity experts are just few and far between these days. And, you know, rightfully so, their salaries are very high. And so it just becomes extremely expensive to do this on an individual company basis. So that's sort of where we come in is that we've been able to do this at a scale where we can provide that level of service, but without having to hire so many employees.

G Grant Walsh 56:13

Awesome. Well, guys, we've got two minutes left, and there are no more questions and I want to be mindful of everyone's time. Thank you guys for sharing your your stories, your horror stories, especially Justin, Steven, Matt, Tom, and then Grant and Tyler. Thank you guys for sitting on this panel. We hope this was valuable for you guys. If you guys have not spoken to any of these guys with Mimecast, SentinelOne, Arctic Wolf and IRONSCALES, I highly recommend it, because they definitely do serve a need in the cybersecurity space, especially in the small and mid-market companies. And I think Grant and Tyler can attest to that. What I would ask, if you guys have any questions, please feel free to reach out to Opkalla. We see this every day with our customers. We get the question, "Hey, I don't really know where to go next. What vendor? What tool?" "Hey, there's a process, there's a service I'm trying to address. I don't even know if it exists." Please reach out to us. We see this. We've done it before. Don't recreate the wheel. Once again, guys, thank you very much for joining. I'm going to share a screen as we leave that just shows what's coming up next. You guys can see my screen now. But thank you to you guys for joining. What's next - we're going to send out this webinar recording for all that could attend and couldn't attend. We're also going to attach a cybersecurity checklist for you. I would recommend, if you haven't done this, go through this as an exercise with your organization and see where do you guys fall. We're also going to send out an interactive quick assessment. You can find it on our website, but it's an assessment that will kind of help you guys go through some of your security issues that you have. If you feel like you have something that's an issue, fill it out and see how you scope it. See how you would address it. And then lastly, we have a webinar coming up in November. We'll release those dates. We're going to be talking about unified communications and contact center as a service. So thanks all for joining. Hope you guys have a great rest of the week, a happy Halloween, and thanks for joining us.