With Mark S. A. Smith

Avoiding Digital Disruption: The Future of Cyber Security

Mark S A Smith

Mark S A Smith: Today's podcast is a little bit different. I recently did a speech for a client, Prime Edge, in Washington, DC, to a group of her clients about security issues, and in listening to the program, I thought you might find some of the conversations and concepts valuable. So sit back, listen, and get educated on how you can keep your company secure.

Thank you, Sue. I appreciate it. Thank you, HP, for sponsoring this. Thank you, Sue, for inviting me to come in from Prime Edge. The world is changing faster than you can even imagine. We have been through, collectively, enormous changes in technology thanks to the ever-increasing advance of Moore's Law and Metcalf's Law, and there's another law I'd like to introduce you to that's going to help you explain to your team and to your executives why the topics we're going to talk about tonight are so critical. And that is Martec's Law.

Who here is familiar with Martec's Law? Have you run across that before? All right. I'm going to explain it to you very easily. It happens ... And you can explain it in four lines. It's something you can do on a cocktail napkin, which is a really good place to have that conversation with your executives. It's really simply this: technology advances exponentially thanks to Moore's Law. Everybody here's familiar with Moore's Law? Right, got a quick recap here.

Moore in 1965 wrote an article in Electronics Magazine observing that the number of transistors on an integrated circuit were doubling every 12 months and was expected to do so into the foreseeable future. Here we are in the foreseeable future, and we're still seeing the doubling of compute power every 12, 18, 24 months. Of course, the impact of this on us is that with can get the same compute power half the price every 12 to 18 months or we can get twice the compute power for the same price every 12 to 18 months, which makes it very difficult for us to budget and approve compute power when we know we can get it cheaper next week.

It becomes a very interesting problem. One of the challenges that we face today is that nobody who's approving digital budgets are saying, "Yes, let's plan five years' worth of IT today and we're going to pay the maximum possible price for this, for technology that's going to be worth 20 percent or a 20th of what we paid for it five years later before we retire it." Nobody's saying yes to that anymore, and of course, the end result is we outsource everything we possibly can to let somebody else manage the depreciation thanks to Google, Microsoft, and AWS.

We have this amazing curve that's driving us crazy, but then when you take a look at human behavior, organizations tend to change logarithmically. So what we do is we grow 10 percent year over year till we hit the cognitive capacity of our chief officer. That's so important I'm going to say it again. We grow by corporate standards perhaps 10 percent year over year until we hit the cognitive capacity of our chief officer's ability to handle change.

The problem is that over time, this gap gets to be so big that it forces a reset. Thank you for doing that on cue. That reset usually disrupts the company. Now, large organizations are not immune to this. Half of the Fortune 500 turns over every decade. It's true. Half the Fortune 500 were not on the list 10 years ago, and half of them will be gone 10 years from now. Actually, I expect for it to be 80 percent will turn over, because most of them aren't going to make the Martec's Law gap, filling it in. They just don't have the capacity to do so.

The question that you get to ask your executives is how big is this gap, and how quickly can we fill that gap? What ends up happening in the world of security is that if your gap is here and the bad guy's gap is here, they win. You lose. That's the fundamental driving factor that we all get to consider when we talk about the protection of corporate assets. How big is the gap between you and securing your assets versus how big is the gap between the bad guys having access to your assets?

Quite frankly, there's only one way to tell. You gotta do assessments on a regular basis. You have to do penetration testing. You have to test your people. You have to test your organization. You have to test if people are patching their servers, if they're updating their mobile devices. You gotta find out how big that gap is. So with that fundamental concept of Martec's Law, you have a basis to have a conversation with your team and your executives. Is this helpful?

All right. The name of this, M-A-R-T-E-C, and it was observed by Scott Brinker. He dubbed it Martec's Law. My suggestion is use it as part of your tools and conversations. Cool? With that in mind, I have prepared for you a few of the things that I've run across through the years. I am an electrical engineer by training, but I have recovered. No pocket protector. I have been involved in bringing disruptive technology to market ever since I graduated from college in 1982.

My area of expertise is helping people understand the nature of disruption and the nature of technology. Along the way, I've written 14 books. The book that I wrote in 2004 was Security in the Boardroom. It was specifically designed for executives to help them understand the new wave of cyber security issues. Right now, I'm rewriting version 2.0. While the book still is 80 percent accurate, we don't have things like ransomware in there and some of the other things that are going on that I'm going to share with you.

So I do have some understanding of the security issues based on my experience in working with organizations over time. I want to share with you today, and we've got a little handout that you can take with you, about the reality and the future of security. The first thing I want to talk about is, why is security important to you? It's really important for you to start off with your personal motivation for security. So tell me, why is security important? Just shout it out.

Audience: Protect data.

Mark S A Smith: To protect ...

Audience: Data.

Mark S A Smith: Protect data. Okay. Why? Why is that important?

Audience: Money.

Mark S A Smith: Money.

Audience: Savings.

Mark S A Smith: All right, because the data is translated to our ability to create money. Why else is security important for you? Tell me.

Audience: So that you can hold on to your money.

Mark S A Smith: We can protect our savings. We can protect our assets. We protect the core business. Good. Why else is security important? What do you think? Why is it important to you?

Audience: To protect your people.

Mark S A Smith: Protect your people. Yeah. We do have to protect our people. Yeah. There's lots of good laws that protect our people. Why else? Why is it important to you? Okay. Who here is your job is to protect those assets? Okay. So that's the reason why you want to do it: because it's not only your job, but if you are compromised and there is an impact on the business, your career is over. Would you agree with me? Right.

It's your business. It's your job. It's your career. It's your livelihood. The reason why you've got to protect this stuff is because if you don't, you're going to be working for the Geek Squad or selling IT. You don't want to do that, do you? I know. I know, Sue. We're just having some fun here. I want you to really understand this is the core element of what determines whether you're going to retire from this industry or not. The sharper you get at closing Martec's Law gap, the more illustrious your career will be.

The next question to ask is, what does it cost if you lose your data? Thinking about this, what's the cost or the other side of this? What's the value of retaining your data? What is the cost for your system to be unavailable, for your data to be unavailable? Anybody know?

Audience: Customers.

Mark S A Smith: It costs customers. Let's talk about real dollars. What does it cost when your system is unavailable for whatever reason?

Audience: A lot!

Mark S A Smith: A lot. That's not a good answer. If you were called into court and say what does it cost for your system to be compromised, "a lot" is not going to be accepted by the judge. Anybody know? Let's fix that problem right now. The easiest way to estimate your loss, the cost of your loss, is to calculate revenue per hour. The assumption here is simply this, that if your system is unavailable, you cannot sell. You cannot bill. You cannot deliver. You cannot collect money. Essentially, you are out of business, and so, therefore, your system up-time is a reflection of your revenue per hour. Is that a reasonable assumption to use?

That's a starting point. It's not complete, but at least we get into the ballpark. Cool? Here's how we calculate revenue per hour. It's really pretty simple. If you're a 24-by-7 operation, you need to divide your annual revenue by 8,760. Why 8,760? Because it's 365 x 24. There's 8,760 hours in a year, not counting leap year. That's 24 hours more that you don't get paid for. That doesn't happen for another year or two, so we won't worry about that.

If you divide a million dollars by 8,760, it works out to be $114 per hour per million. If you're a 100 million-dollar company and you're out for an hour, you're losing $11,400 in revenue. Does that seem reasonable? And then just multiply that up by your revenue. If you're a billion-dollar company, wow, you lose 1.1 million an hour for not being available. If you're a four billion-dollar company ... You can see how this works out.

Usually, the challenge is that we're not out for just an hour. We're out for more than that, aren't we? Especially if it's unexpected. Storage goes out, you're down for 10 hours. It's not like we're just rebooting a virtual machine anymore. There's some serious cost to this. So by using this factor, you can calculate the value of protecting your assets and making sure your system is up and running.

Now, if you're an 8-by-5 operation, it gets even more intense because we're packing all that revenue into a much shorter period of time. If you're an 8-by-5 operation, divide your annual revenue by 2,080. You might recognize that number. It's the number of hours you're paid on per year. That's 52 x 8 x 5. If you divide a million dollars by 2,080, it ends up being $480 per hour. That's pretty intense, isn't it? So if you're a 100 million-dollar company and you're down for an hour, you've lost 48 grand in revenue potential.

Now, of course, this doesn't take into effect things such as what it cost to clean it up or the lost customers because they have selected the next vendor in the Google search. But it's a great place for you to start the conversation. My suggestion is stop talking to your executives about nines. Nines means nothing to your execs. Start talking to them in a revenue-per-hour loss, and you'll get their attention. And it's a whole lot easier for them to write checks to help you protect data when they understand that if the data's not protected, what it costs them in revenue per hour.

The person to have the conversation with this about is twofold. One is the COO because they're responsible for PNL, and the CFO because they're responsible for cashflow. Cool? Is this helpful? Very good. I want to give you some stuff that you can go back and use immediately to have intelligent conversations. Of course, that information is all right there in front of you. Next, let's find out why we might have data unavailable. What are the reasons for loss? This is the list of the top five reasons. I've given you the URL there so you can go back and run that to ground if you want.

40 percent of the reasons is hardware systems malfunction. Now, how do we handle that? Redundant systems, raid sets, dual networks. That's how we handle all that stuff if it's valuable enough for us to keep it up and running. But notice that's only 40 percent of the reasons why we lose data. Quite frankly, 40 percent of the reason why you lose data, for the most part, is under your control in that redundant situation. The rest of it, not so much.

Next is human error, 32 percent, including device loss and theft. All right. Who here has dropped a table on a database? Come on. Admit it. I have. That's a little human error or loss. You forget your device or somebody breaks into the car and steals it. There's a lot of interesting situations that a third of the reason why we lose our data is because of our people. So you gotta protect against that.

And then software corruption, 15 percent. Anybody lost data because of a software release that did a bad job ... Yeah, right. All of us have. We've all had that experience. Next is viruses and malware, just 10 percent. The reason why is we do a pretty darn good job looking after that. We have our Norton Utilities if you're still using that stuff. We have a firewall if you're smart. We don't click on those emails that we don't recognize or those commands from the boss that look like, "Why are you doing that?" That still happens, I know.

And, interesting, natural disasters only three percent of the time. We build two data centers to cover natural disasters, and that's only three percent of the issue. But notice that the biggest issues here, for the most part, are humans. That's the biggest issue that we face when it comes to data protection and data loss. When you build your security policies, it's not just about preventing bad actors. It's about every potential thing that could cause you to lose data.

You have to have a holistic approach to protecting your assets, not just a firewall. It's not enough. We have to have much more than that, and that's why I wanted to present you with these fundamental five so that you make sure that you are covering and taking advantage of the assets that you have available to make sure that you can have a business that continues and that you don't have those losses. So far, so good? Anybody need a cocktail? I'm way better when you're drinking. Yeah.

Let's take a look at some key security outcomes, and this is directly out of my book. There's four fundamental things that we're looking for. Number one is keeping confidential things confidential: confidentiality. We want to make sure

that the trade secrets or client data, the things that could give our competitors an advantage or it could be that gives our competitors what they need to succeed, those are all protected. Number two is integrity. We don't want people changing the data on us. In my opinion, data integrity is the biggest potential forthcoming issue.

As we move more and more into the intranet of things, spoofing of emails, getting bad data or the wrong data could steer us the wrong way. Hey, we just saw that recently with Hawaii getting an early warning for a nonexistent missile. That's a good example of bad data integrity. By the way, have you seen the picture on the internet of that guy that was responsible for that? His password for the system was on a sticky note on his monitor. How dumb can this be?

Now, you're sitting there thinking, "Oh, that can't happen to me." Oh, it happens to you all the time. You gotta change this. I'm going to share with you some strategies that I suggest that we look at as we move forward. Isn't that crazy? Anybody want that picture that you can share with your team? I'll get it to Sue, and then she'll send it to you. Okay? Dude, it's true. We got the picture zoomed in, right? There it is. The craziest thing. All right.

Number three is availability. Obviously, we've done the calculations. If the data's not available, you're out of business. So we have to have that covered, and then the last one is accountability. I want to make sure that people are treating the data appropriately. So we need to be able to track what people are doing and hold them accountable for what they do with the data. As you build your security policy, as you review your security policy, you need to make sure that these four elements are part of your security policy.

Now, you're probably just a little bit surprised that I haven't really been digging into things such as malware. You might have thought that I might have been coming up and telling you that we have to protect ourselves from intruders and all that kind of stuff, but maybe that's a little bit of bait and switch. The reason why is because that's only 10 percent of our issues. I need for you to consider all these issues to make sure that your assets are secure.

Let's talk about the seven layers of security. Consider this to be the seven-layered dip of security. We start off with a layer of beans, end up with a layer of cheese, a little avocado underneath that, sour cream. You're getting hungry, aren't you? The steaks are coming. The seven layers. First of all is access control. We have to decide who gets access to what. Obviously, if we have a website, we want everybody with money to access that information. If we have trade secrets, if we have personally identifiable information, we want that to be not at all.

Next is we want to deter people from trying to get access to things they're not allowed to get to. For years, we've been using things such as password, user ID and password. Of course, that's not terribly secure anymore. We've added two-factor authentication. Now we're moving into more biometrics. I think that we're going to be seeing some really interesting and novel ways of deterrents over

time that are a combination of invisible biometrics, such as facial recognition, as well as behavior, how you type on your keyboard, and taking a look at those elements that are ... Well, because we all type in a slightly different signature, and we can actually measure those things.

So it'll be a combination. Is it your face and is it your fingers on the keyboard? It's going to keep you from drunk texting. Is that an advantage, do you think? Might be.

Mark S A Smith: I can't understand you. You're slurring. Siri, would you quit slurring? Okay. Number three is we gotta detect. If they get through those two layers, we have to be able to detect very rapidly anomalous behaviors. A lot of that's going to happen coming out of artificial intelligence. AI is going to help us a lot with identifying those unrecognized patterns. Of course, that happens on a regular basis with some of the more popular applications.

Next is, if we do detect something, we have to determine the level of intrusion so that we can apply the correct response. And then after that, we have to do everything we possibly can to delay their access to the good stuff while we can send in the troops or shut things down. And then we have to defend whatever is left there, and then afterwards, you gotta clean it up, so recover. Those are fundamentally the seven layers of security.

My suggestion is that you spend time, when you're protecting your assets, looking at all seven of these things. Otherwise, you're going to be in a cleanup nastiness that's going to really cause issues and provide downtime. Next, let's talk about why security breaks down. Number one on the list, abdication of responsibility. Who agrees with that? Yeah? Whose responsibility is security?

Audience: Everybody's.

Mark S A Smith: Everybody's. Everybody's got to be responsible for it for the reasons that we've listed. Since 32 percent's going to be human error, a third of the time we gotta make people personally responsible for what's going on. Gotta do it. And the sooner that we do it, the more secure we will become. Abdication of responsibility has got to be turned around.

Next is lack of security education. Who sees that as an issue in your organization? I know. Isn't that crazy? Yeah. Security education probably is the most important thing you can do because of its impact on everybody. There's a couple of little quotes along here at the bottom of this page. It says, "Security is everybody's job. To not take seriously protecting our assets means you don't value your job and it's time for you to go." It has to be at that level.

The reason why is because people that don't take your security policy seriously are a substantial business risk to your organization. There is a particular phrase for that. You've probably heard of it. It's called conduct risk, and it is going to be the next big thing, specifically in the financial sector. There are consultants that

are now in the business of identifying and rectifying conduct risk, which includes the capacity of firing people that are unwilling to adjust their conduct, because it's 30 percent of our issues comes from conduct.

Next is unenforced security policy. Anybody see that happen in your organizations? Somebody has to be the bad cop in your company. If you can't do it, Sue can. It's okay. We can break up with people. We can show up and say, "Here is the security policies that you are not enforcing. It's no longer time for you to be here. Goodbye." We can do that if you don't feel like you want to do that. Next is out-of-date security policies. Who sees that as an issue?

This one is really, really going to accelerate because as we bring on more and more mobile devices, as we bring more and more intranet of things online, there will be more attack surface available for people to mess with our data. You have to keep looking at your security policies to figure out where a potential attack vector is. For example, anybody here familiar with the Amazon dash button? Anybody here familiar with that? Do you have some? Yes? All right. Great. Fantastic.

For those of you that didn't raise your hand, let me explain to you. A dash button is a little device. It's about this big. It's about the size of a piece of cheese, about the size of a shrimp, and it has a logo on it and there's a big button that's a little smaller than a quarter. You stick this thing up where you want it, like, for example, the number-one button ... Or let's say the number-two button with Amazon is for Tide pods. So you stick it up by your washing machine and when you run out of Tide pods and you throw the last one in, you push the button and you get a refresh show up the next day automatically. Voila.

If you push the button because you're out and then your spouse pushes the button because you're out ... Not likely. You only get one package come in, so they figure this stuff out. Number one is Charmin. Yeah. And number two is Tide pods. The reason why is because not only can you order laundry detergent, but you can order snacks for your kids. This thing is an intranet of things. It's logged to your particular wireless point, and that is a potential attack vector.

What does that mean to your corporation if your people are bringing Amazon dash buttons on and putting them on your access point? Are you watching for that kind of stuff? This is just the beginning, friends, and that's just a simple example. So out-of-date security policies. We have to keep things like that in mind. Next is incomplete security policy. So you just don't have everything covered, as I've pointed out, and the reasons for loss and those seven-layer security. You need to make sure that your policy is up to date.

Based on the number of hands raised, I would say the next thing you need to put on your action idea list for Monday morning is to review your security policy. Gotta take a look at that bad boy. Let's move to the top of the next page. If the value of cheating is high and the risk of getting caught is low, there is a 100 percent probability that someone is cheating. That is the number-one threat: the

opportunity to make money the easy way, and that is the thing that drives most of us from an outside-attack standpoint.

Now we're moving into the bad actors coming in and potentially attacking our property. The key threats ... Number one is inattention. People are just not paying attention to what they're doing. That's why fishing works, why spear fishing works, is because people are just moving too fast. They have a thousand emails and they do not have the attention they need to make sure that they're getting the right answer. Number two is greed. People see an opportunity to collect a $100 gift card and they give away their information, and voila, we have been attacked. It's amazing what people will give you for $100 that you don't really get.

Number three is social engineering. Who here has a regular anti-social-engineering training with your team? Anybody here do that now? You do. Yeah. All right. That's important you do. Excellent. You have to do that. You have to teach people about the strategies that others are using to get in and get access. Next is unprotected or ignored devices. We talked about the Amazon dash button is a good example, or mobile and wireless access issues. I have a suggestion for you: do not use public WiFi of any flavor, of any kind, anywhere, especially on airplanes.

Come on. Somebody's out there sniffing your WiFi pack as you're surfing your corporate intranet. Unless you've got a VPN and you got it wired up and it's working perfectly, don't use public Wi-Fi. Just either wait or use your hotspot. Now, the hotspot is at least an order of magnitude safer. Doesn't mean you can't be sniffed. It's just a lot less likely. Any moron with a laptop can snort your stuff off the air if you do not have the security enablement that you need to have. Most morons don't have it. That's part of your security policy.

Next is printers. Thank HP for being here with the printing. Printers are an attack point. If you don't have a secured printer, somebody can walk in like they're cleaning your office and they can plug a USB port into your printer, and they can update your firmware and start shipping out your images to another server. Unless you have a really good system, you may not detect that. There's a lot of really weird stuff going on these days. You just have to be aware of that and understand the tools and the methodologies to lock that stuff down.

Bluetooth is a real issue these days. Damn Apple with this device here that we pay an enormous amount of money for has decided that Bluetooth staying on is a really, really good idea. Why?

Audience: They want to know where we are.

Mark S A Smith: Beacons. They want you to be able to Bluetooth to the beacons so they know where you are and what to offer you and all those other interesting things, because it improves location services. A lot of location services these days are run off of Bluetooth beacons. But the problem is it's an open channel directly

into your device. And so Bluetooth could be a really interesting issue. If you do not have the policy set correctly on your executives' devices, they can be compromised through no fault of their own, but just the policies are not being enforced and watched.

Alrighty. Next is USB ports. Who has their USB ports wired down, locked down, you put superglue in them so people can't put things into the USB port? It's a massive hole for a lot of organizations, especially on older machines. Yeah. We'll get to that in just a moment. Next is web portals. If you use web portals to access your corporate data, I can get access to your corporate data. Here's how I do it. I send a young man in. He's very nice. He's very polite. He's well dressed.

He walks in and he says to the person at the front desk, "Hi. I'm here for an appointment with ..." and he names a name he pulled off your website. "But before, I really need to use the bathroom. Can you tell me where the bathroom is?" They direct him to the restroom. He goes inside there and he dawdles around till he's the only person in there. Then he lifts up the ceiling and he drops a little box about the size of two decks of cards up in the ceiling.

Then he walks out and he holds his stomach and he walks out and says, "I'm going to have to come back. I can't do this interview right now," and he leaves and he walks out to his car. That little device, which is battery operated and randomly turns on and off with random signals, is going to pop on and it's going to disrupt the wireless access to the web portal. It's going to pop up an identical version, and there's going to be one or two people in there that say, "Oh, damn Wi-Fi just took a hit. I gotta log back on," and you'll never know it. You will never detect it.

100 percent success cracking web portals with that methodology. That should scare you to death. We can be in there, we can be surfing around and it can be years before anybody detects that's what [inaudible 00:31:21]. What does that mean? It means you have got to really be careful how you qualify who gets on your web portal and who has access. You have to lock it down to the certificate on the device that you have issued. If you don't have the device level for certification, you are vulnerable to that, and it's not a matter of if. It's a matter of when you are valuable enough to somebody else to get access to your corporate web portal. That's what it takes. You gotta be careful with your web portals.

Next is old hardware. There comes a time when that hardware is out of support life, and you have to start keeping it running by buying parts off of eBay. You've just been hacked. You buy stuff off of eBay, you plug that board into your server, you have just been compromised, not necessarily by the person who sold it to you, although it sure could be, but by the people that haven't updated the firmware on that thing you just plugged in. You just cracked open a great big hole.

There's a reason why you want to roll over your hardware every three to five years, period. Three is better than five. It's because of security. Forget the

money. I guarantee you the cost of a cleaning up from an old-hardware hack is going to be superseded by the value of replacing that. And then the last one is doing backup on production hardware. Why do you not want to have your backup system on production hardware? Why is that a really dumb idea?

Audience: Because it can be hit by ransomware.

Mark S A Smith: Right on. You're on the production network, it's going to be hit by anything that can hit the production network. Your backup system needs to be independent, and it should not be administered by your regular admins because 30 percent of your problem, 30 percent of your problem is human error. You need your backup systems to be a completely separate organization that's a completely separate system. Otherwise, the morons are going to make the same mistake that took you down on the backup and recovery system. That's what happens. They're morons. Otherwise, they wouldn't do that.

So far, so good? Everybody getting some ideas you can use, some ideas you can take back and scare people with? Good. We have some upcoming threats, and I'll share those with you. Number one is cloud-based attacks. We're already starting to see that. There's a Microsoft 365 attack where we can ransomware your Microsoft 365 deployment if you don't have things just right. It's potentially ugly. You better have that ... Sue's shaking her head. She's aware of that. A lot of people aren't aware of it, but that is the beginning of a really bad trend. Really, really ugly trend, which means that education becomes more important than ever before.

Next round is social media applications. As much as Twitter and Facebook has been in the news about bad acting, you haven't seen anything yet because the people that the millennials are going to jump to replace them are going to be worse. One of the issues with millennials ... I have five millennial kids. I raised five millennials. I'm a successful dad. You know how I can tell? Nobody lives at home. It doesn't mean we don't subsidize rent. But the problem is that if they move back in, then we're cooking, we're cleaning, they're sleeping in and pissing us off. At least if we subsidize rent, we don't have to do any of that stuff.

We only have two kids that we have to subsidize out of five. It's okay. It's going to end soon. I don't know how they do it. They're paid nothing, and their living expenses are really high. It's crazy. All right. The next round of social media, I think, are going to be a really interesting challenge because what happens, of course, and you've seen this, is on social media people are running these quizzes. And what are the quizzes about?

Audience: Your high school ...

Mark S A Smith: Right, your typical challenge questions. It's the typical security-challenge questions are what the quizzes are asking for. And the bad actors are harvesting this stuff and then selling it. Bad news, friends. Your challenge questions no longer have any security capacity whatsoever. Bad news. You gotta change

security challenges to something that's more biometric. How many fingers am I holding up? No, that won't work either.

Next is 5G deployment and application. Who here is familiar with 5G? Anybody here familiar with 5G? Okay, good. Just as a quick review, 5G is the next generation of cellular communication technology. It is going to provide gigabit to the device. 10,000 devices on a single cell, self-healing mesh network. Here's the challenge. How big is your pipe from your data center to the internet? How big is it? 50? So how long is it going to take for us to burn up your 50-gig bandwidth pipe when we have gigabit to the device?

How long is it going to take for us to overrun that bad boy? Not much. Your big, fat pipe right now is going to look really teeny like a little soda straw really soon. Remember, 5G already exists in three markets. It'll be in 100 markets with two carriers by the end of the year. Verizon and Sprint both rolling it out today.

Audience: Seriously?

Mark S A Smith: Seriously. That's why you come to these kind of events, just to learn this stuff. Like, seriously. Why is Sprint and Verizon rolling it out early? Because they want first dibs on people buying that bandwidth. Millennials are going to switch wholesale to 5G. They're going to give up on Wi-Fi. The reason why is because sub-millisecond ping and fast no matter where the hell they are sitting, which is not connected to their Wi-Fi at home.

When that happens, we're going to open up a whole bunch of apps that are going to take advantage of that bandwidth, and those apps will not be secure. They'll not be as secure as you want them to be, and it's going to open up a whole brand-new set of attack vectors that are going to cause us challenges. Who here is thinking about retiring based on some of this bad news I'm delivering right now? Okay. On the other side of this, who sees massive amounts of money that can be made when you incorporate this correctly into your organization?

First movers are going to dominate 5G. Most organizations haven't even got this on their radar. It's going to catch a lot of companies by surprise because they won't be able to move fast enough to keep up with their competitors who already have this on theirs. So you just put that on your list of things to look at on Monday, right? How are we going to handle 5G onslaught? All right, good. That means I've done my job.

And then the last thing we've already talked about is the intranet of things I see, massive coordinated biotechs, because these little devices are not secure. The security on them is just absolutely nominal, so you have to be very careful about isolating anything that you're using to collect data from the intranet of things on a completely separate network that then aggregates data and then ships that securely to your production network. They have to be radically different.

Now, I want you to understand this. 40 percent of the intranet of things right now uses LTE to get data back. What percent do you think is going to use 5G when it becomes available? 100 percent. 5G is designed for the intranet of things. That's why there can be 10,000 devices on a single cell. That's what they want to do. 5G carriers want to be the hub for all things data, and that opens a lot of really interesting challenges for us, really interesting stuff, my friends. You just gotta have that on your radar.

Next, let's take a look at some key protection strategies. Number one, top of the list, is a culture of security. That is the number-one best possible thing that you can do that has the longest sustainability and scalability, is you've got to turn security into part of your culture. It kind of feels a little big brother-ish, but it's the only way we're going to survive. It is the only way. So how can you pivot your culture to make security top of the list? Because, quite frankly, if you don't have security at the top of the list, your customer service doesn't matter. Your value doesn't matter. Everything else doesn't matter given the face of what we are looking at today and the threats that we're facing in the future.

Number two is nonstop education. How much time do you spend training your team on products? You need to double that for security. Security is going to become a brand value. If it isn't already, it will become a brand value for your organization. Next is routine security policy review. You gotta make that thing part of what you do on a regular basis, and at your quarterly policy review, routine the security policy testing, which you're doing right now, you have to continue to do that. And then take a look at how you move into using biometrics and facial recognition as methodologies for securing your devices. We've got to get away from passwords and user ID. That's got to go as fast as we possibly can.

Traditional ways of securing things is what you know, user ID and password, what you have and what you know, which is two-part authentication, using your cell phone as a device of what you have. But next, what we're going to really have to look at is who you are and what you know. Your personal physiology, whether it's fingerprints or facial scans, that combination ... And probably what we're ultimately going to go to is three-factor: it's who you are, what you know, and what you have. And then we're going to add other things to that: where you are and when you are.

The more of those factors we can bring into play, the more secure we can make our systems. My suggestion is, as you create your policies, look for methodologies that you can add more factors that are as invisible and frictionless as possible. The more friction that you use to implement security, the less likely it is that people are going to do that. The next is Blockchain. Who here is familiar with Blockchain? All right. Good. Do you have a strategy for incorporating Blockchain into your organization?

If you don't, get on it now. Blockchain is way, way more than cryptocurrency. That just happens to be the most popular application for Blockchain. Just to do a quick summary, Blockchain is the concept of a distributed ledger, which makes it

easy to secure intellectual property and information, and it makes it extremely expensive to hack it. That's the fundamentals. It is radically going to change e-commerce. It's going to radically change how we identify and prove ownership.

If you have the word "broker" anywhere in anybody's title in your organization, you will be disrupted by Blockchain unless you have a strategy for using Blockchain to disrupt yourself. If you do not eat your young, somebody young will be eating you. Just as a side note, I work with a Blockchain startup lab, so I'm doing everything I possibly can to understand it from a strategic standpoint. I am doing an event in Las Vegas on how to develop a Blockchain strategy, not crypto, but a Blockchain strategy. If you'd like to find out more about that, I can tell you about that.

And then the last one is third-party audits. The reason why is you have to bring somebody in who's going to ask you the tough questions that are going to make you squirm. Now, my job here is to make you squirm at least a little bit, because if you're not squirming a little bit, you've gotten too comfortable. And if you've gotten comfortable, you are an attack surface. Whoever's job is responsible for security needs to be very paranoid until they go home.

To wrap this up, I've got a couple ideas for you. Here's seven security questions that I suggest that you ask everybody you run into. Number one is, what do we need to secure and why? You don't need to secure everything. You don't. There's some things that you just want to insure. Forget about securing it. It's okay. It's not too expensive. It's easy to replace. If I can order it from Amazon, don't bother doing too much security on it other than lock the door.

The four things you want to look at is people, property, processes, and proprietary data. Those are the four Ps of what we need to protect. Make sure that you're looking at all of those. Number two is, who is responsible for securing these assets? You need to really drill down on each one of these. Somebody must have a fireable offense protection for securing those assets. It's the only way that we're going to get things secured.

Number three is, what is our policy for securing these assets? Make sure that you have a policy around that. And then number four is, when was our policy last updated? The answer is probably going to scare you. Number five is, when was our policy last audited? That's probably going to scare you as well. Now, the thing you have to keep in mind is if you have a customer sue you because of some data loss and you are taken to court, one of the first things that the suing lawyer is going to say is, "Do you have a security policy?" If you say no, you just lost the case. You'll be found in negligence, which of course means triple damages.

The next question they're going to ask is, "When was it last updated?" "It's been a couple years." Negligence. "Audited?" "Hasn't been." Negligence. The fundamentals, here, my friends, are you gotta have a policy in place, updated and audited, if you're going to have any chance in hell of surviving a court case

around data loss. And then what happens if they're compromised or destroyed? That gives you a cleanup plan. And then last one is, if there's a breach, what will it cost to clean up and who's going to do it?

Those questions should at least help you scare some willingness to take a closer look at security in your organization. The last thing I want to leave you with is the best attitude to security is the golden rule: protect our assets just like you'd protect your life savings. With that, I'd like to check in with you, my friends. Best idea from our conversation today, just shout it out. What's the best idea that you can use to go home and say, "I'm sure glad I hung out with HP and Prime Edge today?" Just shout it out. Best idea.

Audience: Protect our assets.

Audience: Developing a security culture.

Mark S A Smith: Culture security. Gotta do the culture security thing. Without that, all your policies won't matter. Other best ideas? Just shout them out.

Audience: Holding people accountable for their roles.

Mark S A Smith: As accountable as if they had stolen money. If they don't need protect the assets, it's letting somebody else steal the money, so they're accountable. Good. Other ideas, best ideas? Shout them out.

Audience: No public Wi-Fi. You know that, that you don't ... Just think about it. I mean, you hear it. You don't think about it.

Audience: I have a question about that. Would you recommend a VPN?

Mark S A Smith: My suggestion is a VPN as long as it is absolutely transparent to usage. Otherwise, they'll stop using it, and since they're using Wi-Fi as part of their habit, if the VPN goes down, they're just going to bypass it and they're screwed. The issue is, unless they can use the VPN for everything, including doing Facebook, it's not going to provide the protection you need.

So my suggestion is hotspot, unless you have an absolutely dead-solid VPN back there that they can get to any URL that they want. Make sense?

Audience: Yep.

Mark S A Smith: Okay. Great. Best idea? We got time for two more.

Audience: Changing your culture. That's a big thing. Changing your culture to security is ... I mean, it really takes that in order to make your whole organization secure.

Mark S A Smith: Because your company is as secure as your least security-aware employee. With that in mind, my friends, thank you for sharing your time with me to share with

you some of my insights. It's a delight to hang out with you. Hey, I'll be here all night. Thank you very much. Thank you. Thank you. Anybody have questions before the steaks come in and I fill my mouth with dead cow?

Audience: What does Martech stand for?

Mark S A Smith: Martech is actually marketing technology. Yeah. Marketing technology. The idea here that Scott Brinker is a Martech expert, and he's the guy that pulls together the survey of all the companies in the world that are selling marketing technology, which is things like HotSpot market ... And, by the way, Scott does work for HubSpot.

What he observed is that people's ability to adapt marketing technology is really constrained by their ability to change that. I'm applying it to technology in general. It still flies across the board. I did have the opportunity of interviewing Scott Brinker on my podcast. My podcast is the Selling Disruption Show. It's about three shows back. It's absolutely worth it. We talk about how do you prevent being disrupted by Martec's Law?

I'll give you the number-one thing that I got out of it, and that is you can't. But don't ever waste a crisis. Anytime there's a crisis, it's an opportunity to close the gap. Other questions?

Audience: You mentioned Moore's Law and you mentioned Martec, but you mentioned another law.

Mark S A Smith: I did. I mentioned Metcalf's Law. Metcalf's Law is the law of the value of the network. The Metcalf's Law says the value of a network grows exponentially by the number of users. The reason why Facebook is one of the most powerful companies on the planet is because two billion people are part of the network.

So the more people we can get on our network, the more valuable our network becomes. The concept is that as we look at value-creating platforms, the more people that are on the platform, the more valuable the platform becomes, which is why Uber is worth billions. It's because of the number of the people on the platform. So that's Metcalf's Law. That helpful?

Audience: It is.

Mark S A Smith: All right. Good. Other questions?

Audience: To continue education in security, do you recommend that we do that ourselves as a company, or should we bring someone in?

Mark S A Smith: The answer is yes, and ... So the answer is yes, it needs to be internal, and yes, it needs to be external because you're going to get two different viewpoints. The "and" is everybody gets to lead security classes on a regular basis. Everybody

stands up and is the security trainer on a regular basis because what you want to master, you teach.

So from the most junior employee to the most senior employee, everybody gets to teach an aspect of the training class on a regular basis. It's the only way you can inculcate it in the organization. Is that helpful? I hear sizzling steaks. Bring it on.

Waiter: That is correct.

Mark S A Smith: This gentleman is going to say, "Don't touch the plate."

Waiter: Don't touch the plate, please.

Mark S A Smith: All right. Thank you, my friends. It's a delight to be with you. There's all kinds of stuff on the back: how to get ahold of me, also ways to learn more about the other things that I do. Thank you to Sue from Prime Edge for inviting me in. Thank you, HP, for buying us steak and giving me the opportunity to share my time and efforts with you. Let's enjoy, and let's make sure that we live a secure life. Yes. All right. Thank you.