accenture

ACCELERATING OUR NATIONAL CYBERSECURITY STRATEGY

VIDEO TRANSCRIPT

Susan Lawrence:
Thank you, Ben. I love being back here at home in San Antonio with this great team here. It's good to see you all, and thank you to all our guests for being here today. I'm especially excited about the topic that we're going to talk about, and that's that cyber poverty line which I lived with while serving in the Army. And we continue to find the right solutions here at Accenture Federal as we move forward. And so with me is our guest, Mr. Gus Hunt, who leads Accenture Federal's cyber strategy for us and most recently served in the government as the chief technology officer for the CIA, so someone that's truly qualified to help us lead this effort across as we go forward.

00:00:56
As I was talking to Gus Hunt earlier about the cyber poverty line and what it means, it is something that I think we as a community have to tackle soon and put our resources towards. It's an environment of have and have nots, as we think about who can afford to do the cyber work at the level it needs to be done and those organizations that do not have the resources. And we all know we're only as secure as our weakest link as we go forward.

So let me give you just a couple statistics as we go forward on this. In 2018 a report from the Office of Management and Budget and the Department of Homeland Security found that three out of four—three out of four—federal agencies have cybersecurity programs at risk today, and a 2018 Government Accountability Office report found that federal agencies have not yet implemented roughly 1,000 recommendations that were put forth to federal agencies to help improve their security posture.

00:02:00
And as a past CIO G6, I think about that and I remember getting these mandates and these instructions to go do these things. But when you live inside of a budget process that is already expended, how do we find the ways ahead as we look at this? So we're very excited about the work that Gus Hunt is doing for us in this area. And he recently wrote a paper discussing the cyber poverty line. So Gus Hunt, let me just start by asking how bad is it?

Gus Hunt:
Well, in my book it's actually really bad, and it's getting worse as things go ahead. And the reason

for this is pretty straightforward. If you look at what's really been happening in the cyber world, particularly cyber attacks, the adversary has learned that they don't have to attack you directly to be really good. What they do is they attack you through somebody else who you do have a business relationship with. And this first emerged through the Target HVAC vendor relationship several years ago.

00:03:01

But just most recently the penetration of the electric power distribution control grid, which is an air gapped environment, was a result of the fact that the adversary, a nation-state, went after their third party support vendors and inserted malware into their equipment they use to do maintenance, and then when they plug their equipment into the air gapped environment, that's how they manage to jump the air gap here.

The Mirai botnet is another classic example of something that has emerged, particularly in the world of IoT, which is that people who don't secure their equipment, particularly Internet forward-facing equipment, very well is now resulting in these massive attacks by assembling millions and millions of these devices together, IoT devices together to go try and take things down.

And then if you think about it from a DOD perspective here, you've got things like the MUDCARP report that we recently issued where the attacks were not directly at the Navy, the attacks were through the people supporting and doing research for the Navy.

00:04:01

So while the Navy may be really harmed, the third parties doing the work, they discovered, were the weak points, and they were able to get in there and do that. So you're going to see this trend, I think, continue. I think it's going to push really, really, really hard. Our adversaries are going to push really, really hard down this pathway.

And it's something that, as you had mentioned, that we have got to figure out how to address together. We have to stop fighting cybersecurity as an every man for himself battle. This is where I think we are failing miserably as a nation and as a globe. We have made this every individual, every individual company, you name it, has to do this on their own, and we have to get to solutions that solve that problem.

Susan Lawrence:

Yes, I like that. In fact, you made a reference to the devices on the Internet of Things. Gartner just recently released a report where there's going to be, they're predicting, over 20 billion devices to be connected on IoT by 2020, so you already are recognizing a problem. How are we going to go after something at that magnitude?

00:05:02

Gus Hunt:

Well, so first off, that's the thing that scares me the most, because what's going to happen is that while there's roughly seven billion connected devices prior to IoT that were out there, now we're talking 20 billion by 2020.

Susan Lawrence:

Yes.

Gus Hunt:

There are people that are predicting by 2025, 2030 there may be 700 billion of these devices out there. And what's happened is that the manufacturers—all around the globe manufacturers—this is a big rush, this is the big gold rush, right? So make something spark means make some money. So if I have my Internet connected toaster so that I know when my toast pops up and it's ready and it's done while I'm blow drying my hair in the morning or whatever it's going to be, I can go down and take care of my toast while it's still hot, right?

Susan Lawrence:

Right.

Gus Hunt:

So you're going to see this emerge everywhere. The problem is security is an absolute

afterthought into these devices, and so the more of them that are out there, the more that can be connected, the more that you can do destructive, damaging things. And they also provide the gateway in to our adversaries.

00:06:00

So how many guys heard about the fish tank attack in Los Vegas? Okay. A classic example. The Internet connected fish tank—why the fish tank had to be Internet connected is a great question you can ask yourself, but okay—was the avenue of attack into casinos. So then you go straight at casino security. They went through the fish tank, and the fish tank maintenance guy, and that's how they got in. So this becomes the—this is going to become the primary avenue of...a primary vector of attack that people are going to take advantage of.

And you asked the question how we solve this. So this is really interesting. One, of course, is that you have to have the people that understand how, when you install and use these devices, to set security. But two, I also think the manufacturers themselves are going to have to step up in this case. And then three, I think we need some form of an Underwriters Laboratory for IoT devices. I don't know if you all know the history of Underwriters Laboratory, but they came into existence because electricity was going to houses, and people were building electrical devices, and a lot of them were not well made and having a lot of fires.

00:07:04

So the UL label went on as a device that was made properly, and it was all these other things like that. I think you'll need the same thing on IoT devices, that somebody has done the basic security on them, the security is good, when you go to buy them you can trust the label, and now you have confidence that what you've got is appropriately built, secured, and delivered.

Susan Lawrence:

You bring up two very interesting points there. I remember meeting with Dr. [Vince Serve] 00:07:26 at least six years ago, and he was predicting that each of us would carry on ourselves, you know, 50 sensors. And I thought, really? But think about today. Everything you're carrying on yourself is a sensor, and you are now connected to that Internet of Things. And so how do we build in that security as we look at that piece of it? Because at CENTCOM, where George and I served, we looked at over a million intrusions into our network every day, and as you started working it down as to where then our vulnerability came, guess who, the majority of the time, where our vulnerability was? The human.

00:08:03

Gus Hunt:

The human. Yes, of course.

Susan Lawrence:

The human. So how are we going to address this?

Gus Hunt:

So human error is one of the toughest things that we're always going to deal with. Let's just say that with education and with training, and with constantly putting the need for people to think securely, be secure all the time in front of them, much like what happened in World War II, right? There used to be, remember—I wasn't that old yet—but they used to have a sign, "Loose lips sink ships." What we need are signs that basically say "Loose clicks sink ships and everything else." Because fundamentally it's just that constant reminder to people.

The other thing is that we've made it too hard for the average person. And this goes back to my earlier point. If we are going to rely on everybody individually to make things secure, we are in... it's not a solvable problem. So we really have to think about how we're going to go at this and we have to create environments, and we have to build systems that themselves are smartly built.

00:09:05

They abstract away from most users the responsibility for security because they actually provide as much of it as they can. You can still click on stupid links, but these are things that we can

deal with. And you have to build your systems to be cyber resilient. And that's the big push that we've got going, which is that the way we currently build our systems today, they're not cyber resilient.

So I don't know how many of you have suffered a cyber attack, but if you ever had one, what's the result? You've got to turn off all your systems, business comes to a stop, all the revenue ceases across the board, the mission stops, in the case of government, and everybody all hands on deck to fix the problem.

Today we possess in our hands the technology to build truly cyber resilient systems. And when we talk about it, when I talk about cyber resilience, what I mean is the ability to take a licking and to keep on ticking, to steal a phrase out of the old moonshot era from Timex. But it really is lessons taken out of the Bible of cloud technology applied in the cybersecurity realm that allow mission and business to continue to operate despite suffering an adverse cyber event.

00:10:07

We know how and we can deliver and build systems that are designed and built to work in this manner today. And this U.S. IT modernization, right? So as the government looks to modernize the systems going forward, one of the key things I think that they need to do and that we, as their support folks who are building these things for them, we really have to take into account that we're going to build them to maximize cyber resilience as we look to the future.

Susan Lawrence:

Yeah, that's very important. We're working with a new client and they didn't ask for a capability, but we have worked with them since and said look, you have to bake security in from the beginning, and we all understand that. So the government is more and more looking at small businesses because of their niche capabilities. And when you look at the cyber poverty line and how much a small business can afford, is that introducing greater risk to us as we continue down this road?

00:11:04

Gus Hunt:

Yes. Well, if you really think about it, yes, that's the point about the HVAC guy at a Target, or the fish tank guy at a casino, or one of these things, is that if you look at the U.S. government, and look at DOD in particular, for example, right, I can't remember the number. It's either more than 60,000 or 6,000—I think it was 60,000. DOA has more than 60,000 small businesses, small, medium sized Mom and Pops, things like that that they have to do business with, and the hardest thing is how do you get some form of assurance of security when you have to deal with the population at large.

And that doesn't even include those that, when you think about small business set aside that happens across all DOD and all of government so that you engage with small businesses, a very, very important thing to do. But do these people actually have the wherewithal, can they afford the talent? One of the biggest issues in this is that it's a very complex space and talent, as we know, is scarce and expensive, and getting more so.

00:11:59

In fact a lot of the process of use, this every man for himself model, is, while not responsible for the shortage, certainly dramatically exacerbates the shortage because we're all bidding for the same limited talent pool and we're driving the prices up for the talent. This is great for the kids. But who's from UTSA? Anybody? These are great for your kids, kids that are now in college. You know, wonderful place to be, guaranteed employment for life. But it really doesn't, it's not scalable and it's not workable as we head into the future.

And so this is where things like managed services come into play. So that's one reason we're here in San Antonio, is we're trying to provide managed services both to our federal clients and to our commercial clients so that they don't have to worry about—you know, it's not...let's phrase it this way. It is not a core business for most folks

to be doing cybersecurity, so much like what happened in the world of the cloud, where people began to learn that running infrastructure isn't necessarily core to my business, let me turn that over to somebody else to run, right?

00:13:01

That's why at the CIA we pushed the cloud deal, C2S, things like that, is that you want somebody that does it really, really, really well. You've got to watch it very, very carefully, don't get me wrong. You don't turn it over blindly. But okay, so a similar thing is going to happen in the world of cybersecurity, is that large companies or large federal organizations with substantial resource bases and the ability to hire the talent and do these things will be able to continue on their own.

But the smaller organizations who don't have the resources, can't afford the talent, the space is extraordinarily complex, and because we're all interconnected, we're going to have to turn to some form of managed services, if you will, so that we can raise all boats, so that the skill sets now in the managed services realm, we become responsible for hiring the best talent, we become responsible for making sure that everything is kept current, we're responsible for bringing in the latest technology to help them out, but then everybody benefits.

00:13:56

And so remember like in the cloud world when Amazon patches, they run one patch through a billion servers in order to solve their problem, and they can do this very, very fast, like this. A similar outcome must happen in the cybersecurity world, which is the ability to, you know—or using the vaccination thing. I heard vaccination, right? You're not saying that somebody won't have an event. What you want to be able to do is, if somebody has an event, you isolate them off, you go do the remediation for them, but you inoculate the rest of the herd as fast as you can through the changes that you put into place inside the environment.

And these are the outcomes I think that we can drive. And this is how you're going to lift the have nots up, okay, is that they're the ones that can take advantage of this. And the goal being that they take advantage of it at a cost level that is much lower than what it would take them to do it by themselves, but they wind up with an outcome that is on par with what they...the people they have to engage with and support across the globe.

00:14:52

Susan Lawrence:

Yeah, I think that's a very important part. We heard from John Goodman that our number one resource is our people as we look at this. And I'm excited that we have academia here with us. We have an average of 150,000 computer science degree opportunities in America, but we're only graduating about 32,000, so guess where those jobs are going? So the same thing here, is how are we going to get ahead of this and get the young individuals engaged in STEM that will eventually graduate to the cyber? And so any secrets there for us as we go forward?

Gus Hunt:

[Laughs.] Well, one of the papers you can grab is one that we wrote a little over two years ago now we called...basically it was a cyber moonshot paper that we originally put out, and the premise being that we actually need to have some formal call to action around cybersecurity, much like what President Kennedy did for the space race in order to drive the energy and attention.

00:15:52

So the outcome of the Apollo moon program and things like that, the space race, was a massive re-interest in STEM education. They didn't call it STEM back in those days. That convinced me I wanted to be an astronaut, an engineer, and I wanted to do all these things like that, right? That was what my goal was. Didn't get there. Ah, funny.

Susan Lawrence:

[Laughs.]

Gus Hunt:

But it really sparked this massive interest. It also created an environment into which government

and academia and the private sector gelled around an objective in order to solve, okay? And those two things together are extraordinarily powerful. And we haven't yet gelled. That's one thing. And we have a push for STEM. I think that something like the cyber moonshot concept is absolutely essential for us as a nation to get and energize behind these things across the board. Of course it's a very different era, so we don't want to go too much into that. But that's got to be kind of the objective there.

The other thing I would say from an education perspective is that—in fact this is really important, I think, from a development/IT perspective—which is we have too long treated cyber and IT as separate pillars, and we need to bring them together into a unified whole.

00:17:03

And so that while I may have my...I may major in cyber, but my minor is clearly in IT. You guys are, I think, doing this already, right? But if I'm going to major in software development, I've got to take a whole lot of classes in how to make it and how to do it secure, right?

And so this is like, you know, the big push we have on [DEF SEC ops], right, is for exactly this reason, is that you've got to bring together business with—and we were talking about the gap in the understanding of what the business actually needs to do the job well, right? That was the maintenance guys, right, as we were talking about that. So business has to articulate the need, right? Then you've got to bring together IT. So DEF SEC ops brings together business, IT and cyber into a common set of decisions, particularly in an agile framework that allows them to make shared, coherent and transparent decisions about where the dollars are going to go.

And so now I think from the federal space in particular, we need to bring together the limited pool of resources that the federal agencies have for IT modernization and cybersecurity and begin to treat them as a common pool to which, through these processes, we can actually make the best sets of decisions about where the next dollar ought to go.

00:18:11

So if WannaCry just happened, yeah, that next sprint cycle is going to be all focused on making sure we're protecting WannaCry. But the next sprint cycle ought to be focused on delivering business needs to get building very securely in order to get that right. So it's those techniques that I think we have to have, bringing these things together, and then, from an investment perspective, it's really important for us to stop treating them as separate investment pipelines, but look at how we integrate them into a common whole.

Susan Lawrence:

There's a current debate going on today about the need for every employee to have a four year degree to be hired by industry versus maybe a trade school. Is there room here that we can develop a trade school cyber to up the number of individuals?

00:18:55

Gus Hunt:

Oh, absolutely. In fact I'm glad you raise this because this is really important. I think there's a clear bifurcation that's happening now in cybersecurity practices. One is that I don't need a four year degree to provide the basic critical cyber services. We call these brilliant basics, right? If you don't do brilliant basics right, you really are in trouble, so you've got to have people that are really good at that.

That doesn't really require a four year degree. What it requires is fundamentally you call it a two year degree. A lot of our soldiers and whatnot, you know, our enlisted people coming out through like 24th Air Force and whatnot who already have these skills, understand these things, they're ideal to do this. They just need an education framework that is very agile, adaptive and continuous for them that makes it easy for them to consume, learn and apply, given the velocity of the change that's happening in the space.

And then the other big shift, I think, is the fact that you're going to see...you're going to have to drive together cyber, IT and AI, and machine learning. In other words, these guys are going to have to come out with not just four year degrees, but maybe six, you know, PhDs, master's or PhDs, even.

00:20:01

Because the ability to apply AI really effectively in the cyber space is going to be...is hard. It's very, very hard, as people are learning. And in order to understand what's happening and what's going on you're going to have to be able to understand both sides of these things, right? So they may not be the statistics experts next to the PhD statistician that's going to understand how to do all the math, but they certainly have to understand what it means to do it. They have to be able to articulate the problem and then be able to work side-by-side with those that have that. So that, I think, is going to be the big shift in the four year degree program, which is this integration, not just IT and cyber, but the AI aspects of this as well, too.

Susan Lawrence:

Yeah, very interesting. So you meet with a lot of federal leaders, especially our clients as we go forward. Have we... What do you hear from them as their number one concerns, or two or three? And what are they sharing with you as to what we can help solve as we go forward?

00:21:00

Gus Hunt:

So you mentioned this earlier. You know, the money thing constantly comes up, okay? And I'll tread back to this just slightly, because I don't buy the money thing a lot, okay? Driving transformation is hard. It doesn't necessarily require billions of dollars of new investment. What it takes is a coherent focus and strategy that you're going to work on over a multiyear period as a journey as opposed to trying to solve the problem with a big bang all at once. I just answered that part of the question.

But the reason this becomes important is that the other things they raise, and the reason they raise this financial thing is they have this mountain of legacy apps, okay? Everybody has this problem, right? So federal has this problem, state government I'm sure has this problem, commercial has this problem. They have this mountain of legacy apps, and when they look at the mountain of legacy apps what happens, I find a lot, is they get analysis paralysis. Oh, my god, how do we even begin to get out from under this mess? All right? And what they have forgotten is that you got to this mountain of legacy apps one step, one app, one data set, one whatever at a time, and they just built up over time.

00:22:04

So the way you're going to get out from under this is you're going to get out from under it one step at a time. And this is where I believe that things like IT modernization and the great paper that David Crow wrote on decouple to innovate come into play, is that your objective in this world is to not tackle them en mass, but to begin to look at them as holistically looking for commonality across these things.

The classic—well, I hate to turn this into a me thing or anything. But when I did this at CIA, I ran application services at CIA, right? And what we did was, is we first decided how we were going to go at this mountain of legacy apps, and the first step was, is we needed to create our data lake, because—I used to have a sign in my office called "It's the data, stupid," okay? Remember James Carville, "It's the economy, stupid?" Data is the life blood of every organization, and it's got to be made accessible to the people that need it, but securely, of course, right, across the board.

00:23:02

So you've got to think about what's the step that you're going to be able to undertake and what you're going to do. And so by breaking them down into common things that you have to deliver on, you can begin to simplify the process, because the first one you're going to tackle is going to be kind of hard and complex, but once I get the access to control stuff done, and once

I get my data lake started, and my data model started, and once you get all these things, the second one then becomes a little easier because wait, I've got a functioning access control mechanism, right? I don't have to rebuild that. I just inherit that. Oh my god, look, I've got an ingestion system running to put stuff in my data lake. I don't have to rebuild that, I can inherit that. So the second one becomes a little easier. Then the third one becomes easier, then the fourth one, you see what I'm saying, becomes easier.

Susan Lawrence:
Mm-hmm.

Gus Hunt:
And so what happens is it's the getting started. The next thing after getting started, as I said, is you have to keep a focus on it. And this is a multiyear focus. So the journey, I don't think any organization can do this in under five, seven years, right? You really have to look forward.

00:23:57
You'll get your big ones out of the way, but you're always going to have this small—I shouldn't say small—you're going to have a giant puddle of other legacy apps that you're going to decide whether you want to roll.

And then finally, if you embrace the cloud, which is where I think we need to go because—in fact we haven't talked about that—but cloud is...you can think about cloud as an efficiency play. I think about cloud as a massive security benefit. If you look at cloud and the way it approaches things, and the way that, through things like elasticity and whatnot, you can turn this into a much more secure environment than you have. So build your apps to go to the cloud and then you can apply all these models. And so that's really what's got to happen inside of that space.

Susan Lawrence:
Yeah, that's very interesting. And I was just imagining, as you were talking, that you were sitting down advising the Secretary of Defense how to go after this with all of the reports that he's been handed. And now we have got to do the scorecards and talk about the ways ahead as we move for that. Is that something that... How can we convince him that we've got to do this jointly and gain the efficiencies and effectiveness across the services, if you will? And even, you know, other federal agencies that are in support of the Department of Defense.

00:25:10
Gus Hunt:
Yeah. So I left out two things from my previous answer, but this will answer that question. One is access to talent. Talent [flow] is a [shortage] problem. They complain about that. But the other is the change management, and that's what you're talking about, right?

Susan Lawrence:
Yeah. Right, right, right.

Gus Hunt:
And driving change management is really, really, really difficult in every organization that exists. And so the lesson that I learned on change management was that you'll have those that will embrace what you're trying to accomplish and want to succeed, and those are the people you engage with first.

If you have a really naysayer out there, somebody that's got their feet dug in, and they're not going to do it, butting your head against that is a losing proposition. So you want to go for what you call low-hanging fruit, call it what you want, but the fact is that once you have a success with one group, then you have success with another group, eventually the naysayers come around and say, well, wait a second, this is kind of dumb, why are we, you know, and they begin to learn.

00:26:00
And if they're issues like security is often tossed up as the single most...the single reason why I can't possibly do what we just described, right? Okay.

Susan Lawrence:
Right, right.

Gus Hunt:

It's I just can't do it. Our data's too sensitive, my mission is too this. And all of a sudden they begin to see that wait, this new world that you're building is much, much, much more secure because you have transparency into every touch of every piece of data by any individual, by any system, by any service into the environment. I can see everything that's going on, okay, and I have that absolute transparency. They're hidden away in a closet and they don't have a clue what's actually happening inside of their lab.

So dealing with it really tough. So change management, I will not kid you, that is probably the single hardest thing you're going to undertake. And you've got to remember that in the mechanism of the things we're talking about you're going to break a lot of rice bowls. And so in breaking those rice bowls you will get a massive set of resistance going forward by different folks to these things.

00:26:51

And so a classic example just from my personal past was when you're going to the cloud, we had people that ran our data centers, right? We had so much storage that there was a senior executive officer managed the complete storage environment, things like that, for the organization at large. And these are people whose jobs are going to be dramatically affected because suddenly I don't need an SCS managing storage. What I need is a really smart GS14, 15 who can work with Amazon and keep track of what's happening inside the space, and make sure our [big] buckets are all locked down and those sort of things like that. And so you really tear down what are some of the old constructs.

But you all have to remember that this is the history of IT. We are just repeating it again. I first went to work for CIA in the mid '80s. They still had tape loaders. These were men and women that physically went to the tape room, pulled out a tape, went to the IBM mainframe and mounted it so it could run, okay? Do you know how many of those we have left anymore? A big... In fact they were gone back before the '90s hit.

00:28:00

And so we go through these cycles of change constantly, all the time, and people forget that, right? And we're just at this cusp, I think, of a massive change in order to enable us both from a mission perspective to do things better, but also from a cybersecurity perspective by applying these things with cybersecurity in mind from the get-go. We can create environments, secure environments that you couldn't possibly dream of inside of your legacy data centers and all your vertically integrated silos of excellence is what we used to call them, right, so these apps that are completely self-contained and completely vertical.

Susan Lawrence:

Mm-hmm. Yeah, I recently spoke at an event and I said, you know, a lot of these problems are going to go away when the first generation X person becomes the CIO G6 of our services because they're going to look at us and go, you know, why are you even thinking that way as we go through this. I think that time is going to be important, and that generation is going to make the difference for us because they grew up living in this environment. But as you said, it's click it and... I like how you said that.

00:29:04

Gus Hunt:

Oh, yeah. Loose clicks sink ships and a whole lot more. [Laughs.]

Susan Lawrence:

That's right, that's right, yeah. I like that piece of it. So as we're going forward and wrapping up this great discussion, you all can see why we're so honored to have Gus Hunt on our team and the strategy that he's putting forward for us. So as we look back to those statistics that I started with, with the GAO report, the OMB report, what can we do from an industry side, from academia, to help solve some of these problems?

Gus Hunt:
So being a little bit repetitive, fundamentally, as we engage, you can't solve all those at once. There's no big bang approach with the pixie dust. Whose commercial was it? It wasn't Accenture. That was somebody else. But anyhow, but you all remember these things. There's no single set solution, right? So again, it's a journey. And you have to begin to address them one at a time.

00:29:56
I would go and do some sort of risk analysis/ strategy plan where you can prioritize the ones you want to be able to go after. But I would do it in a way that allows us to take each individual agency on this journey themselves to begin to decompose these things into constituent parts and services, get them into the cloud, drive them into a much better resilient state across the board, apply, bring to bear DEF SEC ops and agile development if they haven't already adopted those things so that we can get complete transparency on the spend on things like that.

And then fundamentally enable them to begin to shift the game within, as close to within the budget resources that they've already got, right? They're already getting IT modernization plus some—the federal guys. I'm sorry, if you are state guys I don't know if you get this or not. But to do that.

00:30:53
And again, what typically tends to happen in those cases is, as I said, the first one is hard, the second one is easier. And actually, you can begin to do cost recovery because it's cheaper to fix the second one than it was to fix the first one, and then things begin to snowball and begin to roll.

As far as—and then, you know, I think the big key, again, is a focus on building for cyber resilience. We need to build these things in a way that deliver an outcome that enable our missions and our businesses to continue to function despite suffering an adverse cyber event. Again I will stress that everything you need to do this exists today, okay? There's nothing out there that you don't have. What we need to do is put them together in a way that delivers resilience, right? We build these as individual separate pieces to go, right?

From the academia side, which is, I think, the most fascinating part of this thing, is that, as I mentioned before, they're all interrelated disciplines, and teach them that way, right? Enable, while people want to focus on various aspects of it, it's a requirement to get things done.

00:31:54
If you're not teaching DEF SEC ops and agile development inside of the schools and things like that, you must do so, okay? That's an absolutely essential thing that you've got to be able to do. Provide for continuing education and make it easy access for continuing education, particularly things like micro courses for, you know, like WannaCry, right? That shouldn't take a massive course, you know, it's how did they do this. And then the hardest thing, I think, in education is that they have to be extremely adaptive to the environment, which is the fastest moving technology environment we've ever encountered. And that is a tough, tough thing to do inside of an educational environment, I think.

Susan Lawrence:
Wonderful. Well, thank you. I look forward to continuing to partner with you as we solve our clients' toughest problems. So thanks for your time very much.

Gus Hunt:
Thanks, Susan. Thank you.

00:32:52
[End of recording.]