The Cyber-Resilient Enterprise
Webinar Transcripts

AJ Harris (00:00)

Good afternoon, everyone. We're just going to wait for a few minutes to make sure that we have a quorum of people who have identified their coming, and then we'll get started.

Welcome to our webinar. This is the webinar on the Digital Resilient Enterprise, hosted jointly by Calian and the Stratford Group. My name is AJ Harris. I'm the vice president of digital strategy and delivery at the Stratford Group.

I get to act as moderator and facilitator today, which is excellent because I get to pepper other people with questions and then watch how they respond. That's my favourite place to be. We're going to spend a little bit of time just talking about the agenda that I see that we've brought up here. I'll talk a little bit about introductions. I'll introduce Stratford, I'll introduce Calian, I'll introduce the panel of folks that we have today to answer the questions.

AJ Harris (00:45)

We're going to have a few opening remarks. Then we're going to talk about a number of questions related to intellectual property, related to cyber resilience and security.

AJ Harris (00:54)

At the end, I will reserve a little bit of time for some questions and answers. So, if you have questions now that you know you want to ask, please put them in the chat. If something comes up as we're talking, please feel free to put it in the chat. We will spend some time at the end covering those questions. And then we'll wrap up by 1 o'clock. So,

AJ Harris (01:12)

To begin, actually I should start beginning by welcoming or congratulating everyone on Cybersecurity Awareness Month, which is where we're in right now. That's what October is.

It's interesting to me when we talk about that, actually Cybersecurity Awareness Month has actually been around for a while. It was launched, I think, in early 2000, something like 2004. It was a US initiative launched by the Cybersecurity Alliance there. But it's interesting because the way that cybersecurity has evolved at the time, cybersecurity at that time and in the 90s, for example, was very much a

AJ Harris (01:42)

responsive type thing, it is a reactive type thing. It covers your viruses, prevent intruders out, very much something you kind of just do, much like you lock your door sort of thing.

And we've seen it evolve quite a bit over the decades since then from something that was very reactive, something that's very proactive, something that's very system focused and very much enterprise focused and employee focused as well because that's looking at all the different threat landscape pieces and the end points that we have.

AJ Harris (02:10)

It's gone from being an IT issue to a board level issue. We now have chief information security officers who are very strategic to the organization's success.

We have seen cybersecurity evolve quite a bit and it's not surprising that we spend time in October specifically talking about how we can all effectively get better at it and make sure that we can make ourselves more resilient to allow our organizations to thrive. So, joining us today, we have two organizations.

AJ Harris (02:40)

I'll start with Calian. So Calian. is a well-known organization to those of us who are in Ottawa. It's a very prominent group

AJ Harris (02:48)

with about 6,000 professionals across Canada, the UK, US, Europe, I believe, has for forty years now been delivering very innovative solutions across cybersecurity and IT, advanced technologies, health, learning, any number of them that I'm sure I'm forgetting. So ~ it's well-known in the community and it's...

AJ Harris (03:07)

very well known for building very strong relationships and reputation with its customers for delivering effective and innovative solutions.

AJ Harris (03:15)

With us today, we have a couple of individuals, Michael Muldner and Farhan Selod from the cybersecurity aspect or practice within Calian They provide a lot of very comprehensive services for cybersecurity, including things like advisory for how to effectively implement cyber resilience like we're talking about today.

AJ Harris (03:34)

Managed security services to help organizations execute on their security strategies and protocols.

Offensive testing to identify weaknesses and such. Incident response services to help when there has been a problem. Very much helping organizations safeguard their critical assets and then build that increasingly complex cybersecurity capabilities. Couple background on just the folks that we have. It's a very high-power team that we're talking with you today.

AJ Harris (03:57)

Michael Muldner, he's the CIO and CTO of the Calian Group. He oversees all facets of companies, technology, strategy, operations, innovation. He's been doing this stuff for over 27 years, deeply passionate about this stuff. And we often have had some good conversations in the past, he and I, about these sorts of things. Farhan Selod is the director of the GRC and he's the virtual CISO for the Calian Group. He leads that enterprise-wide resilience initiatives across healthcare, utilities, critical infrastructure.

AJ Harris (04:25)

25 years experience as well with cybersecurity and digital transformation. You know, his role is to help organizations bridge that understanding from the technology and the governance to build a secure and adaptive and creative capability. On the other side, we have Stratford. So, one of the things that just to kind of bridge those two, Calian and Stratford, work very well together.

AJ Harris (04:47)

Calian has a very strong belief that it's how you do the work is as important as the work that you do. And Stratford, we're very much the same ideology for that. We, take the, the how we execute and making sure that our customers see that value as a top priority. We're a management consulting firm that helps organizations achieve better outcomes and focusing through like better strategies, better leadership, better execution, better capabilities. We operate across three core capabilities. There's the management consulting capability, which I'm a part of.

AJ Harris (05:16)

There is the people and culture capability that provides that capability, know, people and culture services and leadership for organizations.

And then there's the intellectual property, which is a full intellectual property, a full-service intellectual property agency that Natalie Giroux who's with us today is the president of. We are

very much trying to combine these capabilities, these three facets of our business for some real-world experience to help our clients achieve those strong results

AJ Harris (05:43)

and strengthen their capabilities. Joining us besides myself is Jim Roche. Jim Roche is the President and CEO of the Stratford Group.

AJ Harris (05:52)

He's worked often to strengthen leadership, governance, and strategic capabilities. He's been doing cybersecurity cryptology for pretty much as long as you can. I think he studied it in university, if I remember correctly. He developed encryption chips early on. He's been very familiar with how this progressed.

AJ Harris (06:09)

And today he helps organizations build resilience from the inside out, and not just in this area specifically for cybersecurity, but in a number of areas, helping advisory boards and such build up their governing strengths, helping executives understand how to manage and help their organizations thrive. And Natalie Giroux is the president of the intellectual property agency, as I mentioned, one of those three business units. Lots and lots of experience. She's one of those people that you can say she's forgotten more than most people know about this sort of stuff, really understands IP

AJ Harris (06:39)

desperately well and knows also more importantly how to apply those practices and capabilities to an organization and help to make the resilience as part of that.

AJ Harris (06:50)

So, this is our panel today and I want to thank everyone for spending time out of your schedules to help ~ us have this discussion today and talk about this exciting topic. Before we get into the questions, let me reach out to both Michael and Jim. We'll talk about it from kind of your perspective. As we've talked about

AJ Harris (07:08)

the cybersecurity, digital resilience is an interesting concept, is an interesting topic and such.

And we're seeing more and more that this is something we're helping organizations build, both Calian and Stratford are fielding that with our customers. I'd like to see from your perspective, looking at it holistically across your organizations, how are you seeing organizations evolve to

become resilient? What does that sort of mean practically from what you've seen from the clients that we deal with? I guess I'll start with you, Jim, from your perspective.

Jim Roche (07:20)

Thanks, AJ. And welcome, everyone, to our panel. So...

Maybe I'll begin by, like AJ said, I actually started my career in cybersecurity back when data encryption still felt like magic. The early focus, of course, was on technical risk, algorithms, chips, firewalls, data encryption, whatever we could do to lock down technically the environment that we were trying to protect. But of course, over time, we came to realize, and we now really understand that the biggest vulnerabilities, they're not technical, they're human.

And this was probably illustrated, well, for me anyway, best by a pretty cool book. If you haven't read this, I'd recommend it. It's called Ghost in the Wires. It's written about, I don't know, like 15 years ago by guy named Kevin Mitnick, who's like in the Hacker Hall of Fame or should be if there is such a thing. And the thing that he pointed out in this book was that he was very successful as a hacker and he was hacking systems, technically, yes, very competent, but more so people, social engineering was really what underpinned his success. Most breaches today involve social engineering, not zero-day exploits. So phishing, impersonation, misplaced trust. You know, as a quick example, if we look at phishing and click-through rates, like you're running a phishing simulation, how often do people click through? You'd think, oh, it's going to be really, really small. Well, there's one company I'm involved in. I can tell you they're pretty typical. The click-through rate is between 0.8 % and 1.5%.

Jim Roche (09:10)

Okay, so that's, they got thousands of people. So, you blanket that organization with phishing attacks, 0.8 to 1.5, you're getting in. It's pretty much guaranteed. So, an aggressive campaign is going to succeed. And what that shows, at least to me, is the culture gap between understanding what needs to be done and doing it. So not clicking through, being prudent in our behaviour. while tech is absolutely necessary,

And often in these kinds of seminars or webinars, it's the focus. People actually define the perimeter. So, when you end up with repeat offenders in click-throughs, what do you do? Remedial training, which is good. So, they serve the remedial training, but really the focus should be changing the culture, building the culture, such that people understand and care.

about cybersecurity and pause before clicking on that simulation or on the actual phishing attacks. And of course, culture starts at the top. It starts with the board of directors, and it starts with the executive team. And you might think, yeah, of course the boards understand this. Let me share a little story. This is a public company board. It happened over here, a CEO talking

about a technology, novel technology that we're contemplating that they were contemplating for their business. And his statement was over my dead body. Whoa. OK, so if that's permeating the culture of the board, I can guarantee that it's having an impact on that organization's thinking about cybersecurity. So, the takeaway from that for me was don't assume that you've got an understanding and alignment at the board level. So, from a cybersecurity perspective,

Often you kind of, I've seen many organizations just kind of ignore the board and assume, the board will be supportive. But no, we need to focus on the board. We also need to focus on the executive team because not all executive teams are supportive of cybersecurity initiatives. And in fact, I've seen this very recently with an organization, another sizable organization where the CISO, really strong CISO is pushing initiatives.

and getting resistance from something basic like vulnerability patches, right? Let's just make sure we're installing patches, patches to reduce vulnerability. So, what can you do about that? A couple of things that I would recommend, one of them is at the board level and at the executive level, run tabletop exercises. I mean, it's kind of an obvious thing, but why it's important and what I've seen this effect,

Jim Roche (11:58)

executive teams and boards is that they get a visceral feeling for what it's like to be in it when an attack occurs and it changes people's thinking. that's not technology. When leaders experience it, they tend to own it. anyway, bottom line here for me is that resilience is a lot bigger than the incident response. It's a lot bigger than the technology. Of course, that's very important. I don't want to suggest otherwise.

But the goal here is not just to survive a technical attack, it's to thrive, be prepared to adapt, learn and strengthen as an organization. And that the underpin, that is underpinned by the culture of the organization. So, for me, cybersecurity is a combination of culture, leadership and technology. And actually, that's where Calian and Stratford intersect really well because Calian is super strong organization in so many ways.

AJ Harris (12:47)

Mm-hmm.

Jim Roche (12:57)

And together we're able to offer something to the market, which I think is quite unique. Those are my comments and AJ over to you.

AJ Harris (13:05)

Yeah, I think that's brilliant, Jim. And you're right, we often don't focus a lot in these sorts of sessions, especially about the impact of culture. And you're talking about it from a cybersecurity lens, but you can easily talk about it from an intellectual property lens for a lot of the same ways, which I know Natalie's going to do. Michael, what do you think?

Michael Muldner (13:23)

Yeah, no, thanks AJ and I think Jim framed it really well I mean culture is so incredibly important one of the things I was reflecting recently somebody was telling me about how fast things are moving and you know we're talking about how fast things are moving in our company and we're kind of reflecting on how fast things are moving globally and some people kind of look at this like we're in this phase where things are moving quickly but I'd actually argue

Michael Muldner (13:47)

things are continuing to move faster and faster. Ever since the industrial revolution, technology has been shortening innovation cycles. Everything's continuing to move faster. AI is now that fuel that is making things go even faster. the question is, how do you ride that roller coaster? Because this ride is not going away. It's going to continue to get faster. And Jim said it perfectly; technology alone is not enough. It's not enough when it comes to cyber.

Great example. I'm not going to say who, I happened to be in Las Vegas, I guess it was about a year ago, a little over a year ago now, where there was a major cybersecurity event, exactly through social engineering, as Jim mentioned. So, it was quite the experience. I remember checking into the hotel and it took me 40 minutes to check into the hotel because the reservation system was down. The phone in the room didn't work. Everything was completely paralyzed.

The days where you look at this as kind of a one-time thing or just a technology thing are over. It's about building that cyber aware culture. And I totally agree with Jim, it's got to start at the top. It's got to involve the board and it's not something you can do alone. think there was probably a time, you know, back in the nineties where, you could, you could get the right software or team up with one person and that kind of check the boxes. This is very much a team sport now. And that's why I'm also really excited about partnering up with Stratford. Cali has been very intentional about our relationships and our strategic alliances. And I think this is a fantastic alliance. This is not a topic you can solve on your own. And yeah, I'm really excited about this.

AJ Harris (15:34)

Excellent, thank you. And very much thank you for keeping what happened in Vegas and Vegas and not naming names. That's important. That's an important rule. So, let's kind of keep

building on that, right? We're talking about cybersecurity resilience. We're talking about it a concept. If I'm watching this and I say, you know what, I get it. I buy the argument that you folks are telling me. I want to turn it into something real. I don't want it to just be a bolt on that I attach. I want it to be something that's integral to my organization. How do I do that? So, what do you think?

Michael Muldner (15:39)

Thanks. Yeah, I think AJ, some people think about cyber as they do about like their ERP. It's like, okay, I've got to install an ERP, or I've got to do an ERP upgrade. And it's kind of, you know, one of those activities. And the reality is it's not, mean, Jim talked a little bit about the culture and that ongoing culture, whether that's ongoing training or testing or tabletop exercises. I think that's kind of one element but understanding everything has to be kind of customized. So, a roadmap and a plan, if I were to build a three-year roadmap for a company like Calian, that might be very different for a small company or a medium sized company. building those roadmaps has to be customized. It has to have input from the board. It's great to be able to collaborate with the board to talk about, you know, what's our level of risk and what's our level of investment. It varies very much by industry, varies very much by company.

Building that roadmap, I think, is really important because it's kind of your North Star. You're going to continue to adjust as things evolve. And things have been evolving very, very quickly, obviously, as we all know in cyber. But having that roadmap, having that North Star is so important because it is very much a continuous thing. This is not something that is kind of a one and done and you've solved. It's something that you have to continue to work at.

AJ Harris (17:24)

Which makes sense too, then you have to look at it from the perspective of each organization, right? And that also ties right back to the culture discussion that we were just having. ~ So, let's, okay, let's build on that too. So, I'm agreeing with that sort of piece, and I want to do something for my organization. You know what, let me throw this one on Farhan actually. So, there are aspects of what I'm trying to do to build resilience that we would consider foundational, right? So even though we are going to absolutely tailor it towards what our clients need and the position and the journey that they're in and identify them in our star, there are some things that we can say from a security architecture standpoint, from a best practice standpoint, these are foundational capabilities. How would you identify what those are? What would you tell me they're things that I have to absolutely make sure I consider?

Farhan Selod (18:09)

In this day and age, foundation of modern security architecture for me is resilience by design. You're no longer just building just layers of defensive technology in place, but you're actually looking to design systems to be adaptive, to be able to recover and to continue operating under stress. And I don't not just meaning application-wise, but also policies and procedures and individual contributions as well. Some of the organizations that are getting this right nowadays are the organizations that see this architecture as more of an ecosystem.

where things like identity, data, application, infrastructure, these are all things that work together under a zero-trust model. So rather than saying, how do I stop every attack? The question now is, how do you continue maintaining trust and continuity if and when an attack happens, right? One of the things that we do is we, these are bespoke items. We operationalize that mindset through our cyber resiliency program, giving structure to what resilience looks like.

You're not just looking at it simply from a checklist perspective, but it's really a life cycle approach that includes things like proactive threat assessments, aligning your governance models with things like either NIST, ISO, high trust if that applies, then including a realistic incident response preparation program. So, things like tabletop exercises and such being part of that response preparation. At the end, the goal is very simple.

Right? Resilience isn't something that you can stall, you know, echoing what Michael said, but it's really something that you're starting to build into the DNA of your operation.

AJ Harris (19:45)

No, I completely get it. think that's you're actually highlighting what I think is a good strength of both Calian and Stratford for helping our clients with this because, you know, taking some of these foundational pieces and saying, okay, how do I pragmatically turn that into something that I can both understand in terms of this group and implement that takes a little bit of experience that takes some understanding of how this thing works effectively and that stuff we do well. So that's it's a good, good background for those foundations. Thank you.

Natalie, let's start with you. Let's talk about IP. Let's talk about trade secrets. So why are we doing all the cyber screw stuff at all? It's because we're trying to protect our organizations. We're trying to make sure that they can continue to operate and the threats that we see outside that our data is secure, that our trade secrets, the things that make our organizations unique, capable, effective, and let them thrive is kept secure and strong. So, from your perspective, if you're looking at us talk about digital resilience, you're looking at us talking about implementing these practices for digital resilience with the idea of

improving the strength of our intellectual properties, capabilities, the strength, the longevity of it. How does this stuff help our, IP portfolio effect?

Natalie Giroux (20:52)

Yeah, I believe that cybersecurity is the backbone of the IP strategy because you need really strong control. Otherwise, trade secrets will be stolen or leaked and basically you lose your competitive advantage. Also, patent innovation can leak before they're protected, in which case most countries won't allow protection. So that's why it's really important to have the right measures in place to avoid any kind of leakage.

As you know, these days, a lot of innovations is executed on the cloud and reverse engineering can only be done with illegal access as compared to inventions that are on products that can be legally reverse engineered. So, this opens the door to a powerful IP strategy that combines trade secrets and patents. As you know, trade secrets provide lifetime worldwide protection at no registration cost, but it's only ~

a valuable asset if it's kept secret. So, the longer you can keep it secret, the longer you have the competitive advantage. If you compare that to patent, that gives you 20-year protection only in the country you can afford to file and at a very high cost. We're looking at hundreds of thousands of dollars for one patent in its lifetime. So, ~ and you have to give a worldwide publication of your innovation in order to get a patent.

So, I think it's really worth investing in maintaining like a strong cybersecurity and develop an IP strategy that combines both the trade secrets and patents.

AJ Harris (22:31)

Yeah, makes sense. So, let's now, let's go back and talk. thinking from the perspective of someone watching this is like, okay, I get all this. And I just said something that I realized I didn't qualify. said, Hey, Calian and Stratford are really good at turning this into a manageable chunk. And I don't have to take my word for it. Let's talk to the experts here about how we actually do that. So ~ let's start with you, Michael. Let's say, okay, I just said that we can take this very complex idea that need to you know, figure out how my culture is going to work with this, how the landscape is going to work with this, how my technology is going to work with this, how my board is going to work with this, how all these things are going to happen, and I'm to turn it into a manageable chunk that we can actually action, something we can do. What does that look like from your perspective? What would you advise your clients that they should be doing?

Michael Muldner (23:15)

Yeah, and I'll take it back again, AJ, to that roadmap, because I think a lot of people get very overwhelmed and they want to kind of jump from no cybersecurity maturity to we want to be fully zero trust, we want everything. And I would say that being able to prioritize everything, understanding how much risk you're willing to take, how much you're willing to spend, not all initiatives are equal. So, if you look at initiatives from the lens of

AJ Harris (23:29)

Mm-hmm.

Michael Muldner (23:44)

complexity of implementation and cost and ROI. So, one of the things that always jumps out to me, some of the companies that you talk to, they don't even have MFA deployed. And like that's such a very, very simple thing that'll protect you by no means do it. You know, when I say that that's the end all be all in terms of cybersecurity, but it's something that's relatively easy to deploy and it has a huge impact. So being able to prioritize all these initiatives because it can be really overwhelming. If you look at kind of a three-year roadmap. It's like, wow, how am going to climb that mountain? I would say it's kind of one step at a time. And some of those early steps are really not that complex. It comes back to what Jim said, ~ building a cyber aware culture has a massive impact. And I would say it's really not that much effort. It starts at the top and really building that culture. It's something that everyone can get started today.

AJ Harris (24:38)

Oh, that's good. And for our audience, in case you're not familiar with when we talk about acronyms, MFA is multifactor authentication. It basically means that two-step authentication we force you to do rather than just use your password, which if you're listening, everybody should be doing for everything you have right now. Let's just be clear on that. Jim, what do you think about this?

Jim Roche (24:54)

I just want to jump in and add to what something that Mike was saying. Yeah, constant pressure evolving over time. You're not going to do it in a moment. I agree with that. The other thing I wanted to point out is that there are events that will increase the likelihood of an attack. So, for example, if you're acquiring a company and that becomes public, that's a signal to hackers to come after the company that you're acquiring, because they probably have weaker systems in place. They might have a weaker culture. And I can tell you a story. So, one of the companies I'm involved in did exactly that, acquired a company, hackers got in, and it destroyed the value of the acquisition, because we lost our number one customer due to the successful cyber-attack. And that customer's concern that that attack made them vulnerable.

AJ Harris (25:51)

Okay, I'm going to build on these things, because I like your answer, Michael. I love the idea of the roadmap and such. love how that's often the best practice that we do. Farhan mentioned NIST. I want to bring that one up specifically. So, folks that don't know, this is the, I'm get this wrong, National Institute of Standards and Technology, I believe. It's a US-based institute. When we do things like cyber assessments, we use the NIST controls. They're very, very comprehensive. They cover every aspect of your business. They're the ability for you to basically make sure that no stone is left unturned when you're looking to understand what your threat landscape looks like, how strong your current controls are and where you can focus. But there's a downside to it. I've seen this time and time again, because you go through those NIST protocols and you say, okay, here's now a recommendation based on it. And it's an 800-line recommendation of things you can do because it is so thorough.

Here's everything you can look at. thinking about that and thinking back to kind of Michael, your point is that, look, we have to turn this into a roadmap, something actionable, something manageable and tailor it towards the organization's capability. So, Farhan, how do you kind of do this? How do you say, I'm going to use this very well and thorough control scheme to make sure I'm not missing anything. Overwhelmed somebody with 150 recommendations of different capabilities. But I still need you to make sure you can be agile enough to be innovative and creative and let your business actually function. How do I kind of make that happen in a way that works?

Farhan Selod (27:20)

Yeah, I think striking that balance between agility and compliance is probably one of the toughest things for organizations these days, everyone’s trying to move fast. They want to modernize. They want to adopt cloud. They want to integrate AI. But once you're trying to go down that path, governance sort of feels like it's always trying to play catch up, right?

It's never at the forefront of where it needs to be. One of the things I've seen really work well with teams that to do this appropriately is they're not treating compliance as a gate or a hurdle that they need to cross, but rather it's part of the design element. It's part of the initial design input.

So, one of the things that we do at Calian is we often start an organization with a complete enterprise risk assessment, right? It gives the leadership a clear prioritized view of what's happening, where are your risks, what are your dependencies look like, how does it align to frameworks like this CSF. And so, you're not approaching these things from a strategic perspective and not necessarily being reactive, right? And then you start to bring some of those things to life through things like tabletop exercises, because that's when you start to see

maturity from a real perspective, right? You tend to see how your people, your processes, all your technology, how is it all responding under pressure?

You you're starting to understand is being agile actually assisting you or is it having the opposite effect and it's actually hurting the organization in certain terms, right? So, know, frameworks and compliance frameworks, they're going to give you the blueprint, right? And agility is really going to come from how are you testing and refining your process? We've got the old adage from DevOps world saying CI, CD, you're continuously implementing, you're continuously developing. It's a similar mentality, right? Because you're continuously looking to build your resilience. It's no longer a constraint.

And that's when you sort of start to see and hit that sweet spot between being innovative but being innovative in the safety and assurance that your cybersecurity resilience is going to keep up with you and actually enable that innovation as opposed to hinder it.

AJ Harris (29:22)

That's perfect. Yeah, I keep thinking about the old adage about like, want my security to be very, very big. So, I'm to make it very powerful. And then the agility aspect of it is to put a sticky note in my monitor because I can't remember the thing. So, tailor it accordingly, right? Yeah. And I know we've talked about tabletop exercises a little bit. I just want to reemphasize that from my own experience too, because there's nothing that puts the fear in people's eyes, like actually doing a tabletop exercise and pretending this is real.

And then saying, like, how would I tell the board that we just had a breach? And what exactly am I going to do about it when it happens? And things like that. If you can go through it in that exercise, it is so much easier than trying to go through it when it actually happens. Let's pivot back to IP and such. So, Natalie, let's talk a little bit about, you talked about how this is a backbone of a good IP strategy, effectively. And I completely agree with you, because we're here to protect those trade secrets. We're here to protect our intellectual property.

But we've also talked about culture here. We've talked about governance. We've talked about things like that that are instrumental into this kind of an approach. It's not just about the specific technologies. It's about how you build the resilience in the enterprise from the ground up for all these different pieces. So, from your perspective, if we're talking about these same sorts of things, we're talking about governance, we're talking about awareness of these capabilities, we're talking about all of these sort of things, how are they actively being used and pragmatically being used to ensure that and organizations, intellectual property and trade secrets don't walk out the door. I want to make sure that it stays where it needs to be.

Natalie Giroux (30:50)

Right, as you just said, technology alone will not protect inventions and ideas. So, the governance will provide clear policies on how sensitive knowledge is handled, shared, stored, ~ how people should deal with trade secrets and all that. Technology includes identifying, classifying and cataloguing IP.

including trade secrets, which is something a lot of companies don't do. So, what trade secrets do we own? Who has access to them? Who ~ invented them? And where are they? they still with the company or not?

As you know, innovation starts in people's minds. So, employee awareness is really critical. So having ongoing training programs on what is IP, why it matters, what are the company's differentiator, ~ what behaviours put the IP at risk. Like, for example, working in public settings without the privacy screen. I see that a lot. ~ Being on a train, on an airplane, or even using public Wi-Fi to transfer information that is sensitive. there's also the threat of monitoring and ethical guidelines that create a culture where protecting innovation is everyone's responsibility.

AJ Harris (32:11)

I like your examples. I know we haven't talked about this yet, but I think most modern phones come with a VPN built in actually. It's literally a swipe and suddenly you have a VPN connected for your public Wi-Fi. And I can count on one hand; I think the number of people I know that use it. So, you're working in an airport, you're working in those places, you are exposing yourself and you're exposing those trade secrets. To your point earlier, they're only valuable if they're secret.

Farhan, let's talk a little bit about some of the, let's build upon that and the human pieces of it, right? Let's talk about the execution from that aspect. So, we've talked a lot about it's really important to have those human aspects. We've talked a lot about making sure procedurally you've got the governance in place, you've got the awareness in place. How do you strengthen that? So, if I'm going into organization, I'm saying we've done your assessment, we've identified areas that you can improve.

guess what, a number of those areas have to do with behaviour. They have to do with how your organization executes its work in putting up a privacy screen when you're on a train. It's a simple example of a cultural change and a procedural behaviour you need a human to do in order to protect yourself. How do you do that to support a cyber architecture? What things do you put in place that make that easier for an organization to be able to do that?

Farhan Selod (33:33)

Yeah, I'm glad how you frame that, right? Because one of the largest misconceptions that people have when they talk about resiliency is they're thinking just pure technology, right?

They're thinking firewalls, EDR tools, various cloud tools. But really, environment and organization is really only strong as the people in the processes that sort of support it. So, one of things that we do when we're working with a lot of our clients is we're putting emphasis on some of the governance framework.

But the training that goes along with it as well and the operational playbooks that sort of frame the whole thing together because if your people don't know how to respond and your processes aren't aligning with the controls and the response, even the best technology is not really going to save you, right? A good example is when we're running executive and technical tabletop exercises, it's always eye opening to see how leadership decisions and frontline actions come together or sometimes they don't come together.

And those sessions really start to reveal some of the gaps that you have within the organization, whether it's gaps between policy and practice. And that's when we really start to help these teams understand what these are, because these are all sort of like little miniature light bulb moments that happen throughout the exercise. And when I do some of these exercises, I tell them, all of this is done with extreme transparency, because the light bulb moments will happen throughout the exercise. And these are the findings that you will later see in a more formalized format.

But this is how you're sort of helping the teams build the confidence, right? And allowing them to execute under pressure so that when an event takes place in actuality, the muscle memory is actually being built there, right? You're helping the organizations develop that. Technology is going to protect the data, but really, it's the people and the processes around it that are going to protect the ultimate mission of the company.

AJ Harris (35:16)

Completely agree, and Jim, this echoes what you were saying before too, right? Especially when you're talking about, I've got senior leaders trying to build that culture, build that governance and finding resistance either from their peers or from the board or the governance, what have you.

Jim Roche (35:19)

Yeah, exactly, AJ. And if I could just add something to what Farhan said, just to amplify, guess, what he said, I, one of the organizations that I'm involved in that we're helping, ~ experienced flags when a ton of data was being pulled out of the system. So, it was a DLP, the data loss prevention algorithms were working, they flagged it. But the interesting thing is that nobody in the company acted on the flags for weeks. And that individual who was a sort of senior technical person in the organization left and went to a competitor. Well, what did they leave

with? The person who was flagged as having downloaded a ton of information and that led to legal activity. So, to Natalie's point,

There was an example where there was intellectual property that was being accessed by an employee. Legitimately, we don't know. The data loss prevention algorithms flagged it, but the culture of the organization was such that people ignored the flags. And so, the technology worked, but the culture failed and the company lost intellectual property. So, culture, critically important.

Michael Muldner (36:45)

AJ, if I can, one other thing I'm to just layer in on tabletops, because I've seen this firsthand. actually, wasn't at Calian was another tabletop that I was part of. It's fascinating some of the takeaways and this one in particular that I remember was this debate about, you know, we just had a ransomware scenario. Do we pay? Do we not pay? So, Farhan talked about kind of muscle memory. That's not a discussion you want to be having when that event actually occurs, right?

AJ Harris (36:46)

Yeah.

Michael Muldner (37:14)

That's why you do the tabletop exercises. it's, if you haven't done a tabletop, do it. You'll be fascinated at the different opinions on how, you know, how you get out of those scenarios.

AJ Harris (37:25)

Yeah, no, very good point. I was thinking too of the cyber range at the University of Ottawa, where they've got that whole thing set up, the beautiful environment, including a media station with TV cameras pointed at you saying you're about to give an interview to explain why you let hackers into your organization. Doing that in a test scenario before you actually have to chat with the media would be so valuable. Try to do that first time when it's actually live. So great example for that. Yeah, Farhan?

Farhan Selod (37:53)

I was speaking to a medical board yesterday, for directors for a hospital, just asking the simplistic question around what do people still think hackers look like? If you visualize a hacker in your brain, what do get? And you've got the typical images of somebody in a dark phase, hiding in a dark...

AJ Harris (38:12)

Dark hoodie

Farhan Selod (38:15)

dark organi- you know, you're in a dark area, don't really necessarily know what that person looks like. And the board was nearly flabbergasted when I tell them a description of an actual organization with the CEO, the CFO, with, you know, help desk teams that are willing to quote-unquote help you after they've reached you. Like these are now the most-

illegitimate organizations that are raking in hundreds of millions of dollars ~ in a year, right? So, it's, know, there are two, 300 people strong, sometimes even larger. So gone are the days of a 17-year-old in mom and pops basement, you know, hacking NASA. Might've been true about 20 years ago, not necessarily today.

AJ Harris (38:56)

Completely agree, this is a big business. more and more, we're seeing that as of the last decade, it's state-sponsored business often, right? So, you're not just dealing with organizations, you're dealing with nations. And there's a whole different level of fun that you get to have. I want to kind of go back, I'm very cognizant that our audience, we can talk about this stuff forever, but the audience that we're dealing with is looking for things that they can pragmatically do. And I want to talk about one that we haven't talked about yet, which is those collaborative cloud environments, right?

We have very much seen that over the past decade, especially, a lot of our data has moved to the cloud. A lot of our activities have moved to the cloud. I don't need to install applications anymore to execute in this work. I can do it over the web. I can do it from a cyber cafe. I can do all those sorts of things. And there's huge benefits to the level of collaboration we've been able to do because we've been able to make it so much easier for us to work together to share information, to utilize that information, to leverage it.

But that brings on the risks. And Natalie, you talked a little bit about those risks in terms of also some ideas that you would have to say, how do I build the culture and the processes to protect that? From your perspective, if I'm linking specifically about, you know what, I have all these cloud environments, my data is all there, I'm using it to share my intellectual property, my data, my capabilities with clients, with peers, with other organizations to support me. What can I do to balance, you know, I kind of have to balance that accessibility and that confidentiality.

Natalie Giroux (40:22)

Yes, so if companies are planning to use trade secrets as part of their IP strategy, it's really important to give teams access to only what they need to do their job, not to the entire code or

to the entire environment. As you know, at Coca-Cola, nobody knows the entire recipe. It's split between people. Same thing here. So, if I don't need to see a piece of code, then I should not be able to access it. That's really important.

Natalie Giroux (40:52)

At the same time, with these environments where things are moving from a development environment to a cloud and things like that, securing data in transit is really, important, as important as securing the platform itself. Because it's easy for attackers to intercept or spoof the information and then duplicate it, publish it to anywhere else, and then the trade secrets are lost.

Having proper encryption and authentication and making sure that data flows securely is really important, I think.

AJ Harris (41:31)

Farhan, let's build on that because one of the you mentioned before that I very carefully avoided talking about until now is Zero Trust and the same idea of like, how do I use these kind of frameworks like Zero Trust or similar when I'm trying to secure these cloud environments like Natalie's talking about and do that level of access control and do that level of diligence.

Farhan Selod (41:53)

You know, I have a bit of a challenge with Zero Trust because it gets talked about a lot as a philosophy, but a real challenge is really operationalizing it, in practice, I always tell clients that Zero Trust isn't just a singular product that you can go out and buy and implement. It's really a posture that you need to build within your organization, right? The starting point for me is visibility. You cannot protect if you cannot see it. So, to begin with, you need to understand where your data is. Natalie talked about understanding your individual assets and data mapping exercises, having an asset inventory so you know what you have within the organization, understanding how information actually flows through your environment. From there, you can focus on things like identity management, making sure the right people have access to the right things and really nothing more.

Start to add in layers of things like network segmentation, encryption, vulnerability management, and these are all technical enablers that now start to build your Zero Trust strategy. ~ You know, we often pair those controls with ongoing risk assessments, validation testing. Now, you know, your Zero Trust starts to look more like a living framework. These are things that you're going to do over and over again, and these things will adapt as your environment changes, as you mature as an organization as well.

AJ Harris (43:04)

Mm-hmm.

Farhan Selod (43:10)

And you can continue testing it through things like, you know, again, tabletop exercises, things that keeps coming up over and over again, simulating incidents, understanding, you know, and vulnerability tests, things of that nature, just to see how your architecture starts to hold up under stress. To me, you know, Zero Trust isn't, you know, a product checkbox or just a slogan, right? It's really, I go back to designing your architecture so that every connection, every identity, transaction, it's all earned and verified. And it's done so in a continuous manner.

AJ Harris (43:40)

That's perfect. I like how you're defining it. In fact, I'm going to put you on the spot here and say, for the audience, because they're going to take this stuff away and go talk to folks. Can you give them like a, here's your catchphrase for what zero trust is so they can just kind of convey that? How would you define it?

Farhan Selod (43:53)

Goodness.

Honestly, just think of it no longer as a philosophy, but it is part of your DNA, right? Zero Trust to me is how am I designing my architecture so that all of my enablers are part of the layers of security that I'm going to build. And again, not just technology, remember it's part of your process and procedures as well and the people that you train.

AJ Harris (44:18)

Jim?

Jim Roche (44:22)

So quick, just a quick add on Farhan earlier mentioned 27,000 ISO 27,001. ~ And there's another standard which is pretty often bandied about SOC 2, type 2. ~ If you're not familiar with these ISO 27,001 is a standard for cybersecurity. The reason I think it's important is that in the supply chain, more and more customers are looking to suppliers to demonstrate

Jim Roche (44:51)

that their environment is secure. And so, you, you know, the customer can send you a long questionnaire and you can fill it all out. Or you could say we're 27,001 compliant. There's a commercial benefit to this investment. And that commercial benefit sometimes is enough of a

catalyst to get boards and executive teams to make the investments, to move towards a zero-trust environment that Farhan is talking about.

AJ Harris (45:17)

Yeah, completely agree. The SOC 2, I use it all the time and I have my clients use it all the time too. And just so the audience knows, if you get anything, like you're even thinking personally, I'm going to use this web-based SaaS solution to manage my music or something like that. You can actually go to that organization, Security Center, which you can usually just Google and find the SOC 2 report, which covers all the things we just talked about. Even when like Natalie was talking about encryption at rest, encryption spot, it's covered as part of that report.

It's kind like a one-stop shop to say, can I be comfortable that the vendor for this solution has done their diligence while it can be externally audited by someone else with this report on an annual basis? And suddenly half the worry that you have to do about is this thing reliable or not is done. Only half, though. There's lots of other work you have to do, but half is good. So yeah, I completely agree with that. OK.

We are coming to the point now in a few minutes where we're going to start talking about questions that we have from the audience. So, thank you everyone who stayed with us so far and I appreciate that you've provided some input for questions. Before we do though, I'm going to give each of our panelists here to say, okay, and I don't know how I can do this in less than three minutes. So, let's say in 30 seconds or less.

AJ Harris (46:29)

What do you think is kind of that next big thing, that emerging technology, that emerging issue, that emerging piece that we're going to be talking about related to digital resilience, cybersecurity resilience in an organization over the next year? What do you think is going to be that next thing that we have to focus on? I'm going to start with Jim.

Jim Roche (46:49)

yeah, tough question. The go-to now is AI. That is changing both sides of the equation. So, hackers are using AI effectively. You think about Sora as an example, they can now do deep fakes. So phishing, you know, much more effective. But on the flip side, we're using AI inside our companies. You do it wrong, and you could end up losing intellectual propert or exposing yourself to hacks. So, AI is my answer.

AJ Harris (47:20)

That's a good one. Michael, you're next.

Michael Muldner (47:23)

Yeah, I'm to go even broader because I totally agree with Jim. mean, obviously AI is changing everything, but I'm to come back to what I said earlier about change and the pace of change. And I'm going to say adaptability, being able to adapt to that changing environment. Things are going to; you need to go faster and faster. Like if there's one skill that I everybody needs to have is the ability to adapt. Think of it this way. Three years ago, chat GPT didn't exist. only, it only came to be in November three years ago.

AJ Harris (47:48)

Yeah.

Michael Muldner (47:53)

We don't know what's coming next year or the year after, but I can guarantee you that things are going to continue to evolve. They're going to continue to move quickly. That's not a journey you want to take alone. So, find the right partners to go on that journey.

AJ Harris (48:07)

I think that's a great point. And I know we haven't talked about it yet. It's actually not the subject for today but change saturation comes up a lot with my clients when we're talking about it. Not specifically related to cybersecurity, but we could pick any topic and how fast it's changed and how much it impacts the business and how much our clients are asked to be adaptable and figure out how to integrate it into their organizations. And everyone's just kind of done.

So that's a really good point. should probably, maybe we can look at having a separate discussion about how do you deal with change saturation and manage kind of all these changes that we have to deal with on a regular basis. Farhan, your turn.

Farhan Selod (48:42)

I'm going to add on to what Michael and Jim stated, right? To me, if I could leave anybody with a thought process, think of it this way. Resilience shouldn't be stalled. It's truly a mindset. It's one where you're always preparing, you're testing, you're improving, and you're innovating. When you approach cybersecurity in that manner, you're not just defending your operations. You're enabling innovation with a certain amount of confidence, and I think that's powerful.

AJ Harris (49:07)

Very good and Natalie, what are your thoughts?

Natalie Giroux (49:09)

I would say creating a healthy ongoing paranoia around the loss of IP.

AJ Harris (49:18)

Healthy, ongoing paranoia. That's our tagline. I like it. That makes perfect sense.

Farhan Selod (49:23)

I want Natalie to be part of all of our tabletops from now on.

AJ Harris (49:26)

Absolutely.

Very good. Okay, questions. Questions from the audience. There's a couple of good ones here that I'm going to relay. You know, one of them is on AI, so let's talk about that. Because the specific question is, what role does AI play in achieving cyber resilience? And we've talked about cyber resilience, we've talked about it from a technology capability, we've talked about it from a governance capability, we've talked about it from culture, from people and such.

And AI is the big wrench in the ointment for a lot of things. Jim, you mentioned that, yes, we're now using it also to protect ourselves as well as we're finding it as threats that we have to deal with. So, let's start looking at it from a cyber resilience standpoint. And Farhan, I'll start with you. What are you seeing in terms of how AI is impacting our ability to build cyber resilience, both in terms of what we have to deal with and what we have, like the tools in our toolbox to work with?

Farhan Selod (50:16)

Yeah, I think AI makes things very interesting, right? So, you're starting to see more and more ~ security operations centers and SOC teams really start to build AI into understanding what the alerts are, ~ how multiple different kinds of alerts where the human operator may not necessarily correlate them together. AI makes that correlation lot quicker. know, human behaviour analytics, things of that nature.

But I've started to see AI being used in bit of an opposite sense as well when it comes to intrusion prevention and just intrusion testing as well. So ~ this knowledge is slightly older, but you had older AIs like Worm, GPT, where threat actors were actively using these things to infiltrate a network and use AI to infiltrate different components of the network. Whereas now you have organizations that have sort of reverse engineered that from a white hat perspective.

AJ Harris (50:51)

Mm-hmm.

Farhan Selod (51:09)

to do it internally within companies to test, know, ~ how do I use AI for powers of good to understand what my intrusions now look like so I can go ahead and go repair them and move forward.

AJ Harris (51:23)

I like how you say slightly older. We're talking a whole six months ago or something, right? This is ancient technology when we're talking about this for AI.

Farhan Selod (51:27)

It changes so quickly.

AJ Harris (51:31)

Michael, you have any thoughts on that?

Michael Muldner (51:34)

Yeah, I was just going to layer into what Farhan said. you know, I think a few years ago, I remember breakout time and breakout time is basically from the time somebody gets into your network to the time they can move laterally. You know, it was, was in the vicinity of hours. Like for the time somebody got into the time they're moving laterally, they can actually really do damage. was hours. AI has now shortened that. think the latest statistic I heard was less than a minute. So, you know, imagine if you're not using AI to find out that someone's gotten into your network and to be able to contain that because if you're not using AI and your intruders are using AI, you're just not keeping up.

AJ Harris (52:11)

Yeah, so my robots can fight your robots and hopefully protect my insu- yeah, that's all good. Natalie, what about from an IP perspective? How do you see AI impacting our ability to protect our intellectual property?

Natalie Giroux (52:23)

Well, there's a few people from Samsung that got fired because they put a trade secret in chat GPT because there was a bug in their code, but that was a piece of trade secrets. So, AI also brings a lot of risk from an IP perspective in terms of disclosures, copyright infringement and many aspects like that. But and also ownership, right? So, AI creates art, who owns the art? Is it

the creator of the AI engine or like, so all of these things are still being debated and decided. And currently each country has different approach which will create a mess in the future.

AJ Harris (53:10)

Yeah, Jim, you mentioned this too about using these tools in such a way that you have to protect yourself internally from what you put in them. I know when we do AI strategy and AI training, the first thing we do is awareness, right? Just to make sure that if it's being used now, you're doing it safely.

Jim Roche (53:22)

Yeah, just you know, everything, everything that we've heard, I agree with. At the same time, we want to build. We want people to use AI in our companies, but we want them to use it safely. So interesting statistics. So involved. Keep giving you examples. Here's another example company of about 1500 employees, roughly 10 % of the employees are not using their chat GPT licenses. Whoa.

How's that possible? Well, there's laggards, right? There's always a curve. So you can lock down AI and say, it's going to be, you can lose intellectual property. And of course that's true, but you can do it in such a way that you discourage people from embracing AI and using it, which will actually detract from your mission as an organization. So, finding that balance is really important. People need to understand how to use AI safely.

AJ Harris (54:13)

Yeah, I think that's why strategy and a framework to execute that strategy is so important, right? Natalie, you mentioned different countries. I think there's a question I have here which I think fits into that beautifully, which talks about data sovereignty.

So, we're seeing more and more, and I've seen this trend quite a bit for the past decade or so, understanding where physically the data lives and where physically it's created is more and more important, especially as different countries have different legislation related to what protections exist for that data based on where it was created and based on where it's housed. ~ So ~ how do you see specifically data sovereignty related to protecting IP? And I'm going to use one example just because it's very top of mind, especially considering that we're seeing legislation and discussions in the US talking about US companies that even though they're operating in Canada, the fact that US company means that that data is susceptible to interception and use by US authorities.

How do you see that playing out?

Natalie Giroux (55:16)

So, in terms of data, we're talking here about copyrights, right? So like, and different countries have different rules for data protection in terms of copyrights. ~ For example, in Canada, you have the raw data that's protected using some rules, then the derived data that the algorithms modify, and then the final set of data that's used. And the rules are different depending on where it's been created, where it's been modified, and ~ how it's finally used. ~

AJ Harris (55:49)

Farhan, do you see this coming up a lot in discussions related to how you structure systems and how you protect data based on data sovereignty details?

Farhan Selod (55:56)

Yeah, absolutely. Specifically in healthcare, right? Because sometimes you don't want your data leaving Canadian data centers. it definitely does become very important for certain organizations. I work with a lot of companies down in the States as well, and it's a big deal for them as well. They don't necessarily, depending on the vertical that they're in, they don't necessarily want their data leaving Americans.

AJ Harris (56:00)

Yeah.

Absolutely. there's the, I'm very happy to see these days that a lot of the providers are quite keen to help make sure that your data can live on, you know, Canadians or in a Canadian data center, et cetera. But I had one client ask me once like, how do I structure my capabilities and not leverage us software? And that's a, that's hard. I'm struggling to think how you can do that considering how much of it is built in the U S and then patented in the U S right.

AJ Harris (56:47)

Very interesting.

Jim Roche (56:48)

Just a thought on this is probably many of us are familiar with ghost IT, know, people that are downloading applications and running those applications on corporate systems using corporate data. Some corporations are more constrained than others, but that is an attack vector. It exposes often the data to servers and environments that the corporation would want to avoid.

Jim Roche (57:15)

So, this is an area I find a lot of companies really struggle with is how do we, because you clamp it down and employees will go crazy because like you're reducing my productivity. Like yeah,

okay, it's a balance. What you're doing here, what you're using is not SOC 2 compliant and it's running on servers in Latvia or wherever.

AJ Harris (57:39)

All right; we are out of time. So, Natalie, Jim, Farhan, Michael, thank you very much for joining us today. And thank you everyone who's tuned into this discussion for us to celebrate our Cybersecurity Awareness Month. had a great chat. We heard a lot of key takeaways here, but I think kind of the key parts are like resilience is a combination of things. It's not a one and done. We talked about this a lot. It's not a project, it's not a one and done, it's not a bolt on. This is how you structure your culture, how you structure your organization to build in that resilience.

And ultimately, we're building in that resilience because we want to focus on the core business, not focus on how do we fend off the attacks or the thing that resilience allows us to do so. So, you know, aligning governance, aligning IP, aligning your, your culture internally, aligning your processes, aligning the awareness and such.

and building that roadmap. I really much, I do want to emphasize that this can be overwhelming, this stuff. I we work in this business; I find it overwhelming. So having the ability to say here is a very structured, methodological, crackable way that we're going to execute these initiatives to build that resilience over time makes it so much easier for you to plan for, for you to manage, for you to oversee and for you to report on.

And that's something that both Calian and Stratford can absolutely help you do. If there's any point that you think that you'd like some discussion on that, please reach out. We'd be very happy to help. Thank you, everybody, and enjoy the rest of your Wednesday.

Michael Muldner (59:01)

Thank you.

Farhan Selod (59:02)

Thanks

Jim Roche (59:03)

Super, thanks.

**This webinar was transcribed using AI, there may be some errors.*