THE INFLUENCERS: DIGITAL TRANSFORMATION

TRANSCRIPT

CHARLIE LEWIS

Leo von Gerlach (00:24.4)

Hello, and welcome, everybody, to another edition of The Influencers, our podcast on Digital Transformation and Law. I'm Leo von Gerlach, and with me today is Charlie Lewis. Charlie's a partner of consultancy giant McKinsey, with a supreme expertise in cybersecurity for business and governments alike. Charlie served for 13-plus years in the U.S. Army. He led in combat. He dealt with cybersecurity issues and operations, and he's also an associate professor at the U.S. Military Academy at Westpoint. Charlie, wow. This is quite a list of credentials. I mean, it's amazing. I don't really know where to start the conversation, but perhaps it's a nice inroad if we just go back to your time at the military and then the considerations that led you to go into the field of consultancy.

Charlie Lewis (01:30.1)

Yeah, and thank you for the great intro, Leo. It's an honor to be here today. I think one of the items that helped me make this shift from the Army into consulting is, as I looked about where I wanted to go in my career and where I could have the most impact on security and helping secure, from a cyber standpoint, industry versus our national security, when I made the transition from a field artillery officer into cyber operations, I quickly realized that cybersecurity is no longer just a government problem. It is no longer a defense problem, it is not a whole-of-government problem. It is a whole-of-society problem. In the interconnectedness between what happens in the defense side, what happens in broader government, and then what happens in the private sector, it's important to have a broad understanding within there, and I saw that I could, hopefully, and I saw McKinsey as the right pace to do this, scale my impact in helping the world's most iconic brands think about how can they protect their brand, what they provide to us, and how can that make us more secure as a society? So, that transition led there, right? And I was lucky to find a place like McKinsey that, one, has a really strong cybersecurity practice that integrates within business objectives and the broader business strategy, but they were also a great place for veterans to land. Veterans at McKinsey is a large support structure. We are really fortunate to be able to guide and help mentor through there, and now, in my role as a partner, I'm able to also help play a leadership role in that broader group and help other veterans transition into McKinsey, as well into other roles within the industry.

Leo von Gerlach (03:18.6)

That makes certainly just perfect sense, and just speaking about protection of brands, speaking about the protection of organizations, perhaps you can

explain what that means in concrete terms. So, how do you approach something like making an organization resilient to any type of cyber crime?

Charlie Lewis (03:42.1)

Yeah, and I love the word “resilient” there. I think that it is key, right? You’re never going to complete reduce all of the cyber risks that you have, and if you were to disconnect from the Internet, apply a ton of controls, that wouldn’t allow your business to operate and grow its value and achieve what it wants to achieve, as well. So, what we think about serving clients with in cyber, we think about where are the most critical business aspects, the critical business services—what are they providing? How do we better understand what those business risk outcomes are for each of those critical business services, and then how do we think about how much risk each of our clients is willing to accept across a variety of different risk types, and then, from there, help them design programs that let them visualize, measure and actually reduce the risk to a way that meets the risk appetite that the board and the C-suite is setting, but also allows the business to realize the value it has in its ongoing projects, its transformations, etcetera, etcetera.

Leo von Gerlach (04:46.2)

I can easily see that you have a hard time, on occasions, to convey the actual gravity of the risk that an organization may be facing, and you have a number of tools to address this spontaneous level of ignorance at the beginning. There may be playbooks for training days and units, there may be certain schemes, but you may also tailor this to the need of a given organization. So, what’s the recipe here?

Charlie Lewis (05:18.1)

I think a little bit is really understanding—I mean, the first is to meet your client where they are, right? And, again, the value of what we do—at McKinsey’s, I don’t operate separate as a cyber person within an organization, I’m connected to our broader client service team that understands the business strategy and the concerns from there. And by communicating about cyber in business terms, right, so thinking about what is the impact of the risk to the business, we can start making those decisions and conveying where the investment needs to be versus being overly technical or overly engineering focus. By—so, starting in that conversation with the C-Suite helps, but then, on the other side is just recognizing where leaders sit and how to make sure they understand what their role is not just in the risk reduction and the prevention work, but also if you have to respond, and thinking about how do we prepare organizations to respond in a way that maintains operations, protects the data of the company, its employees, and its customers, and then how do they start thinking about their decisions so they can respond faster if a crisis happens. But it’s all about getting integrates into the business, and then taking that risk back approach based off of where their core business risks are and making sure that that communication comes through that way and there’s consistency with the reporting.

Leo von Gerlach (06:46.0)

So, that's interesting, and let's stay with that point for a little bit longer. So, what are the points that you want to drive home when you just conclude a session and we say, "Those things really need to be engrained in the corporate understanding. That is something nobody should be handling wrong at the highest level—of every level of the organization?"

Charlie Lewis (07:13.4)

And I think what we have actually seen is, in my view, there's three places to think about this. So, one is how do I get the board and the C-Suite to understand? And that's a bit of what we just talked about. They're well aware of what cyber risks. Within the United States they have to report within their 10-K. They're talking about cyber risks. They see this, and it should be a component of all of their investments. And so that starts with that risk appetite—risk-based approach. There's then another group that you need to work with, and it's starting to push down into the business. So, making cyber not just a control and compliance function. But someone that can help the business grow and get product to market faster. And by embedding security within product development earlier and starting at the threat modeling and ideation phase and embedding throughout the development lifecycle and throughout any sort of business project, the procurement cycle, etcetera, etcetera, you're actually able to accelerate the product-to-market, the go-to-market time, and the impact you have, and then actually reduce the overall burden in terms of paperwork, documentation, and vulnerabilities identified. That lets the business achieve their objective for which they are incentivized against faster while also building out security, and then generally—look, the attackers are very sophisticated, and they are able to find the smallest little ways into your organization. And they move quicky. So, if you can get through "Where's my risk?" So, I want to invest against there, how can I make sure that what I'm doing as a business, I'm doing securely? But, ultimately, if something goes wrong, how can I make sure that I respond quickly? I understand where the decision-makers are. And so that comes down to simulating incidents, simulating broader crises, and doing it from business level all the way on up to the C-Suite and the board, so everyone understands escalation criteria, decision-making rights, who is making those decisions, and what needs to be said and where. So, that way, if something does unfortunately go wrong, you can minimize the impact as much as possible

Leo von Gerlach (09:33.4)

Well, I think that's very clear. Making the right decisions fast is obviously just mission critical. But I think you mentioned so many other things there, like embedding business objective, risk appetite, and, taking this all together, I kind of understand that there's a cultural element and perhaps I take this a bit further and understand that you are strong in just trying to instill a culture of cyber crime prevention or cybersecurity, however you may call that. Perhaps you just add some more words to that interesting concept.

Charlie Lewis (10:18.0)

No, that's one of my favorite things, and so I do a lot of work on organization and operating model training and awareness, because it's what I did in the Army. Coming out and being able to—how do I raise and train and elevate

not just my cyber and my technical population, but the rest of the business. And then how do we think about broader change management and culture awareness? It is a bit of a shift to think about how do I add on security into, say, development or procurement process. What is that approach? And, so, if we hear it time and time again that the largest vector within your organization are the people who are on the computer, right? And it's more now than just phishing training. It's actually sitting in and looking not just at your critical business services, but it's understanding who are the types of employees within your organization—HR, finance, the developers, digital folks. If you are an operational technology company, who is working on the systems? Who is updating your PLCs? Who is actually going in and out of the manufacturing plants or the refinery? And understanding each individual group, risk assessing them, understanding where their core gaps are, and then applying specific training or guidance or incentives to them to operate in a more secure way, one, just broadly across the enterprise. And then we hear the terms "security champions", but then how do we find folks within business organizations, whether it's a developer, an executive assistant, an HR professional, who are those who champion security, password security, locking computers, making sure you're aware of social engineering tactics and techniques that are happening, and just being aware generally. So, it's taking how do I train and run the general training? How do I target specific training to certain folks within the organization who might be high-risk users? And then how do I embed through security champions to make sure there is always someone who is thinking about security within various parts of the organization?

Leo von Gerlach (12:33.2)

Wow, great stuff. I mean there's so much good advice there in what you are saying. I've almost taken notes. But just moving on perhaps to technology and newer technology. We read so much about arms race just by the technology used by attackers and then the response by the organizations that becomes ever smarter and AI-supported. So, what do you see as the new frontiers, the new challenges with the significant pace that technology takes at this point in time?

Charlie Lewis (13:11.2)

Again, I'm—that question is a fascinating one, because it anchors in the text. Because, ultimately, that is a bit of the threat, right? And when organizations come to us and start talking "Well, what's the risk to my industry?" We know what the risk is to the industry, but, ultimately, it's baked into the technology. Where they sit, where that scowl is. And so we look through there. And it's been—we see an increase in threats, obviously, within the cloud. We see human errors causing some of those threats. We see organizations working to secure new digital investments, whether it's the cloud, generative AI as they're making those pushes. How do I make sure that, for generative AI, that I've embedded the security principles within that development lifecycle, as well? And then, finally, we've got to think about the operational technology side and the actual pure manufacturing, the building, what is being—that technology, which has a much longer

lifespan but still creates a threat and can actually stop production of certain products. And we've seen this take place with a variety of pipelines, as well as manufacturing recently. So, we've got to think about our own threats and where do we secure as we're making advances in technology and what that spread could be? So, how do I bake in budget for security principles there? And, at the exact same time, the attackers are taking advantage of this, and they're leveraging new technology. You see hackers building out their own marketplace of tools that's fairly low cost in your ability to attack. We still see very low tech types of attacks. The recent rash of ransomware though the attacker Scattered Spider was through a phone call and social engineering of customer service representatives. Nothing super advanced in terms of gaining the access, and then they're able to deliver. Then we anticipate attackers still being able to use or taking advantage of artificial intelligence, automated threats, and just moving faster through our networks to be able to deliver their effects faster and get what they need while they're also hitting three times. I'm hitting you for ransom, I'm hitting you for your data, then I'm starting to exploit your customers. And, for them, it's about their return on investment, as well. And so we see them leveraging the same technology to scale and grow their own illicit businesses and activities in the same way we see our clients moving and making investments to better deliver their products to their customers.

Leo von Gerlach (15:58.4)

I think I could go on listening to you forever, but I think we also need to come to a close, and that's why I have only one final question, but it may be an important one. So, we see new technologies shooting—and you just addressed that—but then we also read in the newspapers every day—I mean, this week, in particular, the week before the last, just the world was a different one than it was the day before yesterday. We have very, very strong geopolitical tensions, we have shifting alliances, and do you think that this is also something that increases the risk or that changes the risk to any type of organizations, including business organizations?

Charlie Lewis (16:48.0)

I do. And, again, if we were to take it full circle to why when I made the departure from the Army and shifted over and transitioned to consulting with McKinsey, it's how do you identify that—at this stage, business and private sectors are also threatened not just by criminals, as they have been for hundreds of years, but potentially by nation states or other actors operating on behalf of someone else for or due to the support to a government that they may not like. And, so, being aware of how the most sophisticated actors are acting, where they may be targeting because of a shift in the geopolitical environment, and working not just cyber and technology risk as a standalone risk, but in your broader enterprise risk program, which will account for some of that geopolitical risk. And making sure you shift where you think the risk impact and the likelihood of that risk being realized occurs, that allows you to address and think about what do I need to do, what are those threat actor TTPS—tactics, techniques, and procedures—and how do I adjust my own security controls to help meet

that? And then how do—as a CSO or a CIO—how do I inform my C-Suite and my board on what they need to be thinking about in terms of potential risks, and how do we think about it from, one, where we operate as a global company and, two, what our broader market strategy will be. And making sure you integrate it and frame it on those points will help demonstrate how the risk may have shifted and how you, as a security leader, are adapting to it.

Leo von Gerlach (18:30.4)

Charlie, thank you so much. Thank you, certainly, for this contribution but, most importantly, for just making the world a more secure place. That's dearly needed. It was great listening to you, speaking with you. Thank you, everybody, for joining this time, and I hope you tune in when we meet for the next session of The Influencers on Digital Transformation and Law. For now, goodbye, have a good time, all.