Climate Change: Implications for Information Technology and Security
Transcript

Part 1: Risk Amplified by Climate Change; And Opportunities

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT, working on security governance and software assurance. Today I'm pleased to welcome Richard Power, a distinguished Fellow with Carnegie Mellon's CyLab, and the former editorial director for the Computer Security Institute, home of the CSI/FBI Security Survey. Richard and I will be exploring the implications of climate change for information technology as well as for cyber and information security. So welcome Richard, glad to have you with us today.

Richard Power: Very happy to be with you.

Julia Allen: So why are climate change, and the move to more sustainable development, becoming of increasing concern to business leaders? What are you seeing?

Richard Power: Well there's a range of risks that are activated and amplified by the sustainability issues that we are coming up to, as societies and nations, as a planetary society really. And they involve business risks that aren't really being understood all that well. Our conversation is really ahead of the curve, so I'm glad we're having it.

You might look at it in terms of seven areas of risk that are activated or aggravated or amplified by climate change and related sustainability issues. And I'll just go through them quickly.

There's regulatory risk for businesses. Well there's both regulatory risk, in terms of you can expect regulation, and you're going to have to adapt to regulation and all the implications that will come with it. It's also a fact that many businesses are praying for regulation so that they have some guidance because leaders understand what's happening but they don't really know what their role is or how they should deal with it.

There are supply chain risks. You will not be able to assume that everything you get, you will be able to get from everywhere you have gotten it traditionally. Things will change. The supply chain will be impacted in many different ways. And along, all along the supply chain, there will be uneven applications of regulation. In other words, some areas that you're pulling from may have heavier regulation than you do.

Other areas may have laxer ones that conflict with yours. There are a lot of issues there that kind of dovetail with the regulatory risk.

There's also product and technology risk. You've designed your products, you've taken your products to market. Now there are issues about what they produce, how they produce it, what the consequences of using that product or technology are. And so there are issues there.

There are litigation risks. As the situation intensifies, and tensions around it intensify, there will be litigation risks, similar to those that we understand from the tobacco and asbestos and other issues.

There's tremendous financial risk from all of these things that we've just been ticking off, from everything, in terms of the impact of climate change on the consumer society, the impact of climate change on natural resources, the impact of climate change on global trade, and what it takes to ensure your business and to safeguard your business; there are all kinds of financial risks.

And then there's the reputational risk; the issue of corporate social responsibility and where we are in relation to what is perceived as a good corporate social responsibility posture.

But the bigger framework of it is that we have – everyone who works in the field of security and risk, we have – we work in some way or another with a matrix. That risk matrix will vary depending upon your sector, depending upon your area of focus, and other variables. But we're all working one way or another with a risk matrix.

The main point here is that climate change not only is at the top of that risk matrix now; and that's a fact, a truth, if you will, that's not grasped by enough people. Climate change is really now at the top of that risk matrix. But it also impacts every other kind of risk down along the line, whether you're concerned about failed states or you're concerned about disease and pandemics, or you're concerned about terrorism, or you're concerned about environmental threats. All of these things are aggravated by climate change. So it not only moves right to the top of the risk matrix, but it also impacts everything else downstream from it and kind of warps the whole thing. And we have to really come to grips with the fact that the 21st century risk matrix is really profoundly different than the 20th century risk matrix.

Julia Allen: So it's almost like, based on your research and your observations, you're kind of reframing the context for a lot of the traditional risks that we've addressed as a business community, because this particular aspect of our living on the planet is so pervasive and, as you said, kind of touches just about everything.

Richard Power: Yes. And an important thing to remember here is that the other individual risks, whether it be the insider or organized crime, these risks still exist in and of themselves. They still carry all the same issues and threats and factors that they bring with them. But each one of them, some way or another, is interacting with this planetary thing that impacts everything, from the smallest creatures to the

largest global enterprises and nation states. So yes, it's changing everything. At the same time, the individual risks that we deal with on a day-to-day basis don't go away.

Julia Allen: Well you mentioned early on the different kinds of reframing, the risk matrix, or the risk proposition with respect to climate change. Have you found that argument, as well as some others, can be used effectively to position this whole subject to get the attention of C-level executives?

Richard Power: One mistake that many of us make – and I'll include myself – depending on the situation and circumstances, is we tend to typecast people. And the cognition, the awakening, the light bulb going off, the green light bulb going off, in the minds of CIOs, CFOs and CEOs – it really varies a lot. Some people are really onto it, really understand, can't understand why everybody else isn't dealing with this. Others just don't get it. And it's hard to find that kind of magic key that unlocks it for – the common denominator that unlocks it for everybody.

That being said, a friend of mine said, "You're hitting them where they live. You're hitting them at the part of their company they really want to keep green, which is their finances; the cost and the profit and everything else that relates to the profitability and the success of their company." So it really boils down to the economic issues and the economic implications of climate change; the economic implications of not understanding the risks; the economic implications of not understanding the security imperatives of those risks.

What's the return on investment from a sprinkler system in your building? You don't do a risk analysis to decide if you need sprinkler systems. You have to put them in. And a lot of information security is kind of in that realm. It's hard to show the return on investment for something that you really need to do.

This situation, although it's also something we really need to do, it is a security issue. It is easier to show, in spectacular ways, how not only does green save money and save resources, it also is opportunity and opens up new vistas for workers and for entrepreneurs and everything else.

So that's the way to unlock it, is from the positive side; not "Oh my God, Chicken Little, the sky is falling." But this is a tremendous opportunity and we need to get ahead of it for our own profit as well as for our own sense of social responsibility.

Part 2: A Corporate Climate Crisis Strategy for IT and Security: Points 1-4

Julia Allen: Well that's a great segue into my next question, which is – having read your recent article, I was delighted to see that you actually outline a seven-point corporate climate crisis strategy. In other words, you give folks like chief security officers and chief information security officers, a bit of a roadmap that they can use to promote this issue within their organization. So I wonder if you could briefly kind of walk us through those points?

Richard Power: Sure, that's great. Some of this stuff may already be going on in their company. So there are some natural alliances they can form. Some of this stuff they won't be driving, but they can put their own issues and their own imperatives in the context of the overall push to green, in ways that probably others in the boardroom and on the executive row might not have thought, and so it'll strengthen the whole initiative within an enterprise.

So the first one is in terms of intelligence and risk analysis. Not enough companies spend any time – and this is something, this is one of the things that you actually can resource successfully within a company – but they do not spend enough on intelligence and finding out what is going on in the world, what is going on in the region, what is going on in their sector as it relates to their company.

And not enough people are doing that in general. When you ask how many people are doing it in terms of the business risks of climate change, it's almost no one. But they need to be. They need to understand what is happening with the weather; what is happening with resources; what is happening with the supply chain; what is happening with the political scene, the geopolitical scene; the economic issues, global, national and regional. How is climate change developing? Because we have a lot of models, we have a lot of good ideas. Some of them, they're being borne out. But this really is a dynamic and unpredictable area. And so companies have to be paying attention to intelligence.

The second thing is, of course, to understand your carbon footprint. It will really blow your mind when you understand your carbon footprint. And you understand, conversely, how you can impact it in a positive way, how you can reduce it, and the benefits that come with reducing it. So really companies need to get their minds around their carbon footprint. And they might as well do it now because governments, sooner than later, will be compelling them to.

The third issue is to go green, of course, in your company as best you can, as comprehensively as you can, and particularly in the IT environment. This is an environment that uses a tremendous amount of energy now. IT resources consume as much energy right now on the planet as the airline industry. The only difference is the airline industry's consumption is probably stabilized or going down. The IT drain on energy, demand for energy, is escalating exponentially and is really an issue in and of itself. So if you tackle green in your IT environment, you are a long way along the road to where you need to me.

Julia Allen: Well and it also occurs to me – you made the argument, about the financial argument. I suspect this is where some real significant cost savings can occur.

Richard Power: It is very impressive. And in the article I referenced some conversation I had with IBM. It's a very impressive story what they've been able to do in terms of greening their own enterprise and helping their clients do it. This is not only – many companies going this way now. The cost savings are really impressive, and exciting, and could not be lost on anyone.

And the fourth thing is really significant, and that's business continuity, crisis management, and disaster recovery; re-evaluating and revising your plans and capabilities. Every organization by now has a business continuity plan. It sits on a shelf and collects dust. When you ask people about it, "This is what we do, when something, if something happens." And the model, the paradigm of those plans is, "This is what we will do if something happens someday."

But the paradigm for the 21st century, the century of climate crisis, has to be more like, "This is what we will do because multiple things will happen frequently, and in ways that haven't happened before. And we have to be flexible, adaptable, and develop capabilities and resources that we haven't really thought through in the past."

We just had tornadoes in downtown Atlanta. There've always been hurricanes in the Caribbean, but they are going to be bigger, they're going to last longer. They're going to come in, like Katrina did, come in, hit one state, go back out, get stronger, come in, and devastate a whole city.

This is a different time. And we need to understand that just because an area's always had flooding and they think they understand what to do about flooding, it's going to be different. The flooding is going to be more frequent, more intense. Or they could no longer have floods and be faced with some other extreme weather issue, and an area that's never had flooding could have flooding. Or you could have population displacement from one part of the country, or one part of the continent, to another that completely changes your paradigm. Or conversely, you might be displaced. So it's just a different approach to crisis management, business continuity – to deal with a different time and a different threat matrix.

Part 3: Strategy Points 5-7; and the Role of CSOs/CISOs

And the fifth one is something that is so economical and so effective and so positive. All of us by now, most enterprises by now, have some form or another of awareness and education program for security, for workplace violence, for all kinds of things, for the various social causes that they're impacting.

These awareness and education programs are delivery systems for the workforce. You can tell your workforce – you can offer them guidance on going green, not only in the workplace but in their personal lives, to prepare them psychologically and to prepare them in ways that they can make their own decisions about their own home crisis management plans and their own home economic issues, and help them wake up to the situation and provide them with the resources they need in their lives.

Julia Allen: You mentioned security awareness. A lot of the venues I've participated in, we regularly talk about you need to make security personal.

Richard Power: Exactly.

Julia Allen: You need to have meaning at the level of an individual's behavior and actions and motivations, regardless of home, work, wherever. And what I hear you saying is, I think even in a more compelling way, that that's the argument here. You need to get people thinking about this as part of their day-to-day walk through life.

Richard Power: Yes, exactly because then, again that green light bulb goes off in your mind. But when you talk to somebody about information security in the workplace, I've found that it's much better if you can also talk to them about their home PC security, and child safety online, and identity theft. Because if they see the issues, how they impact them personally, just like you said, then they understand the issues in the workplace better. And it's not just something somebody's telling them they have to do, that's making their job more difficult. It's something, an education and awareness effort, that's empowering them to be able to protect themselves, and their job in the cyber world. Yes, same thing with climate change; exactly.

Julia Allen: Okay. And your remaining two steps?

Richard Power: Yes, the sixth one relates to mobility, travel security, as a whole context. It's not as simple as, "We're going to decree less travel to reduce the size of our carbon footprint." Because that has with it a whole bunch of implications about information security and flexibility and availability and everything else. And you have to look at the whole thing. Because really what you're looking for is mobility. You want your workforce to be able to work in the office, at home, on the road, with the same seamlessness, the same efficiency, the same access, the same interoperability and performance, and everything else. You need to be able to really be mobile and all that means.

And then the fourth [seventh] one, of course, is cyber security, and we touched on it a little bit in terms of the technological vulnerabilities that may open up as we go green. But it goes again back to the beginning of information security: confidentiality, integrity and availability. Of course, that's not all information security is, but that's a lot of what it is. And climate change really impacts all of those: availability, in the obvious way; confidentiality and integrity in terms of the vulnerabilities that may open up as we do computing in a whole new way.

So these are the seven elements that I stress when I talk to people.

Julia Allen: And it occurs to me, in listening to you speak and laying out these points, that the chief information security officer, or the equivalent, can actually serve as the catalyst...

Richard Power: Absolutely.

Julia Allen: ...both for raising awareness on this whole issue, but ensuring that security is part of the beginning of these conversations, right?

Richard Power: Absolutely. If you think about Y2K, this was something that had to be done, that was so successfully dealt with that most people think it didn't have to be dealt with.

But climate change is something that is now inexorable. And the only question is whether we can adapt to it in time to make a difference, and also how it will all play out. Because no one really can know, except that something – it will be different.

And so this is something that the CSO, in particular, can drive within his organization from – and at the end of, once you get that leverage, once you get that moving, that whole issue of return on investment on security kind of fades in the background, because you understand something, which has been true all along; that it's really, security is about protecting what you love – your business, your family, whatever it is. It's about protecting your assets, protecting what is of value to you.

Julia Allen: Well Richard, you've certainly gotten us thinking about the subject, and I feel like we're probably just beginning a very, very important conversation. In addition to your article, do you have some places where our listeners can learn more on the subject, either in general or specifically with respect to the connections with IT and information security?

Richard Power: Well there's a lot out there. In terms of the connection to IT, the U.N. Initiative, the Global e-Sustainability Initiative, is an interesting one and important one that I encourage people to take a look at and the things that flow out of that.

And then in the U.S., the Alliance for Climate Protection is doing a lot of important work and they're something that people can look into.

Julia Allen: Well I so appreciate your taking the time today, sharing your insights and observation and your expertise with our listeners. I've really enjoyed our conversation.

Richard Power: Well I've enjoyed it a lot, and I really thank you for identifying the issue and asking me to talk about it with you.