How the Cyber Insurance is Driving Risk and Technology Management

Part 1: Cyber Insurance as a Risk Management Strategy

Lisa Young: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division 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 Lisa Young. I'm a member of the CERT Cyber Risk Management Team, and I'm pleased to welcome Chip Block, Vice President of Evolver, a supplier of cybersecurity and infrastructure services to the commercial and public sector.

Today, we'll be discussing Chip's take on how the cyber insurance industry is beginning to drive cybersecurity technology. This is our second podcast in the insurance series. Feel free to check out the earlier one. So without further ado, welcome to the podcast series, Chip.

Chip Block: Thank you, Lisa. I appreciate the opportunity.

Lisa Young: Well, we're happy to have you here, so can you tell us then, can you start with sort of foundational -- what is driving or what are some of the driving factors in the growth of cyber insurance?

Chip Block: A recent study by Advisen has shown that there's been about a 50 percent increase in cyber insurance (demand). And I believe the reason for this is the obvious increase in activity, whether it be Target or Home Depot, Sony, and of course, OPM. There's been lots of high publicity in the cyber arena.

What's happening is that companies are now turning to looking at this problem as a risk problem, as opposed to just kind of a technical problem. And that is getting the attention of the C-level folks within organizations.

Lisa Young: Oh well, that's very interesting. So then can you tell me about how does cyber insurance fit into an organization's risk management strategy?

Chip Block: So the main thing is that companies, as I mentioned, are looking at this as a risk problem. I like to equate it to the weather. We used to look at cyber as this black and white technical issue where you went to your technical staff and you said, "Fix this problem for me."

Well, it really is no longer like that. It is now something that is so frequent and is happening at such a level that it's, I think the head of cyber, or cyber group within the Defense Department had made a statement that said, "It's not if you get hacked, it's when you get hacked." So companies are now looking at this kind of at a risk situation, which is, "How do I address risk?" And as soon as you get into a risk structure, the most logical thing that happens is you start looking at, "How do I address risk?" And that's the C-level activities.

Lisa Young: So sure. As a tool then for part of your risk management strategy, I can see that cybersecurity insurance would be really important in that arena.

Chip Block: Exactly. So that's how most --if you go to most board meetings, what is the primary topic? It is risk. And how do companies handle risk today, whether it be anything from fiduciary risk or to natural disaster? They handle it with insurance.

Lisa Young: Ah, great. All right. Well, then, talking about some research that you've been conducting in this community, how do you foresee cyber insurance changing how technologies are developed and sold? Can you say more about that?

Chip Block: Yes. So cyber insurance has been around for quite a while, but what wasn't there before was any real strength in the offerings from the company, the insurance companies, whether it be the major companies such as AIG or the smaller companies. And the main reason for that was that there wasn't enough data.

Cyber activities came and went and there was no real strength in the data. Well, the increase in cyber- attacks has now, is now being captured by companies such as Verizon and NetDiligence and Advisen, who are now able to actually give some kind of quantifiable numbers that says, "This type of attack results in this type of a loss." And as that's happening, then the cyber insurance world is accelerating because the insurance companies can actually start putting actual quantifiable data against a possible attack. And I think that's what's driving a lot of the increase in the insurance industry.

Lisa Young: Sure. Well, that makes sense, because that's how we do it in other fields where we purchase insurance like automotive or homeowner's insurance. So it makes sense that all this data would be collected.

So can you say anything about -- we're going to have in the show notes for those listeners a white paper that Chip has published about this subject -- but you discuss in your paper something called coding of risk. What is this and how does it work?

Chip Block: So as you just mentioned, if you think about all of our insurance programs that are out there, whether it be your house or your car, the insurance companies take a look at what you own or what your assets are and they put a dollar value against that and then they say, "This is the risk to that."

Well, the coding, is the insurance way of quantifying those risks. So for an insurance side, the cyber insurance side, there are now groups that are getting together and they're coming up with these standard codes that says, "Here are the five, six, seven types of risks to a company that they have to face because of a cyber-attack."

So, last year, what was called the Chief Risk Officers Forum in Europe, they all got together and they quantified the different types of risks. And they had what are called first-party risks and those included things such as interruption of business, restoration costs, or the one that we're hearing lot about these days is cyber extortion. So they're going through and looking at a company and saying, "This is your risk for each of those areas."

Lisa Young: So it gives them a way to say if, perhaps, what might be the loss or the impact given a certain situation.

Chip Block: Correct.

Lisa Young: And so what did they find in some of these first-party risks? So first-party risks then are the things that happen to me as an organization?

Chip Block: Correct. So as an example, one of the easy ones would be business interruption. So let's say you have a business, a retail business, and your website, critical to your website is your purchasing system. Well, if somebody hacks into your purchasing system and you're down for two days, they can calculate how much loss you would see over a two-day interruption of your business. And their insurance would then put a dollar value against that and then it would cover that loss over those two days of lost activity.

Lisa Young: So for our listeners then, Chip, can you talk about some of the other things you mentioned, tell me more about this Internet of Things.

Chip Block: And that's an interesting topic on the cyber insurance side, because right now most of the cyber insurance world has been dealing with data. And we all know about breaches and the loss of data and the loss of your credit card or your social security number.

When you get to the Internet of Things, now the risk gets much greater. You're now talking about physical and even human harm. If you've been watching the news, several folks found out that they could hack a Chrysler, actually it was a Fiat, and stop the car, remotely. And that caused a recall of millions of cars around the world because of a cyber problem.

On the Internet of Things issue, that could be anything from a medical device, to an elevator, to an automobile. And now the risk gets much greater and different in the sense that the insurance companies are now going to have to look at this not just from a loss of data perspective, but everything from physical harm to a person or loss of something material. So there's lots of discussion about how cyber-attacks to Internet of Things will be addressed in the future.

Lisa Young: Well, sure. You bring up a good point, because the Internet of Things, really what that does, is it just expands the cyber ecosystem to be inclusive of things that we've never really thought of before as being connected or being physically able to be controlled from cyber technology.

Chip Block: Exactly. And as with all cyber things, the challenge of identifying the cause becomes much greater, because if somebody hacked into something physical like a car, how -- was it the driver's fault, was it a cyber-attack? It opens up an entirely new technology area that's going to have to be addressed.

Lisa Young: Right. Okay. And that actually then brings us back to the coding of cyber risk. So as you think about these cyber physical incidents or Internet of Things, I think the market for technology and insurance actually then grows exponentially.

Chip Block: It does. If you have, again, the elevators in your building or your automobiles or your medical devices, you may be having riders on your current insurance that cover cyber activities.

Part 2: FUD, Risk Quantification, and a $10 Horse

Lisa Young: Ah, I see. Well also that brings you back to your previous point about how this might change technology purchasing, because I would think that chief risk officers or technology folks would be able to then figure out how much to spend to address some of these things in addition to insurance. Can you, have you, heard anything about that?

Chip Block: Exactly. Because our current business model for selling technology is what I call the fear, uncertainty, and doubt model. What that means is that technology people show up at companies and they try to scare the chief information security officer or whoever they're dealing with more than the last guy scared him.

So if somebody comes in and says, "You need to buy my new firewall protection, "or “my new vulnerability scanner, "if the customer says," Well, I just bought stuff two weeks ago. Why should I buy your stuff?" The salesperson tries to scare the clients into that he's not covered for this vulnerability or that type of attack and it is, it's really a fear model. And that's really not a sustainable model as an industry goes. You can only scare people so much.

Lisa Young: So that's a great point. So then thinking about how technology is developed and sold, now we're sort of in the fear, uncertainty, and doubt, but insurance, cyber insurance, gives you a broader brush picture? I think that's why --

Chip Block: Exactly.

Lisa Young: Yeah, go ahead.

Chip Block: And they put numbers on it. So now, if I came in and said that your business disruption loss could be a million dollars, then if I was buying technology products to avoid that type of disruption, I would have some kind of level of understanding. Maybe I'd spend $50,000 to protect a million dollars' worth of assets, where right now, without those type of quantifiable numbers, it's just a pure guess.

So, I heard an interesting phrase by the CISO from the state of Texas who says, “In Texas you don't put a hundred dollar fence around a $10 horse.” This is the same thing. If your risk is only several hundred thousand dollars, you wouldn't want to spend half of that on technology. That doesn't make sense.

Lisa Young: And so this notion of coding and being able to assign quantitative value to cyber risk, that really helps. Can you talk more about how do you think coding risk will help improve the cybersecurity practices of different organizations?

Chip Block: So I think what it will do is then it will start to provide more focus not only on the buyers but on the sellers. And I actually believe that will also help the technology, because we will end up with different product sets that match the risk of what they're trying to protect. So if you're a small, mid-size firm and your risk is one level, you'll buy a product set that matches that, where if you're a major international company, you may buy higher-end products that do more things but that also match the risk that you're protecting against, that you're protecting from.

Lisa Young: Sure. And that's actually a really good point, because today it seems like organizations are trying to solve this by buying all kinds of technology without really understanding a), their risk profile, or b), what is specifically needed?

Chip Block: Exactly.

Lisa Young: Yeah. So this gives a better sort of decision-making to the spend then, if you will. Okay. Well, that's a great strategy.

All right. So then can you talk about in terms of risk management and cyber insurance, can you see how you see this playing out and what might be next organizations should pay attention to?

Chip Block: There’s a couple of things. There's two primary areas. One of them is you talk about the risk management capabilities. One of the key things is in order for this to work then there's going to need to be tools and capabilities in order to measure that risk. And I think you're seeing some of that, such as the CERT Resilience Management model that I know you guys have worked on. There are products now that are coming out. I think there's some product called Risk Lens and others that people are able to actually use to monitor what the risk is for different companies.

So I think there's going to be a whole business growth in that. I think the most critical thing is this concept of commercially reasonable, which is if you got hacked as a company, did you take proper actions to avoid that hack based on commercially reasonable actions? Just like your house -- if you had water damage but you treated your house properly and there was nothing you could do, insurance will pay for that.

On the other hand, if you left the water running all night long, and it ran, it was your own action and you were negligent, they're not going to pay it. Well, that's the same thing that is happening now, which is what is the definition of commercially reasonable? And I think there's standards, the NIST Cybersecurity Framework, and other things are starting to be defined that are defining what that is.

Lisa Young: Well, I was going to say, that makes sense to me, because basically then you can determine the pricing of insurance and other technologies based on how well someone might -- how good their cybersecurity practices actually are in the organization.

Part 3: Secondary Services; Emerging Drivers

Chip Block: Exactly. I think the other area that will happen out of the natural growth will be a secondary market of businesses that leverage off the cyber insurance world. If you think about, say, any other insurance, like your car, there's not only the insurance company, there is the vehicle repair office that responds to the insurance, there are the adjusters, there's the actuaries. There's a whole secondary level of businesses that respond to the insurance group. And I think you're going to see the same thing here in terms of forensics companies, vulnerability assessment companies that will grow in response to the insurance industry.

Lisa Young: Sure. That brings up an interesting point. I've seen some cyber insurance policies where if you buy coverage with a, or a certain type of coverage, the insurance company will actually have vendors to provide these services for you, to understand some of the root causes of what actually happened in the attack or in the event or incident.

Chip Block: Exactly. They are already beginning that type of growth of those other vendors to support the insurance industry.

Lisa Young: All right. So Chip then, can you tell us what other types of events or what other things do you see driving the cyber insurance industry?

Chip Block: Yes. There's been several court cases lately that I think will accelerate cyber insurance mainly because of rulings affecting who can, if you would, sue somebody about a cyber-breach?

One of them is, it's called the Advocate Medical Group, which was a case from 2013, where the courts ruled that unless somebody can prove direct harm, they really can't sue you for loss of data. So if, on the Target example, if your credit card was taken, you don't really have a case against Target unless you can prove that your credit card stolen from Target directly harms you, which is going to be very difficult to claim. Well, I think that will increase insurance, because that's one of the big risk areas, right? Those big cyber, I mean, those big class action suits.

Lisa Young: Right.

Chip Block: This is minimizing that risk, which will increase the use of insurance, because the insurance folks are taking that really big risk off the table, which is massive class action suits.

Now, having said that, a corollary to that was the FTC ruling on the Wyndham case, which is that the Federal Trade Commission can actually sue a company for not having proper control of their data. So that increases a risk that insurance folks will have to address.

So this, as these cases go through the courts, that's going to change the insurance landscape as more and more case law comes out and gives more specifics on what is a risk and what is not a risk.

Lisa Young: Okay. Great. Well, that's actually really interesting. Thank you for that. So then where can our listeners learn more about this subject?

Chip Block: So the paper that you referenced before is called, "And Then the Accountants Showed Up: How the Insurance Industry Will Drive CyberSecurity." And they can find that paper on www.evolverinc.com. There's also a lot of information out there from groups such as Advisen. AIG is a leader in this business. There are other groups that are holding conferences. If you actually search the web for cyber insurance conferences, you'll find one almost every week.

So there's a lot of information that's growing out of this, and I would recommend everybody take a look at not only cyber insurance, but their specific industry and how cyber insurance is being applied.

Lisa Young: Oh. That's a good point too. So there's some diversity in the coverage based on what kind of business you're in then.

Chip Block: Yes, there is.

Lisa Young: Okay. Great. All right. Thank you, Chip. We really appreciate your time, being here with us today, and sharing this information.