Cyber Insurance and Its Role in Mitigating Cybersecurity Risk
Transcript

Part 1: Defining Cyber Insurance; Positioning It as a Security Control

Julia Allen: Welcome to CERT's Podcast Series: Security for Business Leaders. The CERT Division is part of the Software Engineering Institute. We are 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 principal researcher at CERT working in operational resilience. I'm very pleased today to welcome back two of my favorite people to talk about something really fun. Jim Cebula is the Technical Manager of CERT's Cybersecurity Risk Management Team. I work closely with Jim.

And I'd also like to welcome back David White. Dave is the Chief Knowledge Officer for Axio Global. The fun thing about Dave is he was previously with CERT and worked closely with Jim and me on many activities including models for improving operational resilience and cybersecurity. So it's great to have Dave back.

Today, we will all be discussing a new topic for the podcast series: cyber insurance and its potential role in reducing operational and cybersecurity risk. It has a very specific role to play as we all think about controls for protecting our organizations and networks. And our plans are that this be the first in a series on that topic.

So with no further ado, welcome back to the podcast series Jim, happy to have you today.

Jim Cebula: Well thank you Julia. It's a pleasure to be back here again; and it's very exciting to have Dave back with us as well.

Julia Allen: Absolutely. So Dave, great to have you with us. Thanks so much for making the time and really looking forward to picking your brain to see, hear more about all the things that you've learned since you've left CERT.

David White: Julia and Jim, it's a great pleasure to be with you and it's hopefully the beginning of a new collaboration.

Julia Allen: Absolutely.

David White: I'm thrilled to be talking with you and Jim about this today.

Julia Allen: Excellent. So Jim, just to lay the foundation, to make sure for our listeners' benefit we're all on the same page, could you just start to frame when we say "cyber insurance" what do we mean and what does it typically cover?

Jim Cebula: Sure. Thanks Julia. So typically what we're talking about here is organizations buying some insurance coverage to deal with basically first-party costs associated with a breach -- things like hiring a forensics firm, conducting the investigation, things like this; in addition to costs that you might incur of terms of making customers whole in the event of a breach, when you have breaches involving things like credit cards, and where you've got fraudulent charges that accrue to your customers as a result of that credit card data being

breached; other liabilities that might come out of a situation like that, such as costs that the banks may try to claw back in terms of reissuing those credit cards, providing credit monitoring service for your customers, expenses like this. So those are -- that's what people are purchasing coverage for, particularly here, here in the United States.

Julia Allen: Great. And I know as we were preparing for the podcast today, Dave, you said that in Europe in terms of some of the customers that you're dealing with, they have a slightly different take on when they talk about cyber insurance, what they mean. So could you say a little bit about that?

David White: Yes. So it's interesting. One of the things that I've observed -- I think there's a much bigger market for cyber insurance in the United States than there is in other parts of the world, based on what I've learned.

And the market in the U.S. is driven largely by all of the breach notification laws that we have in the U.S. So there are, I think, currently 46 states have breach notification laws. Forgive me if I get that statistic wrong. I know it's in the 40s. But that drives responsibility on the part of organizations that have data beaches relative to what they must do under the law; and that's really driven the proliferation of the kind of insurance that Jim talked about in the U.S.

In Europe, there aren't currently any breach notification laws. It's my understanding the EU is working on a breach notification law and I expect that the market will change in Europe after that law is in place. But in Europe oftentimes when you talk to an organization about cyber insurance, what they think you're talking about is coverage for business interruption -- so non-physical damage business interruption, because physical damage business interruption is typically covered under your property policy but there are other ways today for businesses to be interrupted.

For example, if you're dependent on sales through your website and your website gets DDoS attacked, then you may be knocked offline and that would cause -- it could cause substantial damages to you in terms of lost revenue or lost sales. And so you can buy insurance called non-physical damage business interruption, or some people call it network business interruption, to cover that. That's more popular in Europe than it is here.

David White: I think it's important to know what's not covered as well as to know what is covered, right? And so most of the cyber insurance policies today -- and I say 'most' because of some new products that are just now on the market. But the kind of policies that Jim was talking about explicitly exclude covering damages that are tangible.

So they don't cover property damage or bodily injury. They don't cover any physical damages from a cyber event. And so as you start looking at critical infrastructure, that kind of damage from a cyber event is also important; and there are new coverages that are coming to market that address that.

The way that I think and the way that Axio is trying to position cyber insurance is as another cybersecurity control. We think that it's powerful for organizations, and security leaders in particular, to think about cyber insurance as another control that's in the toolkit, okay? Graphically I think about it as follows.

So you can imagine in an organization that's doing, that has some dependence on technology -- and imagine an organization that's doing absolutely nothing about cybersecurity. Their potential risk impact is really off the charts, right? You can think of them as having low

cybersecurity capability and the risk axis then, or the Y axis, the risk impact would be off the charts. And as they start to make investments in cybersecurity controls or improving their cybersecurity capabilities, that risk curve starts to drive down and there's a diminishing return to scale. So the curve starts to flatten out because you can never get rid of all of the risk, right? But there are a lot of things that you can do to reduce the risk to the organization by implementing controls.

So I think of a cybersecurity control as -- all cybersecurity controls are constraints in some way, right? So they constrain operations. And they have the impact or they have the effect of reducing the risk or reducing the risk impact to the organization. And so when you get to the flat part of the curve is a really good time to think about an investment in cyber insurance. Because cyber insurance you can think of as actually moving that whole curve down; as a control it functions directly on the impact.

So it minimizes the amount of the financial impact that would hit the company's balance sheet or the bottom line really. And so in that way it's a really powerful control. The reason I think that it's important to apply it when you get into the flat part of the curve is because you might not get -- you might not be able to get a good price for it if you're over at the left side of the curve where the risk is really high; but when you're in the flat part of the curve is where you'll get the best bang for the buck on an investment in cyber insurance.

Julia Allen: Right, so if I think about what you're saying and I think about an organization who's looking at cyber insurance as one way to mitigate risk, would it be fair to say that you're really saying to them, “You really need to have your house in order; you need to do the hygiene things, you need to have a basic program in place, you need to be doing some right due diligence kinds of things.”

Otherwise you're likely not to get anywhere close to decent rates on your cyber insurance because you've got too much exposure, too high risk. Would that be a fair statement?

David White: I think that is a fair statement and I think insurers are getting better and better at their underwriting evaluations to figure out whether you represent a good risk, right? And so from an insurer's perspective, insurers always need to avoid what we call the "moral hazard," right?

As an insurer you'd never want to sell a fire insurance policy on a building that was burning, right? You never want to insure a burning building. And so the same is true on the cybersecurity front where insurers want to make sure that they're taking a good risk by selling a policy to somebody. And so they do some underwriting diligence to make sure that you've got those hygiene activities in order before they place the policy.

Part 2: How Cyber Insurance Is Being Used Today; New, Emerging Products

Julia Allen: Great. And Jim, from your perspective with the customer base that you work with, are you seeing cyber risk insurance pop up in any particular ways?

Jim Cebula: Yes, we'll talk about that. I just wanted to comment though. I think that the discussion that you and Dave just had really hits the mark for me in terms of our thinking in the work we've done to date -- describing this as basically another tool in the toolbox of controls and controls operate along a spectrum.

So the cyber insurance, as Dave Described, talking about that flat part of the curve, it really does work best in organizations that have a handle already on where their risks are and they're making a conscious decision to deal with some of the residual or excess risks and liabilities that might accrue from those risks through the purchase of insurance. They're not buying insurance as a way to get out of doing the basic hygiene and blocking and tackling the way you described, Julia.

Back to the question, with respect to our customer base -- so there's been some significant interest on the part of DHS, Department of Homeland Security, in the cyber risk insurance market in terms of incentivizing industry, in particular critical infrastructure owners and operators, critical infrastructure providers, to adopt the NIST Cyber Security Framework (CSF).

And so the NIST CSF was introduced approximately a year ago as a result of a presidential executive order; and it provides a basic framework for cyber security practices, policies, geared really towards the critical infrastructure, which is to a large degree under the control and ownership of private industry.

And the CSF is not a regulatory framework, it's not a mandate. It was developed in a collaborative process with academia, industry, and government and DHS is trying to encourage voluntary adoption.

So one of the thoughts was to try and get the cyber insurance industry behind the idea that if a private sector organization comes along and says, "We've undergone a process to align our internal controls with the principles in the NIST Cybersecurity Framework" that the insurers would then look favorably upon that in terms of offering insurance or offering it at favorable rates or perhaps at higher limits.

Julia Allen: Yes that makes a lot of sense. So to build on that Jim -- and then Dave I'd like to bring you back in as well -- so we've talked a little bit about what it is and the role cyber insurance might play in helping mitigate risk against something like the NIST Cybersecurity Framework or other similar frameworks.

But when it really comes down to it Jim, how broadly, in your observation, is it actually being used today? In other words, what would you say is the current state of the practice? And maybe a little bit about some near term trends. So what do you see?

Jim Cebula: Yes so what we're seeing is -- so the market is definitely expanding; interest in this kind of insurance is definitely growing. And there's more uptake with larger organizations.

We're seeing and hearing from folks in the industry that we've been collaborating with that the challenge right now really is in the small and medium business market, where you have a small organization that perhaps does not have the resources to have.

For example, dedicated staff dealing with cybersecurity issues; an organization like that coming into the insurance market and running into some difficulties in terms of responding to a questionnaire about their security controls or undergoing some kind of a review from the insurer to ascertain like what is the state of their security practices and their -- what indicators of maturity are we finding in terms of cybersecurity in this organization?

So we're finding that as a challenge area for the industry right now, particularly among the small and medium businesses. So large organizations are out there; they're buying coverage. They're typically more sophisticated; they have dedicated staff, they have people at the

executive level with oversight of cybersecurity, people in CISO (Chief Information Security Officer), Chief Risk Officer roles like this.

However, on the insurer side, the market is still relatively new compared to some other forms of insurance. So one of the things that we are finding is that larger organizations want to buy more coverage and they want higher limits.

They're having to go put together basically a package involving several insurers because each individual insurer wants to -- they're setting limits on the amount of coverage that they'll write as a way to manage their exposure in the absence of more sophisticated actuarial data analysis and other tools that they typically have at their disposal in other types of coverage.

Julia Allen: So did you want to comment on that, Dave, in terms of what you're seeing on uptake and the current state of the practice? And then we can talk a little bit about new and emerging coverages.

David White: Sure, sure. So completely agree with Jim that large organizations are the sophisticated buyers of this type of coverage and they are largely participating in the kind of cyber insurance that's available that Jim described earlier.

So recently, I was at an insurance industry roundtable meeting at the U.S. Treasury and heard some interesting stats shared by some of my colleagues in the insurance industry. One was that one broker reported that by their analysis 50 percent of the Fortune 250 firms are buying cyber insurance currently; and they forecast that that number will climb to 70 percent within two years. Now that said, the insurance industry considers this coverage to be relatively immature in its market takeup.

The industry views it as having a relatively low market absorption at this point in time and there is a lot of growth. The primary sectors that buy this kind of coverage are finance, health care, and retail. Those are definitely the top three. And then the second tier would be technology firms and educational entities.

And if you think about those businesses and the kind of coverage that's currently available, those business sectors are the sectors that deal with a lot of personally identifiable information or credit card information or protected health information. So it makes sense that they're the ones who are buying this kind of coverage to protect them from that risk.

If you look at the overall cyber insurance market compared to other insurance markets, you get a sense for how small it really is. So total annual premiums worldwide for cyber insurance at this point in time are around 1.3 billion dollars. And if you compare that to property insurance, annual premiums in the property insurance world are well north of 100 billion dollars. So it's a very small industry compared to the most popular kind of insurance that we all know about, which is property insurance.

Julia Allen: Right, and what do you see as some of the new problem spaces, the new emerging trends; maybe some of the new coverages that are starting to pop up, which will perhaps cause that market to grow a bit?

David White: Well I think there are new products coming into the U.S. market that address the business interruption risk that we talked about earlier. The products that I'm very excited about from a critical infrastructure perspective -- you and Jim and I have done lots of work in the critical infrastructure space in our Careers -- and a lot of those entities have a very different risk

profile because in a lot of those industries you deal with interactions between software and technology and physical devices.
So you deal with control systems; and those open an entirely new spectrum of cyber risk, which is the risk of physical damage and bodily injury or property damage and bodily injury from a cyber event.

There are a number of companies that have introduced this year policies that address that risk specifically. One of them is AIG. Their product is called CyberEdge PC. There's another company called Aegis and they have a product that addresses this kind of risk. And so these products are brand new to the marketplace.

We're finding that companies that buy cyber insurance are struggling a little bit with understanding how to fine tune their insurance program to best meet their risk Exposure, especially because a lot of organizations -- if you imagine a U.S. utility for example. So there's a utility that probably takes credit card payments or bank transfer payments. So they're dealing with payment card data. They may have asked you for a -- they may have performed a credit check when you opened your account. So they may have some other sort of sensitive data about your credit history.

And they're dealing with this critical infrastructure risk that could cross that spectrum into tangible damage from a cyber event. And so for organizations like that, the kind of coverage that makes sense is probably a blend because they definitely need some breach coverage but they also may want to -- they may have some exclusions in their property program that would prevent their property policy from responding to physical damages from cyber risk. So they may want one of these new policies to cover that kind of risk, if that's on their radar.

Julia Allen: Great. And Jim, before we move on, did you want to say anything about what you are seeing in terms of any new or emerging coverages?

Jim Cebula: I know we had talked earlier about things that are generally not covered in this space. And so there continues to be a gap in terms of coverage for loss of intellectual property, right? That continues to be a space where there's really not coverage under a cyber policy for losses associated with somebody misappropriating the organization's intellectual property.

Part 3: Challenges for Consumers and Insurers; CERT Areas of Research

Julia Allen: Okay great. So we've talked about current state of the market, what might be happening, how to position it with respect to cyber risk management. But there clearly are challenges from both a consumer and an insurer perspective.

So Dave, why don't you start us off on that one? What are you seeing in the marketplace that are some of the challenges that both consumers and insurers might be facing?

David White: Sure. I think that one of the challenges that insurers are facing is similar to the challenge that we see lots of organizations facing, which is that there's a shortage in the marketplace of people that have cybersecurity skills.

So as insurers try to build or supplement their underwriting teams with people who understand this risk, they're finding it difficult to hire those people. And we know that DHS and lots of other organizations have published reports on the shortage of people with the right skill sets to improve cybersecurity. That's a big challenge that we all face in our cybersecurity program is finding skilled people. So that's one of the challenges.

Another challenge I think the insurers face is the challenge of understanding enough about an organization in a brief interaction that occurs during the underwriting process to know whether they're taking on a good risk, right? Because there are 50 different insurers who are providing this kind of coverage.

So there's market pressure to make the underwriting process as lightweight as possible. And certainly CISOs in organizations and risk managers in organizations don't want to spend a lot of time filling out forms or participating in interviews or undergoing evaluations for underwriting. And so figuring out how to do good underwriting in a light touch manner is a big challenge that I think the industry faces.

Julia Allen: Great, great. Thank you. Yes just being able to get your pulse on how prepared an organization is and therefore how much risk exposure there is to me seems -- it's something that we try to do for ourselves and now we've asked another party, an outside insurer, to evaluate on our behalf.

So Jim, your thoughts about challenges for consumers and insurers?

Jim Cebula: So it really comes down to being a measurement problem. What are the appropriate measures, the appropriate metrics, the appropriate factors, indicators, that can be looked at, both by the organization that's seeking to purchase insurance and by the insurance company or the underwriter on behalf of the insurance company?

To take a look at an organization, gather a lightweight amount of data but yet have it be impactful in terms of getting a good handle on that organization's state of security to give you the indication about where they fit on a spectrum relative to how much risk are we actually trying to ensure here in terms of writing the policy?

So I think that's one of the key challenges; and that of course feeds right back into: Okay, what are the basic and more advanced practices, tools, and techniques that the organization has in place? We talked earlier about the challenges of the small and medium business sector where some of those may not be as robust or as advanced.

And then Dave brought up also the very real issue of skilled people and finding enough people with the technical skills in cyber, both on the organization side and now increasingly on the insurer side.

I'd even, I guess venture to take that a step further and say that what you're really talking about here in insurance is not only somebody that understands the technical aspects of cybersecurity, but also somebody that can then translate that into business terminology that people at senior management levels in the organization, and business folks on the insurance side can understand, right?

How do we translate the details of technical vulnerabilities into the business impacts and potential monetary loss or exposure to the organization, right?

Julia Allen: Right, well that makes sense. Because as security professionals, we're all faced with that challenge when it just comes to putting a fundamental security program in place and being able to justify investments. And now we've added cyber insurance to the mix where the business may already have a very strong view on the role that cyber insurance is intended to play, right?

Jim Cebula: Yes.

David White: Yes, I think that's a great point that on the consumer side there is the challenge of fine tuning your program to your risk. And in order to do that, you have to understand your current program and you have to understand your current risk, and both of those are changing. So you're understanding one changing, one moving target compared to another moving target, and you're trying to optimize them.

I recently talked to a risk manager at a large U.S. organization and he said that in his opinion it took him seven years to get his cybersecurity, or cyber insurance program fine-tuned to the point that he really thinks that it matches their risk profile, right?

And I was listening to that and saying, “Well that seems like a really long time.” But if you think seven years, the nature of the risk has changed quite dramatically in seven years and the insurance market has also changed quite dramatically in seven years. So it might be that the market has just now matured to the point that he gets the coverage that he needs, right?

Julia Allen: Yes that's a good reality check on not proceeding into this thinking that it's going to be a problem that you're going to solve overnight, right?

David White: Right.

Julia Allen: So Jim, as we come to our close, could you say a bit about why the CERT Division at the Software Engineering Institute has specifically decided to conduct research in cyber insurance. It may not be something that most would typically think of when they think of CERT, and a little bit about what areas you are investigating.

Jim Cebula: Sure. We have a whole spectrum of expertise at CERT, all the way from folks doing very detailed technical analyses, all the way up through trying to translate and make security tangible for senior leaders in private sector and government organizations.

And so in that regard, this idea of how do we come up with a way to describe security vulnerabilities and security events in business language, which in most cases means coming up with some way to monetize those risks or kind of describe them in terms of dollars and cents' impact to a senior business leader, not in a bits and bytes sense, right?

So the insurance space jumped out to us as one place where we might be able to find people that either have some ideas about how to do that, because essentially that's what the insurers are trying to do when they're evaluating an organization, right? They're trying to basically put a dollar figure on what kind of cyber risk exposure am I talking about here? Or people that would be interested in helping to develop some new materials or techniques in that space.

Second, I think would be the idea of measurement and analysis of data, which is historically an area where CERT has been involved in a whole range of cyber security activities, right? So how do we take the appropriate measurements? Can we develop more repeatable, reliable but yet not onerous ways to measure the state of security of an organization and have that be meaningful in terms of their cybersecurity?

And then in terms of data analysis -- so there are cyber events and incidents happening each day. Is there room for better or more analysis? Is there room to develop -- I'll even go so far as

to say like a repository or a kind of clearinghouse of this kind of information, and do some analysis on it to benefit both private industry, government, and folks on the insurance side? So those are kind of the three areas that caused us here at CERT to start getting involved in this area. I mean, our work is nascent at this point but we're trying to get the word out a little bit through things like the podcast series about where our interests lie. And of course we're always looking for organizations that have ideas or might be interested in collaborating.

Julia Allen: Excellent, excellent. Well thank you for providing some of that background.So Dave, just one last question as we come to our close. Again, we've barely scratched the surface here and hopefully we'll be discussing this topic again in future podcasts. But do you have some favorite go-to places for folks who just want to get familiar with this general topic?

David White: Sure. I think some of the places that I frequent for information on this topic are -- so there are two organizations, one's called NetDiligence and the other is called Advisen. They both host annual conferences on cyber insurance and they have a lot of information on their websites about cyber insurance.

Advisen has a great daily newsfeed on cyber issues. NetDiligence just published their annual claims study, which I think -- it's a very small subset of cyber claims and the data they get is, they don't get full data on the claims. But it's still a very insightful study. It's worth reading if you're exploring this kind of coverage.

And then the other thing, I think, AIG won an award last year from Advisen for their website. So their website is actually really good for their CyberEdge product and they rolled out even some smartphone and iPad apps last year that also provide information on the nature of the risk as well. So that's actually a great resource.

Julia Allen: Great. And Jim, any favorite references that you might want to share with our listeners?

Jim Cebula: So yes, Dave touched on a couple of the big data providers. Another resource that I'd highlight -- So DHS, our colleagues over there, have been involved in hosting some meetings of industry participants around this idea of, as we discussed earlier in the podcast, can we bring together critical infrastructure and the insurance industry using the NIST Framework as a way to bring those organizations together, and look at that in a favorable light in terms of underwriting insurance?

So DHS has on their website a series of readout reports from these industry meetings that they had. There's some insightful information and you're getting basically the unedited thoughts and commentary of both industry from a critical infrastructure side and the insurers about where they think there are needs and gaps and what they think is working well.

Julia Allen: Excellent, excellent. Well gentlemen, I really want to thank you both for your time, for your preparation, for your expertise on this emerging area that we'll all be watching and working in. So first of all Jim, thank you so much for your time today.

Jim Cebula: Thank you.

Julia Allen: And Dave, great to reconnect with you, great to have you on the podcast series, and I appreciate your time as well.

David White: Oh you're very welcome. It's fantastic to be on the phone with you Julia.