A Taxonomy of Operational Risks for Cybersecurity
Transcript

Part 1: Increased Confidence in Identifying Cybersecurity Risks

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 our podcast website.

My name is Julia Allen. I'm a principal researcher at CERT working on operational resilience. I'm very pleased today to welcome back Jim Cebula. Jim is the Technical Manager of CERT's Cybersecurity Risk Management Team, of which I am a member.

And today, Jim and I will be discussing a taxonomy for managing operational cybersecurity risk. This is an update of a report that he and his colleague Lisa Young published back in 2010 reflecting things that we've learned since that time. And in addition to the two risk taxonomy reports, for our listeners' benefit, if you wish you can get some additional background on our work and related topics in operational risk and resilience in our podcast series.

So, welcome back to the series Jim, glad to have you today.

Jim Cebula: Well, thank you Julia. I'm pleased to be able to contribute to the podcast series. So, thank you.

Julia Allen: Oh, you're most welcome. And I think this taxonomy is really a foundational piece of work that hopefully our listeners will find quite interesting.

So, just in terms of setting the stage, Jim, for folks that may not be that familiar, could you say a little bit about -- just to set the scope of the taxonomy, what is operational risk and how is that specifically applied or defined for cybersecurity? And as you talk about that, why this whole arena is becoming increasingly critical in our body of work?

Jim Cebula: So, operational risks we define, particularly dealing with cybersecurity, we define really in four main areas as being actions of people, which can be either inadvertent or deliberate, systems and technology failures, which is probably what most people are familiar with or associate with cybersecurity, failed internal processes and external events. So, those four categories we think broadly cover the majority of what you would need to consider in terms of operational cybersecurity risks.

And so you're talking about things like risks to the information and technology assets that have specific consequences that affect confidentiality, availability, and integrity of information or information systems.

And I think the consequences piece there is really key when we're talking about risk. So I think people can envision events or activities in each of these four areas. But it's really tying it to a specific consequence and being able to discuss these things in a common language that's important.

So on our blog post that's up on the SEI website discussing the taxonomy, and we've provided some examples of a number of high profile cybersecurity events and breaches that occurred just over the last twelve months. People are familiar with a number of the major retailers. We've had Target; we've recently had Home Depot -- suffering breaches of the payment card information from the credit card terminals.

Attackers are successfully exploiting vulnerabilities and creating impact and consequences both for the companies and the customers of these companies, and other third parties such as the banks and card issuers that have losses or need to cover fraudulent charges and things in these cases.

We're on the second version of this taxonomy. Since the first version has come out, as we see with the continuing stream of events, things continue to happen. So we continue to need common ways to talk about these risks, ways to talk about the impact across the organization both vertically and horizontally so that everybody's on the same page as far as what we need to do to both try to protect against these sorts of things and detect and respond appropriately when something happens.

Julia Allen: Great, great. So you said a little bit about the benefits of a taxonomy. As I think about the wide range of breaches, you talk about retailer breaches, different attacks on the banking industry. We've certainly seen this in our critical infrastructure work related to things like the power grid, transportation systems, etc.

So operational risk can be a pretty complex and challenging topic. So would you say that having a taxonomy at least can serve as an anchor or a structure by which organizations can actually begin to get a much better handle on how to identify and prioritize their risks? Would you see that as one of the benefits?

Jim Cebula: Yes, I think that's right Julia. This is basically giving you a structured way to both -- for people that are on the ground doing hands-on work with your systems, or that are developing and carrying out processes, it gives you a map, if you will, to think about, "Have I considered things that might happen in each of these subcategories?"

Then it gives people higher up in the organization that same awareness of, "Oh, okay. Well, we're talking about cybersecurity risks but that problem is bigger than systems and technology. There are people aspects to it.

There are process aspects to it." And then external events -- we historically think about those in a physical sense -- protection of facilities. But there are cybersecurity aspects to that as well that -- the way it's broken down, they're in manageable chunks that you can take each one of the specific topics in the taxonomy and give it some thought and some consideration.

And then it's really, if you have this common structure, you can then have a conversation up and down the organization as to, "Okay, we've identified an issue with or a potential risk dealing with something specific. Now, we can have a better chance of talking about what consequences might occur if that risk was realized."

And that's where you get senior management or executive level attention is when you can start to put this in terms of these are the potential consequences in terms of dollars or losses to the business as a result of if this risk were realized. And then we can then start to have an intelligent conversation about what sort of investments we want to make in controls and protective measures, in measures to detect, and so forth.

Julia Allen: So as I listen to you talk, it occurs to me having this structure and having it be so well researched based on all the work that you and our colleagues have done -- not to put you on the spot, but would it be fair to say that if an organization is thorough and deliberate in its reference to or use of the taxonomy that they can be fairly confident that they will have covered the majority of the cybersecurity risks that they may run into?

In other words, they can -- I don't want to really say that they use it like a checklist -- but they use it like a reference to say, “Okay, if I take a look at what's going on in my organization operationally in the -- using the structure of that taxonomy, can I be confident that I've covered my bases?” -- do you think?

Jim Cebula: That's a good question, Julia. I think you could reasonably say that this would give you some increased confidence. We always want to be careful of saying security, resilience -- these kinds of things are not -- they're a journey not a destination I guess is the way I like to describe it.

So using a tool like the taxonomy, I think would help your process of evaluating a broad spectrum of operational risks across the organization, particularly focused on cybersecurity. And using this to drive those activities, I think, would give you increased confidence that we've given -- we've done our due diligence and given broad consideration.

I think in any given organization, digging into the things in the taxonomy might spin off other specific risks that are important to that organization that might not be directly documented in the taxonomy, but that -- it can be used as a very good baseline to increase your confidence. And gives you a jumping off point into maybe some things that are very specific to your organization that you either might not have thought of, or they might not have risen up to the appropriate level of visibility.

Part 2: Four Categories of Operational Risk

Julia Allen: Fair enough, fair enough. So let's spend a little bit of time talking about the taxonomy. You've mentioned the four general categories of operational risk that form the top level structure of it. So let's do a bit of a (if you'll allow me) a little bit of a deeper dive.

So actions of people -- can you give us some examples of some of the things that may occur in that category of operational risk?

Jim Cebula: Right, so in the taxonomy itself, we have three levels. We have classes, subclasses, and elements. So within actions of people, we break that down into inadvertent, deliberate, and inaction --things that, some action that should have been taken that just wasn't. So inadvertent action -- it could be a mistake, an error, an omission.

Deliberate actions -- this could be internal or external. This is where you would cover things like your insider threats -- things like fraud, theft; there's also sabotage; vandalism -- would be covered under deliberate actions of people. And then we also pick up inaction, which is an expansion on the omissions.

But it's the -- due to the lack of appropriate skills, knowledge, guidance, some action that needed to be taken wasn't taken. That can also address issues with availability of people, right? So are we properly resourced to evaluate and respond to all of the alerts that our security event management system is giving to us? Or are those logs not reviewed or not reviewed frequently enough because of lack of availability of people?

Julia Allen: Okay, that makes sense, that makes sense. So we always say that people are at the core of many of these categories of operational risk. So that's a real important category. What about the one that those who work in cybersecurity are likely most familiar with -- systems and technology failures. I'm sure we can all think of lots of examples there.

Jim Cebula: Yeah. We have hardware, software, and systems. And then hardware itself -- there's things like performance, maintenance, appropriate capacity. We have an element called obsolescence. So is the system still supported? That can cause issues in a number of areas. It can make a system more subject to failure if it's past end of when it's being supported. That can also create situations where you have a system that's running. It's considered obsolete by the vendor, so it's no longer being supported with updates. That can create additional opportunities for vulnerabilities.

Then we have software. There's things in there like configuration management, change control, the appropriate security settings, the testing and coding practices. And then the systems itself -- we're talking about things like the integration of multiple systems, what degree of complexity have you created. I think we've seen examples in some of these retailer credit card breaches where you have very complex networks.

And the attackers use an entry point by compromising the remote access credentials of a vendor that's completely unrelated to what's going on at the payment terminal level in the stores -- but were able, through the complexity of the system, to map a path from their entry point to someplace unrelated in the network. And do that without being detected in a timely manner. So this issue of complexity becomes important.

Julia Allen: Okay, great examples. So the next top level category is failed internal processes, which to me seems like it could cover a multitude of sins. So could you make that one a little more tangible for our listeners? What kinds of things are in failed internal processes?

Jim Cebula: So, this could be things like you have systems in place that are production systems that are carrying out certain business activities in support of your delivery of services and your mission.

And then you have things in place, technologies that are specific to security. So you've got logging and monitoring systems. And you have systems that deploy protective measures to your endpoints. You have systems that take care of dealing with your deployment of your patches and updates. You have a security architecture supported by some infrastructure.

All of that security apparatus, if you will, needs to have appropriate process for, “Okay, we're getting significant amounts of data each day in terms of alerts and notifications.” And there needs to be process in place for how to deal with that and processes for how to set these things up. What kind of tuning do we need to do to get to a point where we're filtering out the noise and the alerts that are potentially important are getting through?

When an alert does happen, right, an appropriate process for response. Who needs to look at that? At what point does it need to be escalated? At what point do we activate a higher level of our incident response team, our incident response process? So that’s sort of an operational level, these kinds of things around process are covered in the taxonomy.

We have an area in there talking about supporting processes, so things like appropriate funding, things like procurement.

So is the procurement process structured to be able to get the appropriate systems and software licenses and materials delivered in a timely manner? Do we have the appropriate funding to maintain the things that we have, keep them up to date? Do we have process for ongoing training and development of the people that are managing these systems?

Julia Allen: Right, so would it be fair to say that -- you certainly talked about the criticality of security processes and the technology that supports them. But clearly, any type of business service has underlying processes that rely heavily on technology and information and other types of assets.

So really a failed business process, things like you mentioned -- procurement, another area that occurs to me is perhaps compliance, or acquisition -- anything that has underpinnings where both the technology and the information needs to be secured -- you would expect operational risk to arise there as well, right?

Jim Cebula: Oh yeah, absolutely, that's a great point, Julia. And then even within the organization's delivery of services. One of the things that we advocate in an organization that's taking on implementing risk management or looking at their state of resilience is this idea of understanding the mapping between what are your key assets and what are the key services in the organization -- and which assets support, are critical to delivery of certain services.

So just that process of understanding what are your most important assets is important also from a process standpoint, both for prioritizing, making sure those assets are available and productive. But when something does fail in the business process, being able to map back to, “Okay, what's the underlying technology problem and how can we prioritize getting it fixed?”

Julia Allen: Got it, got it. Well, as we talk about some of these other factors that may affect the business operationally, clearly external events come to mind. So, every organization lives in a context. And there are lots of externally imposed, both requirements, and interdependencies.

So, you did mention the obvious physical ones related to for example, weather, like a fire, or a hurricane, or a tornado, or something of that type. But there's some really interesting things that show up in this part of the taxonomy. So could you say a little bit more about external events?

Jim Cebula: You mentioned the natural disaster kind of events. We're also talking here about legal issues such as regulatory compliance, litigation. So these are things that are done to your organization. A new regulation comes along. You become involved in litigation and suddenly have to have procedures for maintaining electronic documents, electronic communications, e-mails, instant messages, these sorts of things. These all have an impact on your IT infrastructure, your processes, so forth.

Business issues where we get into things like supply chain -- if you have a supplier failure, that's going to impact your ability to carry out a particular service. Understanding which of your suppliers are critical -- do you have backup sources for critical suppliers?

Dependencies on routine services -- utilities, transportation, emergency services, those sorts of things. We saw lots of examples and cascading examples of this back over a year ago now when hurricane Sandy struck the East coast on the United States. So obviously, it was a natural disaster. But then there were secondary effects from that. So the ability to deliver fuel was impacted. And so you had -- which created both transportation problems and ability to get fuel for running backup generators. So you had, for example, data centers going down because of lack of backup generator capability because of the inability to get additional fuel for the generator.

So widespread power outages, which led to -- realizing that we have, that we've become very reliant and dependent on mobile communications devices, cell phones, etc., which, even though the cellular communications network was still operating, people's devices were going down after a day or so because they had no power to recharge them.

Julia Allen: Right, right. It's an interesting category because this -- even though some of the other disciplines that we work in in addition to cybersecurity, such as business continuity and disaster recovery, those tend to show up mostly in this category of operational risk, correct, the external events?

Jim Cebula: External events, right. You also can get into some materials out there on the geo-political aspects of this, right? So understanding what's going on in the world's hot spots and how that might be affecting what cyber attack or malicious activity certain groups are carrying out or contemplating carrying out in furthering their support for a protest against certain geo-political activities that are going on in the world.

Julia Allen: Well, certainly with the emergence of activity in social media and other forms of instant communication, you know you can, as you said, these geo-political hotspots -- things happening in different parts of the world can definitely show up, particularly if it's part of your organization's supply chain, can definitely show up right at your doorstep very quickly, right?

Jim Cebula: Right.

Part 3: Application and Prioritization

Julia Allen: So as we come to our close, Jim, let's talk a little bit about application. So how might an organization -- you talked about some things at the top of our conversation -- but more specifically are you aware of or can you think of some applications of the taxonomy?

And one of the questions that immediately comes to mind as I listen to you speak is, is there anything in the taxonomy that can help you prioritize all of this? Or is that really outside the scope? But first of all, application and then maybe if you have any thoughts about prioritization.

Jim Cebula: Yes. So within the taxonomy itself, we provide some information on mapping the elements in the taxonomy to the controls that are in the NIST Special Publication 800-53. And in this current revision of the taxonomy, we've mapped this up to revision four of NIST 800-53.

So for those not familiar with the NIST SP, NIST has a series of special publications that are put out. I guess their direct audience is federal government agencies. But they are written in a way that other organizations can pick those up as well. And in this particular case, 800- 53 is the -- it's basically the control catalog. So it's one of the flagship documents in the NIST series that describe their risk management framework and risk management hierarchy.

So, for example, somebody wanting to, either wanting to use that control baselines put in there by NIST or that is required to do that, for example, by regulations such as FISMA, they can use this mapping to take a look at," Are we considering all of the potential operational risks that are described in the taxonomy in the context of the controls that we either already have in place or are contemplating putting in place for a new system under the NIST publication?”

Julia Allen: Okay. So you could actually take the taxonomy, given the mapping that exists, and say, “I know I have these controls in place, or I have these maybe ten additional controls. And I'm trying to figure out which ones I need to consider.” You can do that consideration against the types of operational risks that the taxonomy would help you identify, right?

Jim Cebula: Right. Or alternatively, somebody in the organization comes up with, “We think we're concerned about these types of risks.” You could back into this through the, “Okay, how do those fit into the taxonomy?” And then what kinds of controls in the NIST catalog might be useful to you in addressing those risks.

We provide a tie-in in the back of the taxonomy to the OCTAVE method (Operationally Critical Threat, Assets, and Vulnerability Evaluation), which is an SEI- developed risk assessment process that some organizations are using as a means to periodically assess where they are with risks and how those might impact their critical assets.

So somebody that's currently using OCTAVE or is considering using OCTAVE could pick up the taxonomy and it would be a complementary document to the use of the OCTAVE method.

Julia Allen: Great. And do you have any thoughts about prioritization? I know in the NIST arena they have documents that guide users of their, guidance on how to prioritize systems and therefore which controls to select based on the priority of the system or the priority of the information that the systems house.

But just in general, do you think that there's any way in which the taxonomy can be used to help prioritize operational risk?

Jim Cebula: I think this would work in combination with other processes that you might be using to prioritize what are your key assets. Really you're, what an organization really needs to be doing is looking at what are the key services that support the organization's mission and then breaking that down into what are the key assets in terms of people, information, technology, and facilities that support delivery of those services.

That gives you the prioritization based on what service delivery is important to the organization. And then you can then bring things like the taxonomy into play to look at risks specific to those critical assets. By itself, it doesn't lend you to a prioritization but it works hand in hand with other processes that organizations can use to prioritize what's important to them.

Julia Allen: Right, and as you said, going from a critical service to critical assets, using the taxonomy to help you identify operational risk, and then dealing with, as you said earlier, the consequences.

So if this risk were realized against this particular key asset, how much pain could I stand? And if the pain point of that particular operational risk is above a threshold that you would find tolerable, then you clearly need to make some investment, right?

Jim Cebula: Right.

Julia Allen: So, this has been great, Jim. I really enjoyed talking about, talking this through and sharing some ideas and perspectives. Do you have a couple of places where our listeners can learn more if they're interested?

Jim Cebula: We have, the current version of the taxonomy itself is published as an SEI technical note, which is available in the SEI digital file library on our website. And there's also, within the SEI website, there's a series of blog posts up there.

So there is a blog post covering the taxonomy and a summary of what's in there. We've done podcasts in the past on the topics of operational risk, operational resilience. Those are available as well. And also, we talked briefly about the OCTAVE method. There are links to that material as well on both the CERT and the SEI websites.

Julia Allen: Great, well I thank you so much for your time and preparation today, for this great body of work that hopefully will get lots of use and uptake. And thank you again for your time today.

Jim Cebula: All right, thanks, Julia. It's been a pleasure.