Cybersecurity for Association Leaders with Thomas Parenty, as originally aired on June 11, 2020

Chelsea Brasted: Hey, everyone. My name is Chelsea Brasted and I'm the content manager for Sidecar. And today we're launching search connect with a keynote conversation with Thomas Parenty, an international cybersecurity expert who has worked with the National Security Agency and other organizations around the world. I ended up connecting with Thomas after he and his business partner, Jack Domet, wrote a book for the Harvard Business Review.

Their book, "A Leader's Guide to Cybersecurity: Why Boards Need to Lead--and How to Do It," borrows from the principles they've learned as the co-founders of the cybersecurity firm, the Archefact Group. They argue not only is it not enough to relegate cybersecurity to an IT department and just be done with it, it's actually dangerous. So today, Thomas and I are going to talk about why and what you as an association leader can actually do about it.

Thomas, the first question that I wanted to ask you is, your book came out in December. So to just sort of remind us a little bit about why cybersecurity matters so much, can you think of any major hacks or major leaks that have happened in just the past six months that can remind us why this is such an important topic to talk about?

Thomas Parenty: Well, actually I don't have to go that far back. I can just go back to Thursday of last week. And Thursday of last week, there was a report by the FBI that there is now evidence of a large number of cyber attacks sponsored by nation states or countries as they used to be called, on research institutes and drug companies that are trying to address the COVID-19 crisis.

And the reason for this is quite easy to understand. And that is that in terms of the resources necessary to fight this pandemic, it is not just personal protective equipment, but it is the underlying science for developing testing, for developing cures, for developing vaccinations. And so, because of that urgent need, then one of the results is a new wave of cyber attacks. So that was Thursday.

Just today, there were reports that a children's game out of Canada, the account information for 22 million people, namely children, had just been disclosed and is now being sold in the dark web. So those are just two examples of cyber attacks that were motivated by either profit directly in terms of, or benefit directly in terms

of being able to get a, if not a monopoly, at least a headstart on dealing with the virus.

And another relating to the fact that the identities of various online users have value in underground markets. And it's unfortunate in this particular case that it was the information about children that was compromised. Now with that, I would say most of the cyber attacks that we hear about represent a very, very small percentage of what is actually happening. And the reason that we know about them is the parties involved were not able to keep it secret.

Chelsea Brasted: So basically this is a tip of the iceberg situation.

Thomas Parenty: That's right. And one example, years ago, we were doing work for an automobile manufacturer and there was one cyber incident that resulted in a loss of $1 billion US, and that never made it into the press.

Chelsea Brasted: Oh, wow!

Thomas Parenty: And that was one incident involving one attacker that cost a company $1 billion.

Chelsea Brasted: So, you know, in the two examples you mentioned first, we're thinking about how to sort of solve this crisis that feels like someone can maybe see the value of that information fairly easily. But in the instance of kids, or even in the instance of the nonprofits that we typically work with, they may think like, oh, what information do we have? What secrets do we have that anyone on the dark web would actually want?

What reaction would you have to that sort of attitude where someone may think what does it matter that somebody now has a bunch of usernames for children? Or what does it matter that someone has the names of the doctors in my association?

Thomas Parenty: And so, what I would say not having looked at a particular situation or organization specifically, I would say, I don't know, but it is a question that is worth asking. And it's important to realize that hackers or cyber advisers or whatever you want to call them are not like Santa Claus. They're not looking at a list of who's been naughty or nice. And since your nonprofits are probably nice, "Oh, I won't bother attacking them," cyber adversaries attack if they think there is something of value to themselves.

And for those who are in charge of nonprofits, they should think about what assets or aspects of their organization could be of value to somebody else. I'll give a very simple example, is that for some nonprofits, they will track basically high value donors, people who reliably give lots of money to make sure that they cultivate them so they don't stop that.

Now, if somebody was working for not the same type of nonprofit, but generally looking at the same kind of donor profile, it would be of great value to them in order to be able to know the first nonprofits donor list and the various information that they have about their high value donors as a means of being able to essentially poach them and try to move the money that they were giving to the first charity now to the second charity.

And this particular phenomenon is one that has been true in luxury hotels for ages. And so, without naming brands, the information about high value guests at one luxury brand is of immense value to that another, because if you can get them to sort of check across the street, there's a significant amount of revenue at hand.

And so, what is a useful thing for those in charge of nonprofits to think about is, okay, they know their organization, and to first think about what are the risks to the organization? And a risk could be a donor information compromised. Several years ago, I did work for Asian Community Mental Health Services in the San Francisco, Bay Area. And one of the things that was very important to them was their clients. And they used the word client as opposed to patient.

Their personal information was protected because, well, one, it is medical information. And, two, those particular patients were significantly at risk. So it depends on the kind of business that the nonprofit is involved in, in order to figure out what are the risks to it. And once one is identified risks such as the theft of donor information, then think about whether or not that risk could materialize as a result of some attack on the computer systems.

And you don't need to be sophisticated about that, you can just think from the perspective, "Ah, if something went wrong with the underlying computer systems upon which maintaining donor lists or maintaining client lists was involved, ah, could there be a problem there?" And so, to give you an example where a cyber risk wouldn't be a problem is, imagine you're a nonprofit in which your assets are in multiple currencies. So you're an international organization. One of the risks to your organization could be currency fluctuations. Ah, I've got a whole bunch of money in Euros and now that's not worth much or whatever.

Now, that is an example of a risk that there's no cyber security implication. And so, the interesting thing about the two tasks that I just discussed, what are the risks to the organization? And could those materialize as a result of some sort of cyber attack? At the level we've been talking, there's no technical details you need to be aware of. It's more, "Oh, our donor list is on a computer. Currency fluctuations happen as a result of economic and trade circumstances. Ah, one could be a problem, one clearly isn't."

Chelsea Brasted: So you mentioned, just to sort of like backtrack a little bit, you mentioned this idea that some of the data that a cyber adversary may get a hold of could be sold on the dark web. Just to sort of jump into that slightly, what actually is the dark web and why would somebody... Because we're talking about how these

cyber adversaries are not Santa Claus, they're not thinking about like... who's good, who's a bad actor. So what sort of value might that information actually have in the dark web, and what is that? And I'm just asking so that we sort of have an idea of what it is we're working against as we continue the rest of this conversation.

Thomas Parenty: Okay. So in terms of the dark web, and the best example would be something called the tor, T-O-R, web. It is different from the regular internet in two regards. One of which is, if you configure things properly, where you visit in the dark web cannot be traced back to you. And so, there is a certain amount of anonymity that makes illegal transactions easier. The irony is, this dark web was actually developed by the United States Navy to facilitate hidden communications in a military or intelligence environment. So it is secrecy that is considered a value, it depends what you want to do with it.

But from a practical perspective, whether it's the dark web or the internet or meeting somebody on a corner, that is just a mechanism for selling something. And so, the more important thing is what would a nonprofit have that would be worth selling? Now, if a nonprofit actually handled their own credit card transactions for donations, ah, now you're talking about something that's very valuable. Because the information that goes into a credit card, whether it be the credit card number, the expiration, security code, those can be sold to various criminal organizations and ultimately turned into let's say, Walmart prepaid cards that somebody could go in, buy a television set, which then ends up getting sold. So medical records are actually now worth much more than credit card records on the dark web or in any criminal environment.

And so then the question is, whether or not a nonprofit has something that would be of value to somebody else? And one example I could give is, I actually am on the board of directors for a modern dance company. And so, one of the interesting things about the dance world right now is, shockingly, there's not a lot of money in it. And in order for many dance companies to survive, they need to write grants.

Now, if there's a particular dance company that is really good at writing grants and has a very good success rate, that might be of interest to another either dance company or some other organization in the arts, that thinks, "I want to up my game and I want to write better grant proposals. And so I'd like theirs." And it's something that if one looks in the commercial world, and this is an analogy that would also hold over in the nonprofit world, is the more specific information that you have about the business you're in, the more likely the attacker will be in the same business.

So if I am a chemical company, another chemical company would really like to know the formula for my high value products. Like R&D is very expensive, I'll just let you do the R&D and I'll steal the results. If the information that a nonprofit or a company has is more generic, such as credit card information, then the pool of potential adversaries is much larger because you don't need to be a specialist in food banks in order to steal the credit card information that is used to donate to the food bank.

Chelsea Brasted: Got you. So since we're sort of talking about money, it's my very index for transition to the next question, which is, to be addressed correctly, does cybersecurity necessarily need to be expensive? Is this a, just throw money at the problem sort of situation?

Thomas Parenty: So, in my experience, there is a huge amount of money that is wasted on cybersecurity. And so, our advice is not to spend more, it's to spend more wisely. And it's something that with companies, specifically in financial services, because the stakes are quite obvious and quite high, there is a great deal of money spent on cybersecurity, equipment, tools, services. And frequently, while a great deal of money is spent, there isn't a comparable benefit received because those resources are not properly focused on what's most important.

And so, that's one of the reasons why in our book and other publications, emphasize the importance of starting with, what are risks to the organization? As opposed to, what are vulnerabilities in the underlying computer systems? Because having a focus, which is very, very common today, of spending money to fix vulnerabilities and computers, you end up in a situation that is seductively dangerous.

It's seductive because there is actual value in fixing problems with computers. The reason it's dangerous is you could spend all of your budget, all of your time, all of your resources, and have, one, never actually fixed all the problems in the computers. And then two, you've never actually gotten around to the primary point, which is protecting the critical business activities for which the computers were purchased or rented in the first place.

Chelsea Brasted: So in the first few pages of your book, A Leader's Guide to Cybersecurity, you make it very, very plain that you see a problem with how cybersecurity has traditionally been framed. And I think we're sort of getting there. You sort of make this argument that focusing on technology is the wrong method and that's simply relegating it to the concerns of this IT department or whomever, or sending your staff a couple of emails about what phishing is. Why is it, in your words, why is it so important for the leaders of organizational operations and strategy to take this on and not farm it out to the IT department?

Thomas Parenty: Okay. So, one, it comes to the issue of prioritization of what is most important. So that's one point that I was alluding to before. The second is simply an observation that people tend to focus on the things with which they are most comfortable. And people within IT departments are, and I would say broadly within cybersecurity departments, are most comfortable dealing with technology and how certain vulnerabilities in computer systems could be exploited in order to cause harm.

And that is actually the background I come from. Back in the 1980s, when I was working at the National Security Agency, my primary focus was evaluating the

computer security protections for the US nuclear missile arsenal. And so, I was involved in very, very technical details. But the goal was to prevent the Soviets from taking over control of US weapons. So we were very, very clear on what the objective was.

Now, if you look at boards of directors and senior executives, they are much more comfortable with, because of their responsibilities and job, what are the risks to the company? And unless you have your cybersecurity technical activities clearly focused on reducing the most significant risks to the company, you will end up spending countless amounts of treasure and not substantively improve your level of protection at all.

Chelsea Brasted: When we're thinking about sort of identifying those critical activities, who should actually be part of that conversation?

Thomas Parenty: Okay. What I would say is, it is absolutely necessary that one has a representative sample from the organization. And so, there is an expression, sort of, too many cooks spoil the brew, or you've got too many cooks in the kitchen. And perhaps if you're at home, that's true. But if you think about a professional restaurant, there is somebody who just does pastry, somebody who does salads. There's somebody who mans the grill or the fryer. You've got a sous-chef who's coordinating everything. And you've got the chef de cuisine whose name is on the door, who maybe every now and then will actually show up. And it is because you have these people in well-defined roles, cooperating together, that hundreds of people can be served dinner that night.

Now, in a cybersecurity domain, you want to be able to create a link between the primary risks to an organization, and this is true whether it's profit, nonprofit, government, no difference whatsoever, all the way through to the people who are concerned about these very sophisticated technical issues about what things should we fix.

And so, what you want is to start with people who are very, very familiar with the risks to the organization. And those tend to be people at the top, and at least for many commercial organizations, there will be some enterprise risk management functions that actually have a list of the top 20, 10 to 20 risks for the organization. And that is the sort of the logical and effective starting point of what matters to the organization.

And it is something that ... For example, I do work with a local food bank. And their logistics is incredibly important because they try to emphasize fresh produce as opposed to just canned food. And if there is anything that happens to their supply chain, basically lettuce dies and people are not fed. So that is an example, real risk.

And so, if you start with a real risk to an organization, so for example, logistics don't work, then you sort of think about, "Okay, since we are dealing with cyber, what are the underlying system supporting this movement of food, both from suppliers to the warehouse, as well as distributing it to local charities or religious organizations?

We're actually the ones who hand over the food." Ah, so now you have certain systems, people who are involved, "Okay, these are the resources we need to protect in order to make sure that people get food."

And you can have people who are sort of neither the technical ones nor the leadership, but who are involved in the day-to-day activities of, "Okay, we're going to get this amount of lettuce from this place, some pears and oranges from over here." That since they're involved in the day-to-day activities, they know, "Oh, if that goes wrong, we're up the creek."

And so, it really is important in order to get the necessary information to protect your organization from cyber attacks that you have this variety of people who are involved. And then there's a second benefit and that is, if you have people from the board to senior executives to mid-level managers of the people who are actually doing the day-to-day work, to various systems or cybersecurity personnel, all working together on identifying, defining what are these most significant cyber risks, you have now accomplished an incredibly important cultural objective. Which is you're now starting to build consensus across the organization about what's important and what we should be doing.

Chelsea Brasted: And basically, what that is, is its very core, is you're having a conversation about these very specific items and parts of your like processes within your organization that you need to be protecting essentially.

Thomas Parenty: Yeah.

Chelsea Brasted: How often are you sort of helping the leaders that you work with find out that some of their worst enemies are maybe the employees and the systems they already have in place. Because they're just hitting ‘save password’. They're saying, "I'm not going to worry about this. It's too much of a pain in the butt."

Thomas Parenty: Okay. There are a number of questions in there. I'll answer one of them, which is, how often is this a problem? All the time. Absolutely, all the time. And this is, again, one of the reasons why going back to what you had noticed in the first few pages of the book, why it's so important to look beyond these technical problems and technical solutions. And that is, it is very, very easy for somebody incredibly well-intentioned and well-motivated on the cybersecurity side to come up with a control or protection that in principle looks really good. But once you get into the field, no one's going to use it.

I'll give you an example. So in the 1980s, I, in order to get access to the computer at NSA, where I was working, clearly needed a username and password. And the password was generated by the computer. And it was supposed to be both pronounceable and memorable. It was neither. And so, the first time I ever wrote down my password was when working at an agency whose middle name was security. It is incredibly common for well-intentioned cybersecurity professionals to

create controls without adequately taking into account the difficulty of either managing those controls or working in an environment in which those controls are present.

Chelsea Brasted: Yeah. The password thing is a, I think, one of the most irritating ones where you have to change it every like six and a half days or something.

Thomas Parenty: Right. So it's interesting that you should mention that, because the standard reason for changing your password periodically is if a hacker had already compromised the password, then once you change they no longer have access. That's good in principle, but, again, coming back to the difficulty of people being able to remember passwords.

And so, we did a project in Asia ages ago, where there was a financial services company who wanted us to look at password policies and things like that in their company to see if they were effective. And they had a policy, every month you had to change your password. And so, what we noticed is let's say for example, there was an employee who liked cats. And so, their password for January would be cat01, then for February cat02, and continuing like that. Because there was no way on earth they could remember completely different passwords.

And so, what that forcing the changing of passwords, one, meant that people were using passwords that were ever so much easier to guess. That's completely destroying the whole purpose. Because, ah, if somebody's password is like that and a hacker comes in in October, oh, they already know what the password is. If they had compromised in January and they come back in October, oh, that's pretty easy.

And so, one thing that I've used for ages is something called a password manager. The particular one I use is called 1, the letter 1 Password. But there are a whole bunch of them. Individuals should not try to remember scores of passwords that are clearly beyond the capacity of most anyone to actually remember.

Chelsea Brasted: Yeah. So I want to shift gears a little bit and talk about how when you guys start working with a new organization in your firm, how do you start that conversation about shifting the mindset? That cybersecurity should be a conversation for the leaders in an organization. How do you sort of start that shift in rethinking maybe their entire approach to cybersecurity?

Thomas Parenty: Okay. So first in terms of a little bit of context is, a few years, where a few could be five, 10, 20, or in my case 35, the initial discussion would be whether a board member or chief executive even needs to bother with it. That is no longer the situation. Basically, anyone who is on a board or is on a senior executive team, knows that cybersecurity is something that their organization has to deal with. And they also recognize that they're responsible. That, yes, the buck stops with them. Whether they want it or not, that's simply the way it is. So that is a wonderful improvement.

The biggest sort of issue or challenge right now is there is a very common perception that cybersecurity is such a technical subject, only the experts are capable of doing it. And therefore, it is perfectly fine for boards and executives to delegate that responsibility to their IT or cybersecurity teams.

Now, I would say that that's not so much a delegating as an abrogation of responsibility. But it comes from an honest place, which is, they genuinely believe this is too complex in order for them to deal with. So the starting point is to help them realize that for what they need to do, it's not too complicated at all. And so, that fundamental reason why they sort of push the responsibility off to somebody else is not true.

And by way of analogy, think about a car. The skills and talents that are required to build a car, are very, very different from those required to drive a car, which are in turn very different from those required by somebody in the back seat to say, "Driver, take me here." And the role as one could imagine of a board of directors is, "I want you to drive me here." Which in a cybersecurity context is, "I want you to focus on the cyber threats that most could impact business risks to my organization." And so, what I want is the driver who could be the chief information security officer, or if one doesn't have a cybersecurity department, somebody within the IT department. I want you to drive or focus your cybersecurity activities on those that relate most to the most substantive risks that my organization faces. And they will use the car, which could be cybersecurity products or services provided by vendors, in order to accomplish this.

And so, going back to a point you had said just to introduce this topic of perhaps they have to sort of redo everything. No, actually what you want to do is simply provide a clear focus and direction for what you're doing already. Now, there may be certain things that you will discover once you have this direction of reducing material risks to the organization. You may realize that, "Ah, some of the cybersecurity work that we were doing actually doesn't contribute to reducing this risk. So let's move the money from that and focus on something that does reduce the risks."

Chelsea Brasted: Which gets to what you were saying earlier about how you can... You don't necessarily need to spend more, you just need to spend smarter.

Thomas Parenty: That's exactly right. And there have been some people, executives in the financial services industry who say, essentially, cybersecurity has a blank check. And from having done budgeting in the government environment where we rounded off to the nearest hundred thousand, unlimited money is a guarantee for wasted effort and wasted money.

And so, while it is absolutely clear that there are a number of organizations who have underinvested in cybersecurity in the past and need to make up for that, one should not measure a good job by how many dollars you've spent. You should measure a good job by the focus you exercise in spending that money.

Chelsea Brasted: So we've talked a little bit about, and you've used the sort of board... Using boards as leaders a few times.

Thomas Parenty: Yeah.

Chelsea Brasted: I want to ask, in an organization where you have people cycling on and off boards, a relative clip, does that itself present any more risk in having these conversations or does that make those conversations more difficult in your experience?

Thomas Parenty: So what you've just highlighted is the importance of governance and the establishment of solid governance for cybersecurity within an organization, so that one is not so much dependent upon the qualities, interests, questioning ability, of an individual board member, but rather there is this structure into which board members as they cycle through, participate.

Chelsea Brasted: Got you. So in an organization that's maybe not approaching cybersecurity in this way currently, do you have any suggestions for how an association leader could go to the board and say, "Hey, I need you to start thinking about cybersecurity in this way." Do you have any suggestions on how to prompt that conversation?

Thomas Parenty: Okay. So the one necessary prerequisite for that conversation is people who have oversight or management responsibilities for a nonprofit organization, they need to first sort of understand that risks to the organization need to be addressed. So forget about cybersecurity. An organization needs to, as part of its governance leadership oversight, realize risks need to be both understood and managed.

And so, for example, my co-author is on the board for one of the local schools where I think one of his children goes. And one of the risks this school organization faces is, financial fraud. And not just by somebody on the outside, perhaps somebody on the inside, deciding that they were going to abuse their check writing ability and abscond with the school funds.

And so, you first need to have an organization understand that they have risks, and it doesn't matter what kind of organization, all of them have risks. And so, the starting point is, "Okay, let's think about risks." And now when thinking about these risks that already exist, we don't need to create any new ones, we can now think, "Could any of these risks materialize as a result of some cyber attack?" Where you don't need to know about different types of cyber attacks, you could just say, "Could any of these risks materialize as a result of some malicious modification or whatever of the underlying computer systems?"

Chelsea Brasted: For some folks, they're not going to sort of come from that cybersecurity background. So is there like a general language that you sort of need to establish as you're starting to have these conversations?

Thomas Parenty: Yes. Excellent point. And one of the common problems that both boards and cybersecurity people feel when they meet, is they're speaking different languages. And if you're speaking different languages, then there's no means of communication and no means of being able to cooperate to accomplish something. And so, instead of saying, "Oh, the board members need to, like, become much more adept at the terminology of cybersecurity," I would go the opposite way and say, "All cybersecurity discussions need to be in the context of well understood and are to be known risks to the organization."

And it's something that a board member doesn't need to know what a buffer overflow attack is nor do you, nor does anyone in your audience.

Chelsea Brasted: Because I don't.

Thomas Parenty: Right. And there is one sort of cool element of a buffer overflow attack which is called riding the NOP-sled. Which, again, you don't need to know what it means, but it's really fun. Like I'm riding a NOP-sled. That's cool. What board members do need to understand is that a particular risk that they already know about and understand in business terms could manifest as a result of some sort of cyber attack.

And so, what this leads, and, again, this goes to having the right terms, the right sort of concepts to communicate, do not think of cyber risks as risks, think of cyber risks as another means through which a business risk could materialize.

I'll give you an example. I lived in Hong Kong for a decade. And I now split my time between California and Hong Kong. And in summer typhoon season, there is a risk of high winds and rain knocking over electric power poles causing disruption to the delivery of electricity to various people in rural areas. So a typhoon is one means of which electricity distribution would be disrupted.

Another means would be a cyber attack on various distribution substations. And so, in this particular context, it's not like there's a cyber risk. Like what's the cyber risk? I don't know any. I don't understand what that is. However, I do understand the delivery of electricity being interrupted. And so, what you would like in these discussions between cybersecurity people and executive reward leadership is to think about and to discuss, how a cyber causality, as opposed to when, for example, could cause a business risk to materialize.

And again, for a board member, he doesn't need to understand how a cyber attack step by step would take out a distribution substation. He just needs to have confidence that that is actually a realistic way in which the lights would go out. And this then goes back to what we were talking about in terms of the number of chefs

in the kitchen and the number of people who are involved in developing what we call cyber frame narratives that basically pull everything together from a business risk materializing who might attack you, what computer systems would need to be compromised, how to protect against that, and having that discussion.

Again, it's something that helps build a common language in which company can come together and say, "Yes, we're going to address this risk and we're going to do so effectively."

Chelsea Brasted: So in order to effectively address these risks, you and your co-author created the digital stewardship framework. And so, I would love it if you could sort of walk us through the four principles and then the three responsibilities that sort of makeup that framework.

Thomas Parenty: Okay. I'll start with the responsibilities. Those responsibilities revolve around understanding and managing cyber risks. Fortifying the company in order to be able to do this on an ongoing basis, as well as to promote organizational structure and culture that results in more positive cybersecurity behavior on the part of employees. And the third is dealing with a cyber crisis, should one occur.

Now, there are other things that are involved in cybersecurity, but we're very well aware, one, regardless of the resources, you can't do everything at once, nor is everything equally important. And so, dealing with the organization and cyber crises, those are the three pillars upon which everything else depends. And they're the most important to deal with. Because if you haven't handled those, it doesn't matter what else you're doing.

And so, they are responsibilities that a company has to do, that boards have the responsibility to oversee. And that provides a sort of very concrete direction on what companies need to do. And by extension, what senior executives need to direct through their management role and what boards need to oversee fulfilling their governance responsibilities.

Now, regardless of how good security advice is that the company's received, even from such a wonderful book as A Leader's Guide to Cybersecurity, there are always going to be circumstances that have not been laid out ahead of you. And so, you need to have some guidance or I would rather say, a litmus test, that you can use to decide, "Okay, is this the way we should go?"

And so, there are four principles that both boards can use to evaluate the quality of what their companies are doing, and then also can use as a means of gauging their own performance. And so, the first one essentially says that, if somebody gives you a description of something related to cybersecurity and you don't understand it, they haven't done their job.

And this goes back to what we were just talking about in terms of a common language. And the origin of this particular principle was actually the first class I took in philosophy as an undergraduate. And the professor said, "If you cannot explain a

tenant of philosophy to a nonspecialist in a way that they understand it, you don't know it yourself."

And so, again, there are many, many technical cybersecurity details comparable to the construction of a carburetor that executives and board members don't need to know, but you should be able to communicate the essential components. And if you can't, then go back and do it. So that's the first one.

Another one relates to taking cybersecurity from essentially living in a silo and incorporating it into the main core of a business. And so, for example, one of the things that we recommend is that the head of cybersecurity not report to the CIO or the head of technology. Because, one, that makes everyone else think, "Oh, yeah, IT has it. I don't need to worry about it. It's a computer problem." Which as we've discussed, is exactly the way not to solve the problem.

And so, in point of fact, we recommend that the head of cybersecurity report to somebody on the chief executive staff. Because it is then more integrated into the actual running of an operation of the business. We don't recommend that they report to the CEO, because that just is moving it to another ghetto. It's just one higher up the hill, another silo. Because people say, "Oh, they report to the CEO. Oh, we don't have to deal with that."

Another one, leads to the primary focus that it's the business at risk, not the computers. And this again goes back to, if one's primary focus is on fixing problems in computers, and this is the most natural approach that people in cybersecurity would use today because all of the products, services, standards, advice that is out there in the world of focuses on that, you'll spend lots of time and not accomplish stuff. And so, you need to make sure that the focus of all cybersecurity activity is, again, on reducing material risks to the business.

And then the final principle actually relates to something that we had discussed before in terms of people bypassing various controls. And that is, one needs to recognize the motivations of those within your organization when thinking about what kinds of protections to put in place. And so, for example, one of the reasons why we say you don't want to have the head of cybersecurity report to the CIO is because their motivations and their incentives are quite different.

This is a simplification, but most heads of IT departments are rewarded based on how many new applications with more and more convenience and less and less cost can be deployed. That is very different from the motivations of somebody whose primary interest is cybersecurity, who wants to make sure as you're rolling out all of those things that they're actually safe.

And this actually goes back to one of the problems with the Zoom teleconferencing system is that, okay, they played a little fast and loose with some of their security claims, but it was basically that they wanted to make things really, really convenient, but in a way that ended up compromising security. And so, you don't want to have the person who's trying to make it secure, report to the person who's trying to make it convenient.

And so, it's very important that, again, one looks beyond the particular features of the technology or the wonderful things that it could accomplish in principle to then think about, okay, how has this actually been working in real life?

Chelsea Brasted: I'm glad you mentioned Zoom. Because I think it's kind of impossible to ignore the Coronavirus pandemic and the mass implication that's had on all of us. I'm working from home right now and we're talking over Zoom. So is there anything in particular that has sort of come up specifically in the last couple of weeks or a couple of months, that you think leaders should be thinking about? Especially, as we are all working from home, is there anything sort of pandemic related that maybe you would want a leader to be thinking of specifically right now?

Thomas Parenty: Because of the pandemic, people are conducting business in a very, very different way than many of us were just a couple of months ago. And because the way in which we do business and the way in which we use technology is different, that introduces new risk.

And so, actually this comes back to another point is one way that organizations think about new cyber risks is, "Oh, there's a new hack or something like that." Or, "Researchers have discovered a new vulnerability in yet another Microsoft product." And there are just too many of them to provide any means of prioritization.

And so, what we have discovered, and this actually falls under the responsibility of sort of fortifying or structuring the company is, the most significant way in which companies or organizations encounter new cyber risks is when there is some change in business operations. And that change in business operations results in a change in the use of technology that may have not been considered from a security perspective in this new case.

Now, lots of teleconferencing from home using Zoom is one of them. Now, I would argue in terms of, like, the hierarchy of things to worry about, for most people, Zoom is not a big deal. And if you just follow a few little pieces of guidelines like actually using conference IDs in order to get access and not like posting them on Facebook that anyone would be able to see, that goes a long way.

And, again, one thing interesting from a business perspective is, does it matter? So for example, I was talking to somebody, a former student of mine, last week, and he is now providing Tai chi lessons via Zoom. And one of his friends said, "Oh, no, that's terrible. That's not secure. That's a really, really, really bad idea." And so, I asked him, "Okay, so the worst thing that could happen if somebody hacked into Zoom is they now have your intellectual property, which is the content of these Tai Chi lessons." To which he said, "Oh, that's not a problem. I've actually already posted that on the internet. That's something that people can get anytime they want. The value is the corrections I could do when I see them doing the form incorrectly."

Okay. So there's really no business risk. Because of the risk of stolen intellectual property, it's already out there. And so, not a big deal. Now by contrast, last week I was talking to somebody who is in cybersecurity for South Africa's National Electric Power Company. And she had mentioned that the board members and executives are now so much more concerned about cybersecurity than before the pandemic hit.

Because not because of people at home doing conference calls like we're doing right now, but rather people who used to perform critical operations within an electric power plant physically inside the building are now starting to do things from home using an entirely different technological underpinning that was never intended for this job. And so, that's a wonderful example of, ah, we are now changing the way in which we do business in reaction to this pandemic. And that introduces our business operations to new risks that we have not previously identified or analyzed.

Chelsea Brasted: Great. I think that's a really helpful example to sort of see like the different applications of that. So, Thomas, as we're wrapping up, I would love to ask if we've, like sufficiently freaked anybody out, like what could they go and do today? What conversation could they have today with the leadership of their organization to really get the ball rolling on rethinking the way they address cybersecurity in their association.

Thomas Parenty: I will answer this in a couple of different ways. So, if you have somebody who is within an organization, they could either be on the business side or they could be on the IT or cybersecurity side, is as the opening for a conversation with somebody on the executive team or somebody on the board of directors, depending on whom one actually has the opportunity to talk with is say, "I really think we should start looking at the risks we already have identified, but now from the perspective of a cyber attack as the causality."

That given all that's going on right now, this seems like a good time to sort of just look at the risk we already have, but from this different perspective. And going back to the example that I'd given about typhoons and interruption of electric power, typhoons are very geographically specific, whereas if you mounted a cyber attack, one would be able to impact a much larger scale of power stations resulting in a much larger impact to a population without electricity.

And so, that's something that, yeah, let's just look at the things you already have, but now let's look at it from the perspective of cyber conversation. And so, that's something that would be the approach that we would take if you were within an organization, so then speaking up to those with management or oversight responsibilities.

Now another option is, let's say you are within an organization, but you do not have access to leadership. What would you be able to do sort of where you live in that organization? And so, the advice I would give there, goes back to the point you

initially raised about a common language that is necessary for collaborative activity and that is to build bridges between the business side of an organization and the IT or cybersecurity side.

And so, whether you are a government, a for-profit, or nonprofit, there's a group of people responsible for fulfilling the mission of the organization. And there is another group that is responsible for providing the underlying technical support for accomplishing that mission. And so, if you... The way in which I would propose starting a discussion between these two is, in the form of questions.

And that is, if you are from the business side, you have an understanding of the risks to a particular business activity. And so, the question you could have for the IT or cybersecurity people is, what are the cybersecurity protections that are in place to protect my business activity from being compromised? And sort of the flip side for the IT people or cybersecurity people is to think, for the cybersecurity controls that I've deployed, what are the business activities that it protects?

And if you can't answer the first question, then you're pretty much guaranteed that your business activity is not being protected. And if you can't answer the second question, then it's highly likely that the investments you're making in cybersecurity are not actually protecting the critical business functions it's supposed to.

And so, that's a very nice way of sort of starting to have a discussion. And that was actually a concept I introduced in my first book for Harvard Business Review Press that came out in 2003.

Chelsea Brasted: Perfect. Well, we'll get details about both books up when we air this for SURGE. So thank you so much for taking the time to chat with us. Thank you.

Thomas Parenty: Great. Okay. Really nice to chat with you, Chelsea.

Chelsea Brasted: Thanks.