#149 - Board Perspectives

[00:00:00]

[00:00:00] **G Mark Hardy:** Well, hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host today, and we're going to talk about board perspectives, specifically about the Board of Directors views on cybersecurity.

Some of the things we want to kind of investigate are What is their responsibilities? How are you going to interact with the board? What are the big questions that they might want answered? Maybe is there anything different that's going to be from last year? But first, a quick message from our sponsor.

Risk3Sixty is a cybersecurity technology and consulting firm. They work with high growth technology firms to help leaders build. manage and certify security, privacy, and compliance programs. They publish weekly thought leadership, webinars, and downloadable [00:01:00] resources such as their PCI compliance program workbook, a business case for SOC 2, ISO 27001, the path to certification, and many more titles.

All available for download at no charge at Risk3Sixty.Com/Resources. Let Risk3Sixty help you build your business case to achieve certification compliance. Risk3Sixty.Com/Resources. All right, well if we're going to be talking about interacting with the Board of Directors, let's start with some basics.

Now, pardon me if you already know this stuff, but for some people it's always worth a review. What is a Board of Directors, and well, what are they supposed to do? Well, according to OnBoard, a Board of Directors is: An appointed group of individuals with a fiduciary duty to represent the interests of shareholders or stakeholders and oversee a company's management and operations.

It acts as a governing board responsible for making major decisions and providing [00:02:00] strategic guidance to ensure the organization's sustainability and longevity. The Board of Directors operates independently of the day to day management, offering oversight and accountability to safeguard the shareholders interests.

And in addition, the Board of Directors includes inside and outside directors, each with different roles and perspectives. Inside directors provide valuable industry knowledge and operational insights. While outside directors or independent directors contribute non partisan judgment and non objectivity to board deliberations.

Now all public companies are required to have a board of directors. They represent shareholders and many private companies and non profits will also rely on the guidance and supervision of a board of directors. I've seen some smaller companies have a board of advisors. But a board responsibilities might include hiring and setting compensation for executive leadership.

Adopting policies to address conflicts of interest. Shaping the organization's culture and vision. Basically [00:03:00] ensuring that the organization's values and strategic direction align with the interests of shareholders and stakeholders. Guiding the organization toward its long term goals and improving the organization's strategic focus and effectiveness.

Okay, good. That's good old motherhood and apple pie, by the way. Who appoints the board of directors? That would be the shareholders. So if you ever held stock in any public company, you may occasionally get a notice saying, Hey, it's time to vote. And as a shareholder, you get to vote for boards of directors.

And the members of the board then are going to do what? They're going to then allocate responsibility for day to day business. Basically appoint the CEO, for example. And so as a result, You as a shareholder vote for the board. The board would then appoint a CEO. They will hold that chief executive accountable for executing the vision, the guidance, the oversight that the board puts into place.

And if everybody does their job, it all works out. And if for some reason, you ever heard of things such as a proxy [00:04:00] war where somebody is trying to get somebody in the board of directors. I know that Exxon faced that fairly recently where they had an activist group with a very small number of shareholders, but they're effectively able to get Under the ballot for the shareholders, a opportunity for them to elect some, if you will, board members that were not aligned with what the prior board members were, mostly with regard to things such as environment, et cetera.

Nonetheless, it worked and that organization is now doing things differently. So if you're going to change something, the core of an organization. It's going to be the board. Now, with respect to cyber security, how's this board going to interact

with you as a CISO, as a security leader? Boards will likely execute these functions.

They're going to establish and approve the vision and risk appetite and strategic direction. And risk appetite specifically with respect to cyber and cyber security, but IT in general. And overall, how much is this company willing to do? For example, you might find out that if you're working for an Elon Musk company, they're willing to have a higher level of [00:05:00] risk than, for example, an old traditional financial corporation that just goes and does things year after year after year.

Another thing the boards to do is review assessment results and approve significant remedial actions. One of the things you find out is that when an inspection is done or when an audit is done, the auditors who find if everything is copacetic, it's great, you get a clean audit, bill of health. But if not, you get something called a finding.

And as we like to say, findings get funded. And so when there's something wrong, it goes up to the board and the board is now accountable to be able to say, Hey, we will either accept this risk. Okay, so what? Who cares? Or we're going to go do something about it. And when it comes to compliance, particularly audit, as I said, audit to compliance standards, that's sort of a forced hand.

And so therefore, as we're finding more and more compliance requirements for cybersecurity, you as a security leader might find some more of your things getting funded, not necessarily because the board wants to, but because statutorily they [00:06:00] have to. Third thing that I want to do is review management's opinion of cyber risk and preparedness.

Note, as I said before, boards are not involved in the day to day management of the organization. That's going to be the CEO, COO, CIO, CISO, anybody else that's out there that's kind of assigned and appointed for these duties. However, management makes an opinion, a statement on that, and the board has to come back and say, Yeah, you're running a little bit too fast and loose, or this is good.

I was talking to an associate the other day who called me up for a little bit of guidance and he's working for an organization that is attempting to bid on a government contract. And one of the things that you do with government contracts is you have to meet Federal Acquisition Standards, the FARs, if it's federal, it's the DFARs.

And one of the requirements there is your cybersecurity attestation. And a lot of these things in the past have been self attestations. The CMMC, Cybersecurity Maturity Model Certification, is sort of changing all that. Although from version 1 [00:07:00] to version 2, they handed back the ability to do self certification.

Nonetheless, the problem with the self certification is if the board signs off on this and they're found out not to be in compliance, there could be some significant financial fines and consequences as a result. And so why am I bringing all this up? Well, as a CISO, he was a little bit concerned that their CEO, again appointed by the board to go do the things, was willing to take on risk and bid for a contract.

They were not qualified to do, and as a result of not being qualified, required to do a self attestation that was essentially a lie, saying, oh, we do this, we do this, we do this, we do this, from a cybersecurity perspective, and they weren't doing that. And so, my friend came to me and said, like, G Mark, what do I do?

I can't talk to my original boss and his boss's boss or how many levels up to the CEO.

This guy's a cowboy and he just says, let's do it. I want the money, but we're going to end up losing a whole lot of money or maybe even losing the business. And so [00:08:00] my advice to him was, is you need to have a conduit to the board of directors. And I'm not saying jump the chain of command, be an old military guy.

I like to use the chain of command, but you'll find out though, is that there needs to be a pathway to get to the people who ultimately sign on the dotted line, who accept the risk on behalf of the shareholders to say, this organization has to be run correctly. And so there should be some process, and we'll cover that a little bit later when I talk about FFIEC regulations and recommendations for reporting structures.

But as a CISO, if you see the organization getting ready to do something really dumb, ideally you need to say something about that. And if you can't say something about it, or nobody's going to listen, or they're going to do it anyway, Now you've either got to decide to go along with it or resign. And anyway, not going to do any more on that subject, but I just wanted to point out just how important the board is, ultimately is sort of the appealing to the emperor, so to speak, if you think that your organization is going in places that they shouldn't go.

And then the fourth thing with regard to a board with cyber is approving plans for cyber risk management and improvement, [00:09:00] which makes sense. If you're going to go ahead and say, we want to improve this, we want to meet this capability, we want to incorporate these NIST 800 171 standards, we want, etc.

Board's going to have to sign off because typically that costs money and you're going to spend money if you can reduce risk or increase your profitability or improve your return. But in the case of security, it's mostly about reducing risk. Now, financial organizations, they have a lot of regulations and controls, basically because of the nature of their business.

As the legendary bank robber Willie Sutton replied when asked, Why do you rob banks? That's where the money is.

Well, let's take a look into the financial industry. Here's a template for best practice, and you might find something useful from here. The Federal Financial Institution Examination Council. Big long term for the FFIEC.

Information Technology Examination Handbook, or IT Handbook if you will, consists of 11 booklets. Now you can download these things for free on their website, but two are of interest here they want to mention. The [00:10:00] Management Handbook and the Information Security Handbook, or booklet depending on your terminology.

Now with respect to governance, financial institution boards of directors should oversee while senior management should implement. A governance structure that includes the following. Effective IT governance. Appropriate oversight of IT activities. Comprehensive IT management including the various roles played by management, and effective enterprise architecture. I know I'm talking about IT and not IT security, but roll with me for a little bit. Now the board of directors sets the tone and the direction for an institution's use of IT. The board should approve the IT strategic plan, information security program, and other IT related policies.

Now you may expect the board to establish an IT steering committee consisting of senior management, staff from multiple business units, and of course, IT leadership. Some organizations have established IT security steering [00:11:00] committees with similar membership. The purpose of a steering committee is to report to the board the status of assigned activities.

It may be assigned responsibility for strategic planning, Oversight or alignment with business needs. Now, according to the FFIEC management booklet, quote,

the chief information security officer, CISO, is responsible for overseeing and reporting on the management and mitigation of information security risks across the institution and should be held accountable for the results of this oversight and reporting.

But, But I find it interesting that this guidance goes on to state, quote, to ensure independence, the CISO should report directly to the board, a board committee or senior management and not IT operations management. End of quote. Think about my buddy a few minutes ago that I talked about who is facing this dilemma.

Wow, I got to go ahead and the company's, hey, if they followed FFIEC guidance. As a CISO, you go right to the board and [00:12:00] say, Hey, there's something. Now you got to play the politics. You have to understand. We've talked about this a lot of times. You've got four stages in your career. Technical, management, leadership, and political.

And as a CISO, you better be playing your political cards. So you don't want to be considered to be the rat running around behind people going, Guess what he's doing? But at the same time, you have an accountability and a responsibility as well. So figure out how you're going to do that thing, or work it through your reporting structure, but do not be a part of something that's going to cause problems.

That could just be a bad idea. Now with respect to responsibilities, if we're using the FFIEC guidance as sort of a template, these are things we're probably already doing. Implementing the Information Security Strategy and Objectives is approved by the Board of Directors, including strategies to monitor and address current And emerging risks.

And some of those emerging risks could be things like SEC guidance and reporting and reporting requirements because there's a risk if you, uh, do not report on a material incident, you'd be in [00:13:00] trouble engaging with management in the lines of business to understand new initiatives, providing information on the inherent information security risk of these activities and outlining ways to mitigate the risks.

You are invited in, of course, to all these business planning meetings where they're looking at new lines of business, expanding what we're doing, reaching out a new customer basis using third parties, right? Yeah. The problem is, is that CISOs don't always get brought in to those particular meetings because you're not considered strategic.

I remember way back when, when I think it was Verizon was buying Yahoo for some huge amount of money. And after the deal was figured out and they got a number assigned. It came out, Oh, by the way, we've got, just about 3 billion compromised, credentials in Yahoo. I think they went back and they reworked the number a little bit, but the point was, is that the CISO was not part of the deal.

Cybersecurity was not part of that tight, tight group of people. The financial people, can this deal work? The legal people, how do we make that work? Strategic folks saying is this part of our picture, but because it could materially affect publicly [00:14:00] traded stock prices It's not generally known that people are doing stuff.

That's why you hear about something I mean so and so company is now acquiring that company. Boom! The stock goes up It meant they were able to go ahead and keep things quiet but one possible idea is if IT security reported up through legal You might get invited to those planning meetings and a lot of these problems would be spotted.

So if you're in an organization that does mergers and acquisitions, you go out and acquire companies, and you're not having reporting structure or IT security, cybersecurity has some either dotted line or direct line to legal, consider looking into that. Another responsibility, according to the FFIEC for a CISO is working with management.

To understand in the lines of business, the flow of information, the risk, the information, the best ways to protect it. Again, close with IT because IT is going to be flowing the information. Monitoring emerging risks, implementing mitigations, informing the board. Here we go again. Management [00:15:00] and staff of information security and cybersecurity risks, and the role of staff in protecting information.

Can we say security awareness and training programs? Participating in industry collaborative efforts to monitor, share, and discuss emerging security threats. So that means industry collaborative efforts. Listen to CISO Tradecraft podcast, a great way to do it, but also be involved in other organizations and events and things like that.

And reporting significant security events to the board, the steering committee, government agencies, and law enforcement as appropriate. But if you're going to report things to law enforcement, you better have a legal on board and talk to them first. Now that's the management booklet from FFIEC. If we take a look at

the information security booklet, it states a few recommendations for management.

It's distinct from the board, which is of course not doing the day to day. Information security is far more effective when management does the following. Integrates process, people, and technology to maintain a risk profile that is in accordance with the board's risk appetite. If you hear that term risk appetite, it means how [00:16:00] much uncertainty are we willing to embrace to try to achieve our goals.

And I gave the example of someone like an Elon Musk who seems to have a much higher risk appetite than perhaps a public utility or some other organization's been around for years and years. It just kind of grinds it out and you don't get a whole lot of motion. Anybody who held Tesla stock, probably very happy about that risk appetite.

But sometimes companies and owners with high risk appetite, take on the wrong type of risk and things go to zero. So, high risk, potentially high return, but no guarantee of that. And the other thing for management is to align the information security program with the enterprise risk management program to identify, measure, mitigate, and monitor risk, meaning that you should have a risk register and IT security has a risk register, but do you have a part of a bigger risk register?

Are you part of some of the overall things that you should be looking at? And to have effective IT governance, management should establish an information [00:17:00] security culture. It promotes effective security program and the roles of all employees in protecting the assets. Now, it's kind of tough for you as a CISO, as a security leader, to change the culture of the organization.

Now, if you're a founder, it works. I was in the military as a commanding officer. For the most part it worked, particularly if I was a, what we call a pre commissioning or first, first COO there in the Navy. You could set a sense of culture and it tended to persist, but culture is going to be the expectation of individuals in a group on behavior from each other.

And so once the culture is established and formed, it's kind of difficult to change, corporation. And so, okay, Peter Drucker, what's it, culture eats strategy for breakfast, right? You can have all these great strategies, but if your corporate culture doesn't work, I also say that. You know, culture will eat policy for lunch because you could write policies, but if people don't then think that way it's not gonna work.

Management should also clearly define and communicate security responsibilities and [00:18:00] accountability and provide adequate resources to effectively support the information security program. So I'm thinking if I'm in the financial world, this sounds great. I got all these really really good things that are telling me that I'm supposed to get stuff.

And the board According to the institution's written information security program. Meaning that the board signs off on it, not just the CIO. Affirm responsibilities for the development, implementation, and maintenance of the program. And review a report of the overall status of the program at least 7, 8, 9 years ago.

And you're lucky if you got to the board once a year. Now they're going to talk to you every quarter. I brief a board for one of my clients at least twice a year. And that's when they have their board meetings, but I have interactions in between that. But this is a real opportunity now to be front and center.

We'll probably talk, I think I did an episode on how to brief the board and do it effectively, but we'll, we'll [00:19:00] get into that a little bit, but that's not going to be the entire purpose of this episode. But let's go back to our initial four board functions we talked about at the beginning of the show.

Vision and risk appetite, assessment reviews, management's opinion on cyber risk and plans for improvement. Now to improve the company's vision, risk appetite and strategic direction, those things must first exist. And the board is responsible for developing a risk appetite statement. The strategic direction comes from the board, but the execution of that falls under the role of the CEO, who may further delegate accomplishing those functions within the company.

Now, what about the vision? You know, I said, if you are a founder, you sort of establish the vision of what it is you want to do with your business. But as the company grows and gets larger and you bring in outside directors and things such as that, that vision tends to morph a little bit. And so as a result, the board is going to assign vision and say, here's where we think we ought to be in three or five years.

And the CEO executes on that and the chief operating officer to make sure the operations support the execution, which support what the [00:20:00] board wants to do. Okay, looks pretty straightforward. So what's the board going to do then? They're going to focus on governance. That is how can we guide, monitor, perhaps even mentor and hold the C suites within the company accountable.

To the shareholders who ultimately the people who voted for the board. Now, often members of boards of directors are professionals in their fifties or sixties. They get a lot of work experience. They're former CEOs or CFOs. They built and run successful companies. And they all impart that wisdom to the organization and provide a sounding board to assist the CEO in executing the company's mission.

Ideally, there's sort of a positive working relationship. between the CEO. Sometimes I've seen incestuous ones where the CEO has come to dragging the board along and the board is not providing that effective oversight and that gets a little bit dangerous because that loss of accountability, that having that back check to ensure that the CEO doesn't drive the company off a cliff, does present a risk for an organization.

Now, what makes a board member useful is having this experience. They understand business risk. Their wives know that cyber is a [00:21:00] business rift. They understand that programs need funding and staffing if they're going to have the resources necessary to be successful, and they also get to vote on the CEO and say, hey, is this strategic direction correct?

Are we going the right way? Are you executing it? And things such as that. Now, one of the things I've looked at as an experienced cyber professional, having done this stuff for decades, is, hey, should I get on the board? But then again, a lot of the board members, when you look at them, and again, the recent SEC ruling that came out, which did not require.

Publicly traded companies to disclose or identify what cyber experience their board had, which a lot of us said, why would they take that out? Well, maybe it's going to come back in another iteration, but it's interesting to take a look at it. I said, how can you add value at that level? Because boards aren't there doing operational stuff every day.

And so if you've been successful in getting on to a board as a cyber security expert let us know. Send us a little email or something like that or connect with us on LinkedIn. I'd be kind of curious to understand the story and I might want to talk a little bit more [00:22:00] about that. Now within the company, boards of course are going to review different assessments. They're going to be quarterly financial statements.

They look at the health of the company. How are we doing? Based on my experience, it looks like we're not growing fast enough relative to what the market is, right? I'd like to see us decrease costs in this area. So it could be more

profitable or it looks like the economy is slowing down and we really need to pull in some of these riskier ventures that are going to have a requirement or look at the investments we've approved when interest rates are 2%.

And now that they're going to be 7 percent or 8 percent maybe the return on investment for some of these things that we previously approved are not going to be strategically as valuable way to put our money. So all these things go at that level. They can look at audit findings and agree that some things are issues or the worst thing you want to find is systemic problems.

Like a systemic problem is something that a whole organization might suffer from, not just one little element or one person within the company. And so it'd be natural for a board to look at assessments on cybersecurity from the CISO or the audit team and say, Hey, what are we [00:23:00] doing? It doesn't make them experts in cyber.

And so you don't want to share raw vulnerability scan reports with them. Cause that's a way too much in the weeds and they're not going to understand. And they're going to walk around saying, well, this person in the room and they don't even understand how to communicate. See if raw scan data is too much in the reads.

Well, what is appropriate level? In my opinion, board members, especially those on audit committees, are used to reading audit reports, right? So it makes sense to share with them cyber audits. They can be large red team exercises that'll test your defenses or important pen testing on critical systems. And for example, you might say, We hired an external company to investigate if our public website had vulnerabilities that might allow an adversary to disclose, alter, or deny access to our critical data.

During this review, they found two issues. One was minor. We fixed it. The other one was a situation where an attacker could make some changes to the URL, potentially access another customer's data. Once that vulnerability was made aware of, we fixed it within four days. And we are continuing to [00:24:00] monitor for other security issues.

Now, that's probably enough. You don't have to get into, well, what was it? Was it an injection? Was it a problem with the active code? Was it JavaScript? Did it have anything to do with OpenSSL? If it was an old one, or maybe... All these things, these level of details, you ought to know them. And every time I used to, I do briefings, I have what I call backup slides.

So I've got the nice little, here it is, summary and then all the details. So if you have to dive into it, you can do it. It makes you look prepared. And it doesn't mean you look like you're shooting from the hip if you get more questions that way. And after a while, the board member or the board and as a whole realize that you got your act together and you're managing this stuff.

And every time they ask a question, you can answer it. And you've got at least something that you've already brought to back it up. They're probably going to back down a little bit and say, okay, fine. Tell us what you need from us to get your job done rather than we're going to direct you to do things like that.

All right. So have a solid plan to fix things if there's a problem. Now, just because you're doing pen testing and scans doesn't mean you're gonna be 100 percent secure. Obviously, there's [00:25:00] some companies that bug bounties and they're always looking for inputs, which is a great way to lower risk. But sometimes dozens or even hundreds of bugs are found over a period of time.

And that's just kind of the way the industry is. Boards need to understand that. You might hear a board question like, well, are we secure? And that's probably one of the questions that CISOs hate most. Because cyber is not and never will be a binary answer of the yes or a no. And when you hear that question, are we secure?

I recommend you restate it to them as the following, something like this. Security is a process. That's not an end state. There is no single metric to say we are secure and no corporation will ever be 100 percent secure. But what I think you're asking is, are we meeting the standards of due care to reduce the risk of material cyberattacks to a level of acceptable risk?

That's the reason we fund our cybersecurity program to apply the resources to reduce our risk that the board has deemed acceptable. So those [00:26:00] terms I'm talking about... Standard of due care. Due care means that according to the law, according to general common practice, you are doing what the industry expects you to do.

And if you fail to meet a standard of due care, you could be held liable in a court. The other thing I mentioned is material. What is a material incident? That was the whole thing that the SEC came out about. We talked about that previously in other episodes. But the whole idea is, at what point is it going to hurt?

If I dropped a penny, On the sidewalk. I do not consider that a material loss. But if I were to drop my wallet, it had all my credit cards and a whole bunch of cash in it, that may be more material and that was something I would care about. If somebody stole a dime out of my, convertible that was sitting there in the ashtray, yeah, that's probably not material.

Someone steals your car, then you make a police report. It's a, it's a material thing. You get the idea. And the third one then was acceptable risk. That acceptable risk is set by what's called a risk appetite. What is it we're allowed to do? [00:27:00] We have risk and then I apply countermeasures to get to some residual risk.

And if the acceptable risk is here, I need to reduce it a little bit more. And so I go back to the board and say, do you want to live with this extra risk or do you want to fund it? But once I get to here, don't keep going. You're not going to spend 10 or 20 to go ahead and protect against losing a penny.

It just doesn't make sense. And so what you can do is if you press for detail, you could say we've met reasonable security, we brought in an external auditor, they measured us against a well known framework or a well known thing. The NIST cybersecurity framework is nice. It's nationally accepted and then their conclusion is we're much more secure than the typical industry vertical where we are right now.

And the things that we had to work on, we are working on, we've got a remediation plan. We expect to have that fixed within three months, six months, nine months, whatever it happens to be. Essentially, what you're trying to say is an external auditor assess their organization to ask them, answer the question, are we doing enough and are we doing the right things?

It's similar to any other audit that's going to be going to the Audit Committee, but we [00:28:00] want to follow desired control objectives of a familiar framework like ISO, NIST, something like that, CMMC coming out with the NIST 800 171. Don't roll your own. The problem is, is that you don't have an authoritative, no matter, even if you've been doing cybersecurity for over 40 years like I have, rolling your own is not going to be necessarily the way that you build credibility, because someone's always going to question your judgment.

But it's a little bit harder with the herd mentality to point to a government standard or an industry standard and say that that's not the right thing to do.

Now, in addition to benchmarking ourselves against our industry, it really helps to be able to finish better than that. You want to be good enough.

You want to avoid being accused of negligence because if you can say the average cybersecurity score is here and get some of these scoring companies that do that and you're here, that tends to indicate that you're doing a lot more than everybody else. You want to aim essentially though for good enough.

You can't do absolutely everything. There's just not enough money in the world, but if you've got an infinite budget, let me know. I'd like to help you spend it. [00:29:00] But reality is the goal is to protect the revenue of the company from external and internal actors. We want to ensure that we align with the board's stated risk tolerance and we don't spend more on a control or a precaution.

Then we're going to get back in terms of reduction of risk. At some point we got to live with things and the things that we decided to live with say they're either such a low probability that if they happen, we'll deal with it. And that was kind of the pandemic a few years back, right? We weren't thinking about that once every a hundred years like clockwork or the impact is pretty low.

How often does it happen? How bad can it be? What's the damage to our assets? And that's your model for being able to figure out what your risk is. Now, a board that believes that they have a reasonable assurance from the CISO, you still might get asked further about some specific attacks, the stuff that's in the news and things like that.

And so a board member might say, Hey, I read in the Wall Street Journal about this competitor having their cloud account compromised. So, what are you doing about this? To keep [00:30:00] our cloud account from being compromised. I think we're on this Microsoft 365 thing, right? What are we doing about it? So be sure you have answers for them.

Be able to address. Different attack vectors, such as malware, cloud account compromises, insider threats, ransomware attacks, BEC, business email compromise, distributed denial of service, supply chain attacks, phishing, anything that's in the mainstream stream news. If you're going to go brief the board, I would go hit the financial pubs for the previous two weeks and try to see what's top of mind.

Because that's going to probably be on the agenda for somebody to say, I read this. I don't understand it, but I want to admit I understand it, so I'm going to go ahead and ask about it so I can get someone to explain it for us, and I'll look

smart for bringing up the right questions, and I might actually learn something in the process.

Yeah, however that happens to work out. Boards want to confirm that the organization can stop a range of attacks. For which you have been able to build defenses and they tend to look about a year in advance Not five years in [00:31:00] advance. We're not building defenses for five years out Remember G Mark's law on cyber security half of what you know will be obsolete in 18 months And so it's really tough to have a long long long strategic term but if you can't stop attackers now, you better have a P O A M, Plan of Action and Milestones, showing when you can.

Now board items, board members are thinking about big things that could cause material harm to company revenue. Like, what's the impact of disruption to business operations when a large cyber event happens? Is it going to be like cloning a pipeline's bad? Everything gets shut down, it impacts All millions of people.

Is it customers can't buy from our public websites? But we'll come back because they love our stuff because we don't have any, valid competitors. And so they get a little inconvenience. Is it a password change to fix it? Is it going to be the government shows up and impounds everything?

Boards want to understand what the risk is and they want to look at sensitive internal data that could be stolen or made public or both. I mean, if the data is sensitive and regulated, like protected health information, [00:32:00] PII, personal identifiable information, payment card industry, PCI information, then a breach can not only cost you in terms of having to pay fines and regulatory issues, but it could have a reputational impact as well.

Now, I don't know about you, but I think there's enough breach fatigue going on out there that every time I get a notice of like, you know, your information has been compromised. Last few ones, I see they don't even give you the free credit monitoring anymore. Maybe they just get out of that business and people said like, yeah, screw it.

I've already got 10 of them going at the same time. But the point is, is that, you have to consider beyond just the financial risk is the regulatory risk, the legal risk. And, the reputational risk that comes out of a compromise. And just because your company's safe now doesn't mean that you'll remain safe a year from now.

So, if you go back and you think about a castle, if you, defending an old medieval castle, that works pretty well if everybody just kind of runs up and they try to beat on the doors or whatever. They just, you know, whatever you do with castles. You know, throw stones on people, pour boiling oil, hit arrows.[00:33:00]

But if they start showing up with ladders or digging tunnels and you say, Hey, you know, threat assessment, uh, we're taking a look at them and they're doing something a little bit different and we don't have a defense against that. Well, the fact that you can see what your opponent is doing, the threat Intel suggests that maybe we need to change our, um, approach and things like that.

So understand the consequences of how cyber attacks can cause severe disruption, data loss, reputational damages, and, and then things like in healthcare that might even be loss of life. If things go horribly wrong and things such as that, every industry is slightly different. What it prioritizes, but protecting revenue is almost guaranteed to be a generally accepted practice.

So that brings us to that fourth item we talked about. How does this get the CEO and the board to approve our cybersecurity spending? Now, let's compare the scenario with the experience of buying a car. Some of us might have tried to buy a car at some point in our lives, and you look at cars for a while, you have some window, and you say, okay, they've got three options.

So you sit down with your partner and you say, okay, here are the three options we've been considering. Option one is a Honda Civic. With bells and whistles, maybe it goes to about 30, [00:34:00] 000 when you pick it. It's a simple car. It's reliable. It gets you where you want to go. Option two would be a Subaru Outback.

Now it's about 40, 000. It's got a lot more room in the Civic. It's got four wheel drive. If you live in snow and ice areas, if you like to go out and go camping or outdoorsy, that could be a little bit more practical. Option three would be like a Chevy Suburban and it might be 60,000. And I know that's probably a little bit low, but it can fit a lot more people, a lot more storage.

Then the Outback or Civic, of course, it's a lot more expensive. Now, as you can see, it's an understanding that if we spend more money, you tend to get more capabilities. But most families, in this case, have a limited budget and in cybersecurity, we may also be facing similar things. The average family might not be able to buy the 60,000 Suburban as much as we'd like it.

So we have to apply this thinking as a CISO as we provide alternatives to our approvers who are going to decide what we can spend. We might create a cyber budget that has cyber practices. There's a three million dollar program that with the must haves, absolutely got to have these things. A four [00:35:00] million dollar program with the should haves.

And then maybe a 6 million budget with all the could haves. Now, psychologically, if you read about menus and things such as that, when you have a high and a low and a medium, people tend to kind of go to the medium one. The high one, you sometimes price it way up there. So you're like, wow, 57 for a steak, but wow, I can get a hamburger for 12, or you get a salad for nine. It's like, well, actually that doesn't sound so bad when in fact, you know, 12 for a hamburger to me seems like a lot of money, but maybe today it isn't. The whole idea though, is that if you've only budgeted the 3 million, if all you paid for budget in your budget is the must haves, then the should haves and the could haves probably never going to happen. There might be things like having someone dedicated to help the business with their business continuity plan, by an extra application security tool, since you might not have a couple FTEs to run it. And so you need something that can manage that, or having only a single person who can run the SOX audit and the IT controls and therefore you've got a single point of failure if that person leaves the company.

So you want to think these things through and explain [00:36:00] the risk to the board as why these things are important. And when the business understands which... Cyber practices are not being able to be performed or they're resource constrained, they know they've got a choice to make. Either give you the additional budget or accept the risk.

Now, don't be accepting risk on behalf of the organization. You as a CISO are not their risk acceptor. That S does not stand for scapegoat. If you accept risk, you're the scapegoat. What you want to do is you want to inform them of the risk, the people, the board members who are appointed to assign the risk and make sure they make intelligent risk based decisions.

And then you're doing your job right. They're going to be asked for your opinion, perhaps, and your best answer might be of the low, medium, high. I think we ought to have, we have to have the must haves, but the should haves make absolutely sense. The nice thing is it'd be great, but I don't want to ask for absolutely everything because we have to execute the business mission.

There are other things that we have to do to ensure our company meets their profitability targets. However, I would request is that if we are running ahead on

[00:37:00] profitability revenue, that we consider funding these things because that's going to reduce our risk for current revenue model. Yeah, about this much, but if we make a lot more money, all of a sudden it's material and we care about it.

See, organizations often hold a reserve for unplanned events. You're always supposed to have like a rainy day fund or money set aside in case it's in between jobs. This could happen at any level. At the board level, the CIO's level, the money, but C level executives may keep little pocket of money on the side.

If halfway through the year... The SEC passed a new regulation that requires you to do additional reporting, additional work. That might be a way to get the extra money that you need because you left on the table earlier, but then you go back and said, well, this is now a requirement. This is not a nice to have.

This is a must have, but also think about use or lose money. I know in the federal government every year, 30th of September, well, I'm recording this episode on the 30th of September, last day of the fiscal year, what happens? If you don't spend it, you don't get it back on the 1st of [00:38:00] October. And oh, by the way, if you didn't spend it this fiscal year, you must not need it next fiscal year.

So we're going to take it away from you. And so all of a sudden there's a big flurry in the last month of the fiscal year in the federal budget to buy boxes of pens, to buying a fleet of trucks and everything in between. So we find out then if there's a business unit during the year, perhaps, that had a vendor negotiation that fell through.

They had money that was budgeted, set aside for something that just didn't happen. If you are monitoring what's going on in the organization and keeping track of it, you might be able to go ahead and say, hey, I know that you end up getting dinged if you don't spend the money. Not so much that you want to go ahead and have 5,000 ballpoint pens, but if you don't spend it, you're going to get your top line cut next year.

So let me help you spend that for you. And that'll be really good for your next year budget. All right, you're kind of like Tom Sawyer. You're helping them paint their fence, so to speak, but you're getting the benefit from it. And, as a result, you can do this anticipatory planning and also interact with the other executives.

And they see that you're helping them, they're [00:39:00] helping you, and things like that. Now last month in episode 141 on emerging risks and episode 146 living in the materiality world, we discussed a lot more detail the new SEC requirements on reporting on material cybersecurity events. I alluded to them a little bit and I'm not going to repeat that here because now it's redundant, but if you haven't listened to 141 and 146, go do so because I think you'll find that information most helpful.

Okay, so we've covered a whole bunch of stuff about board perspectives on things. So let's recap. In today's discussion, we explored the board director's perspective on cybersecurity, or at least what it should be. Boards would have at least four key roles in cybersecurity. Setting the company's vision and risk strategy, reviewing assessment results, evaluating management cyber risk stance, and approving risk management plans, and despite any lack of technical expertise, and again, that SEC ruling took out that requirement for boards to document what their cybersecurity expertise is. Boards do bring valuable experience and guidance to cybersecurity [00:40:00] and to effectively communicate with them, avoid technical jargon and share audit reports and key findings. See, boards are going to seek assurance about the organization's cybersecurity health.

So emphasize reasonable security measures rather than claiming absolute security. So external audits against recognized standards can really bolster this assurance. And boards also want to understand the potential impact of cyber threats. So be prepared to discuss common and current threats and mitigation plans to deal with that, and potentially some money that you might need if they say we care about that.

When you budget for cybersecurity, It's about choosing the right level of protection and boards appreciate understanding the budget trade offs and they may allocate additional funds when necessary but at some point in time if you're facing funding cuts know where that absolute line is to say if you cut below this point you can no longer provide the level of assurance that the board has said that they need to meet this level of risk tolerance.

You can drive through the minimums if you [00:41:00] wish but understand that we're now running at risk. We're running around without a seat belt. I'm a highway. And the ICE. But we can do it. Some people live. Not everybody, but some people do. And last, the organization's got to have reserve for unforeseen events.

Now, provide funding opportunities for cybersecurity projects, but be careful, I said, when I was a junior officer, I thought if I saved up my money, I could go ahead and get something big toward the end of the year. At mid year review, one of the other department heads who was spending a whole bunch of stuff said, Hey, ops, you're not spending your money.

Engineering is spending their money. So we're going to take it away. But, but I got all these things. So sometimes you got to learn the organizations and front load at the quarter or at the fiscal year to get your stuff spent. So that you can get that allocated. Of course, that's almost the exact opposite when you're dealing with sales or trying to close out the quarter, trying to close out the year, and they'll offer you really, really good deals to get that money in at the last minute, you may not have the money left at that last minute.

So figure out what the politics are and how that works. But in summary, communicate clearly, provide assurance, outline budget considerations. Those are going to be [00:42:00] key when engaging boards on cybersecurity is their role is to guide and oversee, rather than delve into the technical details, and they're not doing the execution.

Alrighty, well I hope you've enjoyed the show on Board Perspectives, and it's been brought by our sponsors Risk3Sixty. So they help keep the show free for you. So support them, visit their links, take a look at the show notes, go to Risk3Sixty.Com, and check out their website. You can also make our day if you give us a 5 star review on your Apple podcast, you're listening to.

And if you're following us on YouTube, go ahead and click follow. I used to wonder why people would always ask that. And then I realized that now that we're doing YouTube, that's how we can keep ads from getting thrown into our stuff. So if you haven't done so already, subscribe to our YouTube channel.

Also our LinkedIn channel, LinkedIn CISO Tradecraft. We do more than just a podcast. We try to keep a high steady stream of high information, low noise, good signal to noise ratio to keep you informed throughout the week of things that we think are important. And as always. Feel free to get in touch with us.

Send us a note on [00:43:00] LinkedIn. Send us an email at CISO Tradecraft. Let me know what you're thinking about and see what we can do to help you improve your CISO Tradecraft. Until the next time, this is G Mark Hardy, your host. Thanks for listening or watching and stay safe out there.