# Episode 146 - Living in a Materiality World

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast to provide you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today, and we're going to be talking about living in a materiality world. Okay, pardon the pun, but welcome to the show.

I want to talk about something that you really need to know about if you don't know about it already, and you should review it. Even if you are familiar with the concept and that's a concept of materiality. Now in episode 141, we had attorney Adam Isles from the Chertoff group on the show and we discussed the new SEC final rule on cybersecurity disclosure for public companies.

Now, if you're not a public company, still pay attention because lawyers don't decide not to sue just because you're private. Now, regulation [00:01:00] is now requiring four days from the determination of a material cyber security incident and public disclosure in an 8-K. Now, in addition to this concept here that we talked about, and you can go back and listen to that episode for a little bit more detail, Tony Robbins had said success leaves clues.

Now, a corollary to that is that, well, regulations leave clues. And so let's look at the antecedent of this new regulation to see what we might come to expect. But first, let's take a moment to listen to a word from our sponsor. Risk3Sixty is a cybersecurity technology and consulting firm that works 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 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 [00:02:00] no charge at Risk3Sixty.com/Resources. Let Risk3Sixty help you build your business case to achieve certification compliance.

That's Risk3Sixty.Com. Okay, so back to our program. What is the concept of material? Now, the Public Company Accounting Oversight Board, in their Audit and Planning and Risk Assessment Rules states, ,quote in interpreting the

federal securities laws, the Supreme Court of the United States has held that a fact is material if there is a quote, a substantial likelihood that the fact Would have been viewed by the reasonable investor as having significantly altered the total mix, yet an even another quote in there, of information made available.

Now, as the Supreme Court had noted, determinations of materiality require delicate assessments of the inferences a reasonable shareholder would draw from a given set of facts and the significance [00:03:00] of those inferences to him. Now, the Security and Exchange Act of 1934 mentions material fact no less than 25 times, and the Securities Act of 1933 proscribes with multiple references, untrue statement of a material fact, and omits to state any material fact required to make the statement not misleading.

So there is a whole bunch of history on this going back to the 1930s. There's even a 1932 case of the T. J. Hooper case where Judge Learned Hand had basically talked about The requirement for due diligence. And for those who want to go back and look at that particular case from a number of years ago, what, 91 years at this point, it turned out that the essence of it was that a tugboat was bringing some cargo.

They did not have one of these newfangled things called a radio. They went out to sea. Hit a heavy storm, lost the cargo, pulled into port. Owner said, Hey, where's [00:04:00] my stuff? And they're like, yeah, act of God, we can't help about that. It says, well, there's a hurricane out there. It's like, yeah, well, you didn't know that.

So it was on the radio. Well, we don't have a radio. Why don't you have a radio? Well, because the Coast Guard doesn't require us to have a radio. So we didn't get one. Well, that went to court and eventually got to the point where the judge had said, just because you're not ordered to do something doesn't mean that prudent behavior is not a responsibility.

And in this day and age, when you consider the cost of a radio versus the cost of losing that entire cargo. You should have bought a radio. And so, pay up. So, let's fast forward another 20 years, around 1954. Now, the AICPA Committee on Auditing Procedure issued a booklet entitled Generally Accepted Auditing Standards, Their Significance and Scope.

Alright, auditors are probably familiar with that. And it states, in quotes, There should be stronger grounds to sustain the auditor's informed opinion in respect of those items which are relatively more [00:05:00] important and in respect of

those... in which the possibilities of material error are greater. Put in words, the principle of materiality is inherent in the work of the auditor.

And so what we're starting to see is that this is not a new concept. So you can't end up in a court case and act surprised as a defense, unless maybe you've been on the same job since 1933, and then I guess you could plead ignorance there. But as Adam Iles had said in our prior show, Quote, what we're trying to think about when we think about materiality is impact, whether that's financial, operational, or reputational, or from other litigation safety concerns.

But at the end of the day, it's a corporate governance practice. Okay, if we understand then that part of governance, which is the oversight that you What leadership management has on an organization to ensure that it executes its roles and missions [00:06:00] correctly and in alignment with the designated risk tolerance.

We find out then is that organizations in general don't always do the right thing or what they're supposed to do. And they've got to be more specific about that. When I say organizations, we like to think of them as amorphous entities. They're really humans and humans that are making decisions. A lot of people are going to optimize their decisions well for themselves.

And not necessarily for the benefits of the shareholders, the customers, the employees, or anybody else. And so what we find then is that, well, I guess you could probably describe cybercrime that way, right? I'm not really concerned about the welfare of the stockholders, or the welfare of the customers, or the welfare of the company.

We just want our money. Got it. Well, in any case, if we take a look in January of 2022, the Security and Exchange Chairman Gary Gensler said, the economic costs of cyberattacks is estimated to be at least in the billions and possibly in the trillions of dollars. Now, [00:07:00] I've also heard that cybercrime is considered to be the world's third largest economy, if you put it all in aggregate.

Well, building up on Secretary Gensler's statement, he stated that investors increasingly seek information about Cybersecurity risks, which can affect their investment decisions and returns. Okay. Let's think about it for a moment. If you're an investor, whether you're an individual investor, small person like me, or you're a corporate investor where you're writing checks with lots of zeros on them, what you want to do is you want to come up with kind of a risk to reward ratio.

The more risk you're willing to take, theoretically speaking, the more reward you should be eligible for. But reality, it kind of works the other way around. If you want to have outsized returns, you often need to take outsized risk. Now, that's not always within everybody's risk tolerance. And so therefore, what we want to be able to do is ensure that investors in this particular case, because after all, it is the Securities and Exchange [00:08:00] Commission, are given sufficient information that they can make a decision without anything being hidden from them with respect to materiality of different issues.

And in particular, we're talking about Cyber. Now, if you happen to know that a company had a major cyber attack, and they're getting ready to announce that tomorrow, and their stock is going to tank, well, what's going to happen? Someone's going to say, sell, sell, sell. Well, that's kind of insider trading.

You have information that's Not generally available to the average investor. So whether you're the consultant and they're doing the investigation, an employee, the executive, or even the criminal doing the activity, doing that represents further criminal activity. And so we're just not going to go there.

Now, what happens though, is that if we think about what is the SEC trying to do, they're trying to design rules that are going to strengthen the technology infrastructure of the U. S. securities markets. And they'd apply to things like stock. exchanges, clearinghouses, [00:09:00] FINRA, and things like that. Okay. Those are the entities that represent sort of the, the core of what we're doing.

Now, what happened is back in 2014, the security exchange commission developed rule known as regulation systems, compliance, and integrity, or reg SCI, not to be confused with SCI if you have ever served in DoD anyway, but it was originally adopted back in November of that year, 2014, for the purposes of reducing the occurrence of system issues.

Improving resiliency when system problems do occur and enhancing the Commission's oversight and enforcement of securities market technology infrastructure. Okay, that sounds like goodness, and we would like for our systems for trading to stay up, remain up, to resist attack, so to speak, and make sure that the oversight and enforcement of the technology infrastructure is there.

Just saying. I got this. Don't worry about it. You don't need to look is not going to essentially meet this compliance [00:10:00] requirements. And this goes back to the original kind of working assumption that people don't always do what they're supposed to do, but they'll do what they're incentivized to do. And if you're facing significant penalties, either civil or criminal, where you change

your pinstripes in for orange, that's a motivator to help people stay on the straight and narrow.

Now, if you're going to do the right thing anyway, you really don't care about what's at the edges of your behavior. Okay, that little electric rail on this side and this side don't matter if you're going to be going right down the middle. But in this particular case, we want to assume, if you're the regulatory agency, that you're going to get a whole range of people.

Not all of them are going to go ahead and do the right thing all the time. So this regulation required cybersecurity testing, data backup, and business continuity plans. Now that's something that we do at very small levels. SMBs do that. Well, if you think about it, it's even more critical if you've got a national financial infrastructure running and you'd have to ensure that you've [00:11:00] got testing and backup and continuity and things such as that. Now, in the event of a reportable incident, something happens at the exchange or whatever, the entity would file a three page form SCI, which OMB estimates, you know, they always have in the tax forms, they'll say, well, here's how much work it's going to take you. The average burden per response is a modest 25 hours.

Well, in the grand scheme of things, maybe not that much. Now this regulation, you say like, well, where is this? Why do I have to do it? How does, why do regulations have the force of law? And because, well, they're in the law. They're in Title 17 of the U. S. Code. And Title 17 pertains to commodity and security exchanges.

And specifically, this is Part 242 of Title 17. And now we finally start to get some definitions that we can look at. That if you will have the force of law because they're defined there. So an SCI event, remember that Systems Compliance and Integrity. An SCI event means an event at an SCI entity that [00:12:00] constitutes a system disruption.

A system compliance issue or a system intrusion, okay? Disruption, compliance, intrusion. Disruption, CIA. Okay, that's availability. Intrusion, confidentiality. Compliance issue. It's not a C or an I or an A. Notice that it's sort of outside of that. But it's still important and you do have to be compliant. Now that's just a regular SCI event. A major SCI event means the SCI event has or had the reasonably estimate that this is going to happen. Any impact on a critical SCI system or a significant impact on the entity's operations are on market participants. Okay, now we're finding there's a little bit difference between having a little problem with one of the servers going down to you cannot trade.

And so that becomes a major SCI event if it's going to impact at that level. Now, what do you have to do? Because again, we're looking for clues here. The SEC has this new rule out. [00:13:00] It's effective 5th of September. 2023. And we're looking at what has been out there in the past to see are these going to serve as templates for what we might have to deal with.

So that's why I'm digging into history here. And here are the details.

And this is section 242.1001 of that Title 17 of US Code. Each SCI entity shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its SCI systems, and for the purpose of security standards, indirect SCI systems, have levels of capacity, integrity, resiliency, availability, and security adequate to maintain the SCI entity's operational capabilities and promote the maintenance of fair and orderly markets. So, capacity, integrity, resiliency, availability, and for security. [00:14:00] And these are the things that are considered to be a requirement. Think about your organization.

Do you have those items nailed? Are they locked down? Are you in good shape? And if the answer is possibly not, then you got some homework to do.

Now, how do you prove it? The policies and procedures that are required by this paragraph we just went through shall include at a minimum The Establishment of Reasonable Current and Future Technological Infrastructure Capacity Planning Estimates.

Hmm, that means you can't be running at 95, 96, 98 percent of capacity, because you, unless you're expecting your business to draw down, you're going to hit a wall. Today, when we look at the cost of computing, the cost of communications, storage, etc., we find out that running out of space... is almost an inexcusable error.

I'm going to mention that in a couple of minutes about how that actually happened very, very recently to a major manufacturer, but you want [00:15:00] to have current and future infrastructure capacity planning. Number two, periodic capacity stress tests of such systems to determine their ability to process transactions at an accurate, timely and efficient manner. Now that's interesting because you do a stress test. Do you want to stress test in production or in testing? Well, you know, the test system, if it goes down, so what, who cares? Production, you don't want it to go down because it's your production system. But I have had a project.

I had a client who wanted to do a stress test or a financial organization, and they wanted to do it during business hours. It's like, are you really sure you want to do this? I said, yes, we are. They want to do like a DDoS approach. Well, I, hired the smartest DDoS guy that I could find. And he was very much in demand.

So much in demand that he basically just said this ridiculously high hourly rate. And he said, I'm not that greedy. I just need this to go ahead and ensure that I can work a reasonable number of hours a week. So if 10 people want me to work and I've got room for 2 or 3, I'll go to the high [00:16:00] bidder. So I actually passed his rate through at no markup.

Didn't make any money on that. Why? Because I felt I had an obligation to the client to deliver them value. And this guy knew how to manage this thing so he could take it right to the edge but not break anything. As a result, we're able to do the stress test. So if you're going to do stress test on production, find somebody who really, really knows what they're doing.

Sure, you could go ahead and find criminals that will stress test your systems. But, they have different rules of engagement, and they don't necessarily, keep things from breaking. The third item is a program to review and keep current systems development and testing methodology for such systems.

A lot of times the testing methodology tends not to be in writing. I remember years ago when I'd work as a consultant, I was with Booz Allen and we were doing a federal government project and we had, we had written all this custom software and we had a huge test plan. And with that test plan, it was all written down and what happened is we went through and if the program does this, if it does that, if it does that, we go through all the way through there and it [00:17:00] all works correctly.

Then we could say, yes, this system is performing in accordance to plan. Now, of course, one of the things that you might not test for is things, well, you didn't think of. And so as a result, if you put in A, it should do this. If you put in B, it should do that. If you put in C, it should do that. Okay, great.

We're done. But what if you put QZXYWN'

that's kind of the security testing that we tend to do, and that gets into a little bit different testing scenario. It may not be part of your regular review and testing, but it's not a good excuse not to think about that. Number five is business

continuity and disaster recovery plans. All right, that makes sense, and that sounds like a good thing, but...

Any more detail? Yes, that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading. Remember what we're talking about here. We're talking about these SCI systems and to our resumption of critical SCI systems following a wide [00:18:00] scale disruption.

So you've got a couple of days to get back. It's a little story. I don't think I'm talking out of school here because it's been almost 22 years, but, if you remember for those of us who were around back on September 11, 2001, probably all were here, but you weren't all thinking about finances, the stock market shut down for a couple of days when it finally did open, boom, you know, the market crashed, but it recovered.

It got some resiliency back in there. The bond market didn't come right back up right away. And why didn't it come up? I mean, everybody's thinking, Oh, we got this problem, this problem. Well, the difference between the bond market and the stock market is sometimes the bond market finances nation states.

Your country gets bonds issued and that's how the country stays in business. And as understood that the primary processing for all this bond trading in New York. was in Tower 1, the World Trade Center. But they had a disaster recovery plan, they had a backup can, continuity plan, and the backup was in Tower 2.

Yeah, it did not include in the disaster [00:19:00] recovery or business continuity a catastrophe scenario. And as a result, we see specifically maintaining geographically diverse backup capabilities. And I don't know whether this came as a result of that. Things were down for a few days. Nobody seemed to notice.

They bought a lot of servers and they got things up and running in a hurry. But the whole idea is, is that having two buildings side by side, or on two different floors. Or, they're both in the basement, if you have a flood coming, is not geographically diverse. Number six, standards that result in such systems being designed, developed, tested, maintained, operated, and surveilled in a manner that facilitates a successful collection, processing, and dissemination of market data.

Which means you can't have gaps. You can't say, yeah, we lost a few thousand transactions or anything that was traded from noon to one o'clock. Can we just

do a do over on that, please? It doesn't work that way. You have to design, develop, test, maintain, operate, and [00:20:00] survey or observe these things in a manner that this doesn't happen.

And lastly, you want to monitor such systems to identify potential SCI events. And the idea of identifying the event is you want to identify them real time and not retroactively. It turns out that a lot of our logs allow us to see what happened. And, you know, kind of the joke that I used to say is that the problem if all you have is logging, but you're not doing active management of your systems, is Monday morning you can sit down with your boss and say, well, hey boss, I can tell you exactly what time we went bankrupt over the weekend.

About 12:47 in the morning on Sunday is when all of our data got exfiltrated and everything got trashed. It doesn't help with resiliency, you want to find out before then that somebody's in their system screwing around and you want to kick them out early. Okay. Let's take a quick commercial break, and then we're going to get into a little bit more discussion here about, you know, so what and who cares.

So for those valuing leadership, policy and governance in tech risk and security, CPrime is here to help. Enhance your skills with our [00:21:00] training and workshops, ensuring effective policy design and strategy alignment. As a tech coaching firm, CPrime offers classes for teams and executives on security analytics and risk management.

Led by a CPrime expert, align expectations, prioritize, and map tools for robust governance across your tech portfolio. Upgrade risk management at cprime.com/train, and use the code CPRIMEPOD for 15 percent off training. That's cprime.com. Elevate your approach. Alright, so this current rule set was announced as it affected the 5th of September 2023 for reporting periods that end on or after 15th of December 2023.

So that's coming up pretty quickly. If you're quarterly or annual report, that might be your next one. And it was entitled Cybersecurity Risk Management Strategy Governance and Incident Disclosure. It's a mere 186 pages. Now, note that the rules do not [00:22:00] include all of the originally proposed elements from the March 2022 proposal, which came out, such as the requirement to disclose the board's cybersecurity expertise.

Now, this was open for public comment. They got a lot of feedback on there. And that's why this thing's 186 pages, because it's not just all rules. It's discussing about what the feedback was and things like that. But some of us felt

that this wasn't necessarily the best idea. taking away a requirement to disclose the board's cybersecurity expertise, because some companies might misinterpret that guidance to mean that cybersecurity expertise is not important at the board level.

Now when I say some companies, remember, it's some people who are saying, I don't know this. And I don't want to pay for extra because it leaves more in the bonus pool for me. So we're not going to do it. That said, it is a responsibility of the board to be able to provide governance and cybersecurity, and therefore it is going to be rather important.

Now, I, for one, thought if it remained, I might get a call from a couple of fortune 500 companies saying, Hey, G Mark, would you serve on our board? Because you've got all this background and [00:23:00] cybersecurity expertise, and you've got enough gray hair that you probably qualify. Well, anyway, many companies may have begun a gap analysis after that proposed rule that came out last year to evaluate the delta between our existing disclosure controls and procedures and what were proposed as the new SEC requirements. Now, the new requirements weren't that different than the proposal. And so that now that this rule is finalized, companies can update their analysis to go ahead and match it to what is actually there.

So if you got to jump on it doing your gap analysis, good for you. Dust it off, adjust it for the final wording, and then get to work, because this is, this is surreal. And if you did not do a GAAP analysis in preparation for it, and you are subject to this regulation, time to get hot. Get to working on this right now.

Now these rules... refer to a 2011 interpretive guidance regarding corporate disclosure obligations relating to cybersecurity. And they state, although no existing disclosure requirement [00:24:00] explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on registrants to disclose such risks and incidents.

Okay, so, in a way, saying it's not in writing, or it hasn't been in writing, is not a valid excuse, and furthermore, now it is in writing. And also, material information regarding cybersecurity risks and cyber incidents is required to be disclosed when necessary. in order to make other required disclosures in light of the circumstances under which they are made not misleading.

That's kind of a long legal sentence, but if we parse that out a little bit, the whole idea is is that you can't obfuscate issues. If your plant goes down and

stops producing devices and you want to be able to explain why it's not producing devices and it's a cyber related incident, you have to say so.

You can't just say, Oh, well, it just [00:25:00] doesn't stop working or we need to buy new equipment or whatever. So you have to disclose. material information on cybersecurity risks and incidents if they affect things. Now this ruling that we have here has been at least four years in the making because in 2019, then SEC Commissioner Robert Jackson cited an analysis that only four of 48 public companies disclosed a known cyber incident in regulatory filings the prior year.

Not too very good participation. Now granted, That 9 percent was up from 3 percent the year before, but it's really a long way from what the SEC has expected, and now what's going to be expected is, well, what? 100%. Now what's interesting is that this new rule includes a limited delay for disclosures that would pose a substantial risk to national security or public safety.

So that if you, for example, are a CISO and your organization has a national [00:26:00] security impact, and there's something that if the word gets out, you think it could cause some trouble, you might be able to not have to release this right away. Now, before you get excited about deciding that you're really important and you don't have to provide timely disclosure, note that the determination is reserved for the United States Attorney General. So that's the office you got to convince that you're super important. But there is a carve out there that would allow for 30 day delay and possibly further delays based upon its potential impact for national security. Now a couple specific definitions just so we have those in the back of our mind.

Cybersecurity incident means an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Yay, there's our CIA. Okay, that's your cyber.

[00:27:00] Security incident and cybersecurity threat means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. So if you think about a potential occurrence that may result in an unauthorized effort to affect any information that could be a very broad brush and you want to be careful with that.

I don't recall the specifics because it's been several years, but I remember starting with California Senate Bill 1386 And it was State Senator Dianne

Feinstein who proposed that many years ago which is really our first breach notification law that different states started to come up with their own language instead of just copying it and just doing a quick cut and You know, delete and replace, replace our state name with their state name and go.

Which actually would have been really nice because then we wouldn't have this patchwork of regulations. You'd have something equivalent to the [00:28:00] Uniform Commercial Code. But anyway, as I remember, it was the state of Connecticut in their first draft that basically said you had a reporting requirement to report to every single customer who is a citizen of our state, any attempt that was ever detected to access their information.

Well, take a look at your firewall logs and you'll find out that you'll cut down every single tree in Connecticut provide written notification in the next two months. It's just, it would just clear cut the entire state. And so that's not really what they're trying to say. But the thing is, is that again, as they're writing these rules and regulations, sometimes it's stuff that comes out of the Capitol Hill and the Congress isn't necessarily written by the experts.

If you think about it, your elected official is not there because of his or her expertise in necessarily a particular technical subject, but they're probably there because, well, they got a mechanism that helps them win elections. That said, it's not kind of a jaded view on it, but it's more importantly is it's the staffers who write the stuff.

And the staffers who are underpaid and overworked often rely on other people to come in and say, can I help you [00:29:00] here? Boom. How would you like a copy of this document? Off you go. And we call those people lobbyists and they could be lobbyists from the Perspective we think of that they're looking for horrible things and also they actually have a genuine interest in getting the right stuff written.

This having come through the SEC, being a number of years in the making. It's kind of the point I'm trying to get across. This is not shoot from the hip regulation. This is not something happens. And two weeks later, there's a hundred page piece of legislation. This is something that has been worked through a long process.

They've had some feedback. They've looked at it and things such as that. And they've come up with a way to say, okay, this makes best sense in what we need. Now what's the estimated impact? Now by adding item 1. 05 requiring

disclosure of material cybersecurity incidents to form 8-K. within four days following the determination of materiality.

The OMB, and then also the stock estimates, it'll take about nine hours, and they expect about 200 filings per year. [00:30:00] Okay, not too bad. Form 6-K, which adds cyber security incident to the list of information required to be furnished, nine hours of work, but maybe 20 total filings. This is not per organization, right?

We'd be in real trouble if you had to file 200 8-Ks a year. This is expected across the whole. ecosystem of publicly traded companies. So it's suggesting that that materiality is a fairly high threshold. Regulation SK item 106 requiring disclosure regarding cybersecurity risk management strategy and governance about 10 hours times 8, 292 filings.

Whoa. This tells me that if you're a consultant and you want to follow the money, You create an offering for cybersecurity risk management and strategy for public companies, instead of helping them fill out the 8K forms. I mean, specifically the summary of item 106 says that registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats and [00:31:00] describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to material effect their business strategy, results of operations or financial condition.

And that registrants must describe the board's oversight of risks from cybersecurity threats and describe management's roles in assessing and managing material risks from cybersecurity threats. Now, how does that sound to you relative to having the language redacted or pulled out of the final draft that says the boards have to have cybersecurity expertise and they have to report on it?

You see, you might not have to report on it, but you better be able to know how to do it because you have to describe the board's oversight of risk.

Now there's plenty of articles and summaries, announcements to read if you actually want to see the actual text that matters. It's in the Federal Register. It's published on the 4th of August, 2013. It's 50 pages and it begins on page 51, 896. Now, how about something more actionable? Now, the FAIR Institute has just published a document [00:32:00] called An Introduction to the FAIR Materiality Assessment Model, or FAIR-MAM, I guess we call it FAIR-MAM, in which they state...

It's a standard taxonomy and analysis model for assessing the financial materiality of cyber incidents that is legally defensible. Yay! That's a big thing there, legally defensible, as compared to, you know, Bill Murray. You know, we wrote it ourselves, sir, so to speak. Now, quoting from the document, The Fair Materiality Assessment Model, or FAIR-MAM, is an open financial loss model that enables organizations to quantify the impact of cyber incidents so they can quickly and reliably disclose legally defensible material risk on the SEC Form 8-K. All right, that's one of the requirements, and if we can fill that out, that's good. Number two, report financial risk internally to inform cybersecurity investment and management decisions for a full range of custom cyber risk scenarios.

So now it's not only helpful reporting outbound. internally as well. And number three, create a [00:33:00] timeline of the multi year life cycle of the total cost of an incident. Because if we think about it, you know, that takes a while. TJ Maxx had their, I think they were their sort of the poster child for that of figuring out the total cost of ownership of a, of a material breach.

And it came to, I think when they're finally done, maybe it was the Poneman group, I forget who, added up like $251 per record. When all was said and done. Loss of customer confidence, paying lawyers, paying technical people to fix, defending lawsuits, loss of stock price, et cetera. But within a certain period of time, the stock price was back up where it was and kept on going.

So it turns out then that if the lesson learned out of all that is that on the multi year lifecycle of a total cost of an incident gets buried in proper operation where you grow the company and you get better and better, and that interruption of the stock price then becomes sort of a, yeah, so what, who cares?

And so that's something to think about is you want to make sure people are motivated. At the board level to defend these things as compared to say, yeah, we'll just make it up or write a check [00:34:00] and get it off. We'll make the SEC go away. Now, the document we're talking about, the FAIR-MAM reports that the new SEC materiality disclosure rules require reactive and proactive actions.

The reactive actions are to disclose material aspect of a cyber incident as well as a material impact, and you have to do so within four days. And you have to disclose previously undisclosed incidents that become material in the aggregate. So the little being pecked to death by a duck at some point in time is enough there that you have to report on that.

The proactive stuff is the 10-K. Your periodic disclosures on process for cybersecurity risk management. How are you doing that? So we find that as I'm issuing, looking at my annual statement, we want to look at that. And of course you want to hide those things. I think it was Warren Buffett who said the best way to read financial statements by companies like a 10-K is to start with the footnotes.

Why? Because they're the smallest font and that's what the stuff that they got to tell you, but they don't want to tell you. So that's why it's like this big at the bottom. So start with that. That's [00:35:00] probably where the stuff will end up. Now what's needed is an architecture to build a financial materiality assessment model for cyber.

That is, of course, as we said, legally defensible. And the FAIR-MAM is an open cyber attack cost model. That's what we're looking at here. Now they compare themselves to the MITRE ATT&CK framework insofar that it's MECE. Mutually exclusive and comprehensively exhaustive. And if you remember, we heard about that when we had Sounil Yu on the show, where we're talking about his model, okay, the MECE, but the model here is comprised of 10 cost categories and has a total of 26 subcategories scattered across those 10.

So it does sort of look like, a MITRE ATT&CK framework on a diet. And, and these are selected from cyber insurance claims categories. Now, what would they be? Information Privacy, Proprietary Data Loss, Business Interruption, Cyber Extortion, Network Security, Financial Fraud, Media Content, [00:36:00] Hardware Bricking, Post Breach Security Improvements and Reputational Damage.

Okay, so not expecting you to memorize that list, but to me what seems to be missing from that list is regulatory risk, which is kind of ironic seeing as being issued to, well, address regulations. Now, if you go through that list, Privacy, Data Loss, Business Interruption, Cyber Extortion, Network Security, Financial Fraud, Media Content, Hardware Bricking, Post Breach Security Improvements, Reputational Damage, doesn't fit in any of those categories.

You know what else doesn't fit in there? Operational risk, beyond just a business interruption. I mean, what if your manufacturing processes are changed surreptitiously? Because somebody got in there and they hacked around and they had an integrity problem. Or, what if your manufacturing doesn't work? As we heard recently from Toyota, an assembly line stopped working because, well, a hard drive got full.

Now, that's granted, it's not an overt cyber attack, but it is a... Material, in my humble opinion, and it has to [00:37:00] do with cyber, and it needs a place in the model. Now, what else is missing, or what else is not there? Download a copy of it. It's not that big. It's well written. And if you hurry, they're still taking feedback until the 30th of September 2023 to say, how can we improve on that?

I mean, the bottom line is if you're directed to move out smartly and developing a plan of action for compliance with material cyber events, you now have a framework that should be defensible to those who don't think that rolling your own is sufficient. Okay, so let's summarize. Let's wrap up a little bit about what we talked about.

We covered quite a bit. Today we're looking at the whole idea of materiality. What is it that represents that threshold above which we need to do this new SEC reporting and below that, and really it has to do, it's a substantial likelihood that the fact would be viewed by a reasonable investor is having significantly altered the total mix of information made available.

That is, if it could move the needle on your stock price, it [00:38:00] is material. Pretty simply boiled down to that.

We looked at the history going back to the Securities Act of 1933, the Securities and Exchange Act of 34, the AICPA 1954 auditing procedures, and the like, and we found out that, you know, in the 1932 T. J. Hooper case, this is all rolled forward into a solid legal precedent for having to report when things go wrong. But the problem has been in the past that what? Cyber incidents didn't get called out specifically. And we found out that unless you are inside this Regulation Systems Compliance Integrity or Reg SCI for securities markets, like stock exchanges, clearing houses, things like that, people weren't reporting them.

And so the idea here is that if we have 3 percent and then 9 percent annually of publicly traded companies that are actually reporting and stuff like that, that's a call to action and that's what they've done here.

And so by being able to have [00:39:00] capacity planning, stress testing, keep your systems up and running correctly, do a regular review, continuity and disaster recovery plans.

Have some standards that show that you're doing it and then monitoring the systems, then you've got a better chance of being compliant and you don't have anything to worry about these rules. Again, this is not so much a problem that if

you report that somehow things are horrible. What we're doing here is we're basically trying to keep you from getting in regulatory trouble by not reporting.

And now, what's the best way to determine? Is it material? Should you as a security leader, as a CISO, make that determination yourself? I recommend not. That's your legal department. You've got Risk, perhaps a Chief Risk Officer. Call those folks up and say, Hey, here are the facts. Here's what it is. Is this material?

And then get that determination in writing. Because if later on, somebody externally like SEC determines that they thought it was material, And you didn't report it, and they're looking for a [00:40:00] scapegoat. And oftentimes the S in CISO is a scapegoat, scapegoat officer. You've got a little piece of paper saying, yeah, yeah, legal officer said that this is the case.

And then I'm not saying throw somebody else under the bus, but you want to keep yourself out from under the bottom of the bus. And so as a result of these new reportings, Form 8-K, we have to disclose material cybersecurity incident within four business days, a Form 6-K. Adding cybersecurity incident to the information you have to file, disclosing cybersecurity risk management and strategy and regulation SK item 106.

And also in your 10-K, your annual forms, putting that out. That's important. And we looked at one methodology. I'm sure that other organizations will come up with them, but FAIR has a excellent reputation for doing risk management and their FAIR modeling. And I taught some of that stuff before. And so the FAIR-MAM or that particular model, the FAIR-MAM, if we're going to use that for the pronunciation or materiality assessment model is a great way to go. Okay. Wow. So that's a lot of stuff for you, but [00:41:00] I think I've covered that topic fairly exhaustively. And so if you're trying to get somebody in your organization to listen to you because you think something's material and they're not listening, whether it's your legal department, whether it's your risk management or just somebody else in your organization.

Line Managers, happen to know CISO Tradecraft. Now I'm sharing this episode with them. In fact, you should be sharing these episodes with your peers, with the people that work for you to help them with their career development. And it's a way for us to go ahead and help more people. It's a way for you to develop credibility with other people because you're recommending something that hopefully we believe is world class and great.

And it allows us to continue our mission of helping to inform and educate the next generation of cybersecurity leaders. So with that, we're going to wrap it up for the week. And I thank you for your time and your attention. If you're not following us on LinkedIn, do so. Cause you get a whole lot more than podcasts.

We put out good stuff and subscribe to our YouTube channel. We're almost at that threshold where we own it, where we don't have to worry about having commercials thrown at us. So if you haven't done that before, [00:42:00] I just do that as a favor and I just go YouTube, look at YouTube at CISO Tradecraft, give us a subscribe and besides we think it's good stuff there. So this is your host, G Mark Hardy. Thank you for your time and attention. And until next time. Stay safe out there.