Bill Murphy: I want my team to get this. As my team's listening grab this TaSM as a Tasmanian devil that Ross has a branded this with and TaSM stands for Threats and Safeguard Matrix and we have a Tasmanian devil there. Cool. Let's get started. Ross, I want to welcome you to the show today.

John Ross: Thank you. I'm excited to be here Bill.

Bill Murphy: This takes on kind of an interesting theme because I have [00:00:30] Brett Johnson on a couple of weeks ago and he was the guy who founded the dark web if you can imagine. Been in jail seven times and he's on the good side of the fence now but it was just an amazing, amazing interview. It's not often that you get a chance to see behind the curtain and to really see how... And now he's doing a lot of good out in the world. That's important but I think you bring in the unique perspective I'd like you to talk to my audience about [00:01:00] as having worked for the three-letter agencies. And let me just pause there and I'll give you a chance to introduce yourself and a little bit of your background.

John Ross: Sure. My name is Ross Young. I'm currently the Chief Information Security Officer at Caterpillar Financial. It's the bank behind the large construction company. But prior to this I was a Divisional CISO at Capital One and I spent about 10 and a half years in CIA where I had a lot of great opportunities to really learn the Nation State hacking [00:01:30] side of the house. And I had a couple of other stints, The Federal Reserve and NSA. But it was just a great opportunity to learn the offensive side and then bring that into the security side. How do we build DevSecOps pipelines? How do we secure our transition to the cloud? And really how do we position what we want ceases to be for tomorrow?

Bill Murphy: That's amazing. When you say the offense side of the fence [00:02:00] I break my CIO innovation group into offense and defense innovation but sometimes that has different connotations with people. And since we're talking about the security world what does it mean to be offense oriented in security versus defense oriented?

John Ross: When you look in any IT Organization you may have a red team or a penetration testing team whose sole goal is really focused on how do I break into something? How do I find vulnerabilities [00:02:30] on a system? Offense is that in my regard... Although we'd have different objectives for the intelligence community than you would for an internal penetration testing company.

Bill Murphy: Sure. And how good are the hackers that we have at the United States on the CIA, NSA side of defence? How good are the people that they recruit?

John Ross: I think most people understand how hard it is become a Navy [00:03:00] Seal and I think you have to look at it even more competitive to get into the CIA or NSA in some of those roles. It's quite a caliber of personnel.

Bill Murphy: I would imagine. Would you consider what you learned in your experiences there put you at that type of a caliber person?

John Ross: I would hope so. I'm trying not to be too grandiose but I think what [00:03:30] you get is a place where you can see the future of technology, the future of hacking 10 years out in the future. And then hopefully you can leverage those skills and other roles and still benefit from those experiences.

Bill Murphy: And that's fantastic. It's great that you're in the commercial world now because that's a great way to leverage skills moving forward and I think this is an opportunity to talk about what you put together here [00:04:00] because it's coming through your lens into reality which is not based on some theoretical nonsense and a book out of a college but it's based on real practical experiences which I think is fantastic.

John Ross: What I've really pioneered is something called the OWASP Threat and Safeguard Matrix. And what it is, it's a simple matrix that on the top side identifies the NIST functions of [00:04:30] identify, protect, detect, respond and recover. And on the vertical side you put down the biggest threats to your company.

Bill Murphy: Can we put that as we put that up on the screen.

John Ross: Yeah. Let me share the screen-

Bill Murphy: It's fired up. This is called the OWASP Threat and Safeguard Matrix which Ross has nicknamed TaSM like the Tasmanian devil. Go ahead.

John Ross: This OWASP Threat and Safeguard [00:05:00] Matrix is really designed to help people understand what are the biggest threats and risks to the company so we can focus on that. I think anybody who has ever tried to implement NIST or ISO 27,000 just knows how much that takes. And you spend all this time and resources doing things instead of, what do I really have to protect against in my organization? And I think if you were to talk to [00:05:30] a lot of folks you would say, "Phishing is a big one, ransomware is a huge one, web application attacks and third-party or vendor data loss if you will. Now there's a number of others that you can include in and certainly it has the flexibility to add is anything that's unique to your environment. Perhaps you might have insider threat or something else but what we do from this matrix is once you list the threats how do we think of a response that is a defense [00:06:00] in depth framework?

And if you think about it, if these are the biggest threats to the company something like ransomware where we're thinking we're going to experience an eight or $10 million outage and we expect that to come every three to five years in our environment. I want to be prepared. Right? I don't just want something in a risk register that says, "Hey, we're going to work some things." I want a defense in-depth strategy, right? How am I really locking down my admin accounts? How am I using Endpoint [00:06:30] Navy to lock that down? How am I hardening macros? How do I have my SIM tools tuned against those? And how do I put a variety of defenses in place to safeguard the enterprise?

Bill Murphy: Ross,`` I love that you've just picked on ransomware. As I'm reading the horizontal from ransomware on the left all the way through so you're basically categorizing based on the identify tools, your protection [00:07:00] tools in your detect, respond and recover from left to right. Is that correct?

John Ross: That's exactly right. What I did is leverage some of the NIST framework here. The identify would be how do we know all the systems that we're worried about ransomware being on. Right? These may be your financially significant applications, your Sox applications, places where your PCI data is stored and how we have a list around those. The second thing is how do we [00:07:30] protect against those? Right? What are the active protection mechanisms? The email security tools like a proof point that are going to block malicious phishing from coming in. Any virus you're going to run that's going to block malware from running. And offline backups is another way where we could protect ourselves. And then it moves through the phases so if we couldn't stop the attack how would we detect the attack? Right? Do we have any IDs, some Intrusion Detection Tools [00:08:00] going on and it continues with respond and recover.

Bill Murphy: Now I see least privilege accounts which is super important in the web world right now. Tell me what your definition of least privileged accounts is just for the audience.

John Ross: Having administrative privileges allows you to install things that you wouldn't normally have rights to. If you can compromise a domain administrator account then you can start putting malware on [00:08:30] so many systems. Right? How do we restrict that to a small number of folks? And when folks need to install things that take administrative privileges might we have a PAM solution, a privilege access management. Something like a Beyond Trust where you could go and install something with a credential that's good for a one-time use only.

Bill Murphy: Excellent. Under the detect section you have deception technology. What in your mind [00:09:00] does that... What does that mean for my audiences deception technology?

John Ross: Deception technology is really about how do we have fake credentials that are out there that people can try to steal. Think of the honeypot systems we used to have-

Bill Murphy: Sure.

John Ross: If somebody steals this credential and tries to use it you instantly know you have someone inside your network that shouldn't be there.

**Title:**

**“Recover with Speed and Resilience from Ransomware”**

**Ross Young, CISO Caterpillar Financial**

**Post Intro Teaser:**

**How Fast Can You Recover From Malware?**

**Ross delivers security thought bombs as he discusses BIAs, DR Planning, IT Disaster Recovery Testing and Developing a threat matrix that he calls TASM.**

**Begin at red:**

Bill Murphy: Clever. Fantastic. [00:09:30] Now in the case of ransomware what's your thought pattern on... Now we're moving into respond and recover. What's your thinking pattern on the ability for how quickly your organization can recover? How do you divide Caterpillar financial systems which are quite significant? How do you break that up so that you can recover quickly and have a resiliency in your response [00:10:00] and the resiliency in getting back online?

John Ross: I think organizations need to start with something like a business impact analysis where you work through and you say, "Here's all my critical systems. How long can this be down before it causes operational impact?" Right? "Can I be down 48 hours for the system? Makes sense to me." Now let's go ahead and actually test that with the disaster recovery plan. We are going to say this machine is dead in [00:10:30] the water. You have to deploy it from scratch and you have to pull your backups from whatever system that you have and can you do a full restore exercise in less than 48 hours? Because that's what your service level agreement was with your business owners. And that allows you to have some insurity of, "Hey, it's going to suck for 48 hours." But the fact that we can respond out of ransomware and provide this without having the operational disruption of a [00:11:00] week where we can't serve as clients is a really good place to be in as an organization.

Bill Murphy: What's your lens of reality? On recovery side you have business continuity plans here. Actually on your previous comment you're saying you should have a shim BIA in here so that you actually have... You don't treat the whole enterprise as one unit but you can actually break it down into most critical systems first and with ARGO systems and the dependencies around those systems is that how you would approach it?

John Ross: [00:11:30] Consider BCP or Business Continuity Plan is a little bit different from your disaster recovery tests. Business continuity is how does the business live on if there's no IT system availability, right? Can we do things by writing them down old fashioned with paper and forms and actually doing the sales and recording and then resolve it later when the systems come back online? Right? It's kind of the fail safe if you will.

Bill Murphy: Sure.

John Ross: [00:12:00] The DR test or Disaster Recovery test are really focused on IT systems, right? If this system goes out because AWS is closed can we fail over to a different region? Can we restore from backup in this period of time? It's more periods of metrics around a IT system versus business continuity. It tends to be for non IT related functions.

**END POST**

**Kate would you take the images from roughly this time stamp on youtube and add it to the image. Make sure that it includes Ross and I’s faces/heads**

Bill Murphy: Gotcha. Perfect. I don't want to stop [00:12:30] you so keep going if you want to make some other points real relative to this.

John Ross: A couple of other key points with the Threat and Safeguard m. Matrix that I want to highlight is there's two additional ways that we're recommending folks use this. One is how do we take it into a broader approach? And so what we've done is said if you just put a column to the left of it where you could identify an organization [00:13:00] group then you can make this much bigger than just a cyber framework. And I'll give you the example. Let's say on the left side of all the threats you have certain threats come in from a legal organization. You have other threats that come in from an HR organization. Maybe the building is closed because of COVID. Maybe there's anti money laundering risks from compliance. Maybe there's some type of marketing regulations present by legal. **Now we can use one [00:13:30] framework as a risk committee to think about how we identify protect, detect, respond and recover to these threats.**

**And what this really allows us to do is create this failings of overarching shields like the Romans used to do. Think about it this way. Compliance may say, "I'm really concerned about an Anti Money Laundering." And Cyber can partner with them to say, "Here's solutions we can do to add this. And HR can say, "How do we put two man rule [00:14:00] and processes in place?" Together we're working as an effective risk committee to use these Safeguards to protect the organization. And not only that but when we can standardize on these threats we can see which ones are the biggest impact to our company and where do we want to put money behind them.** **When you have your legal and HR officers recommending money to prevent phishing that's a good place to be as a CISO.**

Bill Murphy: In this particular [00:14:30] slide here where you talked about... Metaphorically speaking like a risk committee with multi different... With many different owners. What is the actual problem that's being solved? Is this the money laundering as a general challenge? Or is it phishing as a challenge? What is the overall arching challenge here?

John Ross: I think the is how do we treat threats that are the biggest to our company in a consistent way. Right? So that when I focus on [00:15:00] doing ransomware and phishing and giving it the level of safeguards and attention it needs to the executives within the company, we can work and partner together so that legal gets their risk and cyber survives the throes. HR gets their risk. Financial officers get their risks and threats and together we're working more effectively to lower our risks within the company.

Bill Murphy: Understood.

John Ross: Another interesting [00:15:30] way that we can use the framework is within a threat model. And on the website for a loss Threat and Safeguard Matrix you'll see two diagrams. One is a data flow diagram that just shows how does card data or credit card data move through a system? And then on the right you have this Threat and Safeguard Matrix. And with these two things you can simplify how you use threat models in [00:16:00] your organization. And by using a repeatable framework like the TaSM what you're able to do is identify. "Hey, on 30 applications where we leveraged this for threat models we consistently saw we didn't have a way to detect. We didn't have really good logging and monitoring on our systems. We should prioritize this because this is where all the teams identify as having a huge threat vector." Right? And so it brings that visibility up and allows a consistent [00:16:30] and standardized way to perform threat modeling.

Bill Murphy: And Ross this is on that left, the picture which I love, that is one specific system, correct? It's just one focus system.

John Ross: This is one application and if you managed 50 applications you could have 50 of these-

Bill Murphy: Sure.

John Ross: Right?

Bill Murphy: And you can [inaudible 00:16:49] all patterns.

John Ross: And you can use this to identify patterns and trends.

Bill Murphy: A lot of new and old but certainly [00:17:00] security professionals we get lost in the details. We get lost in being able to visualize the complexity is super important. That's why I love that you've taken this and we don't need multiple slides to do this we just got one slide. And one slide talks about the system layout and then one talks about the functions and safeguards related to that.

John Ross: And it's a simple way where teams are thinking about the threats. Too often does security come to an app team saying, **"Here's what you need to do to [00:17:30] defend yourselves." And they know the app better than we do, right? They know where it's unpatched. They know where the loopholes are. Letting them lead with the threats is so much more impactful than when we let them focus.**

Bill Murphy: Good point. This gives focus to it for sure. I love it.

John Ross: And then the last thing that I really want to highlight for folks on the show is I showed how you can go from the **Threat and Safeguard Matrix to making something that [00:18:00] you can measure and monitor. Within here once you identify all the safeguards you want to implement not every one is going to be as important as another.** Right? **If you had 50 things you don't want to focus on all 50, you want to cherry pick like five things to really focus on**. And so what I did is I created a couple of items that I highlighted and then I created a basic cyber report card around those to really drive the focus. **For me it was patching vulnerabilities, secure [00:18:30] configurations, having good cyber vigilance on phishing and making sure we had things like good resilience or let's say read only backups from our financially significant applications.** Right? And as we start to think of these things here this allows us to provide metrics to risk committees, **to the CIO where they can monitor us and see how effective we're working as a CISO in driving those desired [00:19:00] compliance States.** And I think this is just so key what gets inspected becomes expected.

Bill Murphy: What gets measured gets... What is that? I'm going to try...

John Ross: Get done.

Bill Murphy: Gets done. Yes. But also what's is back... Can you go to slide 12 or 13. Try 13. Also what is super important for people watching is that you can see that Ross has a... This is an example of a very complex environment. Most businesses have built to [00:19:30] and inherited over the years but we're not saying that all of this is the most important and it's a focus with the red boxes on. I call the parade of principle the critical 20% that gets you 80% of the outcome. And it's an interesting... I don't know if it works out to actually 20% but you said focus and I love that you've leaned into the focus for security is if you try to do everything you're going to get minimal results everywhere but you're focusing the attention on the critical [00:20:00] few which I think is amazing that you've done that.

John Ross: And this is where you want to lean in on the subject matter expertise of your team. Right? If you have a system that's already 90% effective. Focusing on that system is not really a huge value add, but if you have a system that's only deployed 20% and you can take that to 80% that can be a huge opportunity to focus on. Really take the time to focus and then use [00:20:30] those as ways you can share with the CIO so that that person can bring those as a key driver of what the expectations are for the rest of the IT organization.

Bill Murphy: And just to build upon that Ross, what we find from a security organization it's something like a simple as a firewall is completely some of the most advanced technology has been built into these virtual and physical firewalls and we find them generally deployed about 22%. because deploying the advanced [00:21:00] features of those firewalls actually you've got to do some hard work. You've got to tune search. You've got to look at inbound and outbound inspection it gets in the way of users. You've got to go actually to get Help Desk involved. But deploying that system if you don't have the expertise around a fully from getting it from 20, 30, 40% up to a hundred is super important. And even something like MFA. How often do people have MFA but they don't really take advantage of conditional access and some of these [00:21:30] advanced features that you can do within MFA whether you're using Microsoft or some other tool.

John Ross: Exactly. Hopefully people get a chance to take a look at the OWASP Threat and Safeguard Matrix. We've got a cute little logo of a Tasmanian devil so you can remember TaSM. And please check it out on the OWASP website

Bill Murphy: And Ross how can people reach out to you? I'm going to put show notes to where they can hit [00:22:00] this model that you've built on on the OWASP website. And what's the best way for people to reach out to you if they have questions?

John Ross: I think the easiest way is to reach out to me on LinkedIn. You can search for me, Ross young. You'll see OWASP TaSM or CISO at Caterpillar Financial and just message me. I'd love to see if anybody's interested in and using this solution or evolving it. It's a open source framework. We're still adding to it. If you'd [00:22:30] like to be involved in the project please reach out.

Bill Murphy: Fantastic. Thank you Ross for coming on the show today.

John Ross: You're welcome. Thank you for having me.

Bill Murphy: All right. You can close down this screen [inaudible 00:22:45]

John Ross: And let me give you...