Risk in Context Podcast

Episode 40

Managing evolving cybersecurity risks

Allison Pan:

Hi, I'm Allie Pan, a senior vice president in the Emerging Risks Group at Marsh Advisory.

Welcome to *Risk in Context*, which features conversations with Marsh colleagues, risk professionals, and others, intended to help you better understand your key risks, build more effective insurance programs, and think more creatively about risk.

Cyber risk remains pervasive within most organizations. To find out why, Marsh and Microsoft partnered again — our third collaboration in four years — for our 2022 cyber risk survey, this time focusing on the state of cyber resilience today.

In this episode of *Risk in Context*, I'm joined by Jim DeMarco, director of insurance digital strategy at Microsoft, and Faizal Janif, Marsh's head of cyber advisory for Asia-Pacific. We will examine some of the findings of the report, what it means to build a resilient team, and share some best practices we learned from our survey respondents.

=====

Allison Pan:

Hi, Jim. Hi, Faizal. Thank you guys so much for joining the conversation with me today.

I do want to give you a heads up: We've got a fourth, uninvited guest. That's my 11-month-old, Tommy. So apologies in advance. She has comments about cybersecurity too. We just can't understand her yet.

Jim DeMarco:

She's very welcome. Best background noise in the world.

Allison Pan:

All right. So for our listeners, the Marsh-Microsoft survey is the third iteration in four years where we interviewed 650 cybersecurity leaders around the world, around key trends in cybersecurity, key issues that they're facing, that they have to deal with, as well as what they are experiencing in terms of activities that they're doing, best practices that they see, et cetera. All around, ultimately, cyber resilience.

I'd like to just jump right in, Jim and Faizal. Can we share with our listeners some of the top learnings that really stood out to you? Faizal, if I could start with you?

Faizal Janif:

Yeah, definitely. Thanks, Allie.

Some of the key things that really stood out was the discussion around ransomware, the discussions around supply chain. And we are looking at the skill shortage as well, and it's great to see that these are being acknowledged.

Ransomware plays a big part in what we're seeing. It's very widely covered in the media as well. But every time we are able to combat what's coming out from the cyber criminal end, they come out with a new version. So it's a constant chicken-and-egg game that we're having a lot of back and forth.

One of the other things that really stood out was the skills shortage. We're facing that throughout Asia-Pacific at all levels of cybersecurity as well, which has an impact on organizations' ability to appropriately

secure their organization, because you don't have the right skills in place.

Allison Pan:

Jim, what about you?

Jim DeMarco:

Faizal, I think you've addressed two key learnings coming out of this. I think there's two others that I might want to highlight. As we looked at the outputs of the survey, one of the key things we learned was that hygiene really, really matters, and the need to actually put protections and controls in place. There are a lot of protections and controls out there. And one of the key learnings we found was, as enterprises actually adopt those controls, they actually get not only better scores, they get better cyber footprints and they're more secure as a business.

So the tools are there. They have to be used. And I think that was one of the key learnings that came out of the survey.

I think another one that's quite interesting to call out has to do with the need to continuously monitor your systems as well. One of the key attack planes that we noted in 2021, coming into '22, with the survey, was the increasing use of supply chain as an attack vector in the cybersecurity world. And so the need to continually monitor your systems — not just at deployment, but keep them current — was a key takeaway, from not only the survey, but also from what we're seeing in the field.

Allison Pan:

I think it's so interesting that you mention supply chain, because it also brings to mind a key finding that struck me. My background is supply chain, but I'm working with procurement teams, I'm working with vendor management; not necessarily the CISO and her team.

But when you mention supply chain, the transition point would be: How do we think about the enterprise-wide approach? And the key finding that struck me was that it's an absolutely best practice to have an enterprise-wide approach. And yet, a lot of the leaders that we surveyed kind of admitted that that was a weakness in how their organizations are less resilient than they like to be.

So Jim, do you have any thoughts on why this exists? Why this is still a problem?

Jim DeMarco:

Sure, I do. And Faizal, I'd love to hear from you too on this, as a cybersecurity expert.

But one of the key things we've learned with the deployment of any technology, as we see this as being a supply chain issue and an enterprise-wide issue, is that deployment tends to be a little bit lumpy in organizations, to use the technical term. When I say lumpy, I mean it takes a while. Organizational complexity drives a great deal of challenge.

Some of the issues we face are, you don't necessarily have a centralized IT organization that has a one-size-fits-all model. And the larger and more complex that an organization becomes — like a conglomerate or somebody who has multiple business units, each with their own IT strategy, each with their own implementation plan — that gets a little bit hard to coordinate. And while we'd love, in an ideal world, for everybody to have one button to push and the result to come out, that's just not how it plays.

It plays through organizational complexity. And that means this problem is not just a technology problem; it is not just a simple cybersecurity, "oh, you've got to go do that" problem; it's much more sophisticated than that.

And so while some tools [that] may help exist, there is the ability to coordinate across systems, it's not limited just to technology itself.

Faizal Janif:

Perfect, Jim. Just to add to that. What also needs to be looked at is, depending on the type of organization you are, regulatory compliance. A lot of organizations are very heavily regulated. Therefore, some of the services that you are receiving from a third party, depending on the type of services, they need to have a level of security in place that allows you to be able to meet your regulatory compliance as well.

So then it becomes a part of that contract that you have with those organizations. And in different sectors, this becomes quite important. But as Jim pointed out, we are still seeing an uptake in maturity in that space. But it's not where it needs to be.

The second part of it is moving away from the traditional mindset. And what I mean about that is, in certain industries, from your supply chain you would order whatever you need. As technology has changed and the adoption of digitization [has grown], now, you don't need to order parts or groceries from your suppliers. It's automatically done. You're able to see what gets done through the checkout, what gets sold, and there's automatic reordering.

So what that means is, now there's a level of interconnectedness. And the human part of that has been taken out. But the mindset isn't there that [says] "well, hold on, that now poses a risk to us." So if our third-party security isn't high and it's very low and that gets breached, now that we're connected, what impact will that have on us?

So there [are] a lot of questions that still need to be answered in this space. And the maturity in organizations, they're slowly coming up, but not where it needs to be. Because technology is moving quite fast — digital adoption is moving quite fast — but we are still falling behind in this space.

Allison Pan:

Faizal, do you think that the partnership that you just described — I have to think it does, but I might be wrong, so help me out here. The partnership internally in an organization, within an organization and with vendors, what brings this to mind is ultimately your comment about regulations and how many of our partners are so heavily regulated. How much of that partnership do you think also extends to the public-private sector? Do you see that also as being critical to not just systemic cyber resilience, but can that partnership also trickle back down into resiliency for an individual organization? Do you think that that's an important area?

Faizal Janif:

Definitely. Because once we start looking at the public sector and the private sector, the private sector, in my opinion, has always been, from a cybersecurity point of view, maybe a step or two ahead of public. But what we are seeing now is there's a lot more investment in cybersecurity from the public sector. They're building out the capability; they're building out departments. In Pacific, in Australia, we now have a Minister for Cybersecurity, which we never had. And that shows the importance that the public sector is really putting on cybersecurity. And from that, there will be more requirements from the private sector as well to uplift their game, especially in organizations and businesses that possess data that could impact national security.

Allison Pan:

Jim, your role at Microsoft, I think, also lends a really interesting perspective on this question of cross-organizational partnership, public-private. Do you have any thoughts to add on to what Faizal just said?

Jim DeMarco:

Sure. I think the way we might want to talk about it is, we think of it as a team sport. That is to say, when you are combating in the area of cyber criminals and cybersecurity behavior, we have to look at it not just as a good guys versus bad guys. We are actually coordinating our efforts across multiple parties, and they have to fly in formation or act as a team.

And to that end, that team consists of a lot of different players. It's not just the enterprise and the enterprise cybersecurity organization. It is also the IT suppliers. IT suppliers can mean a number of different things. There's platform suppliers. There's cloud suppliers like Microsoft and some of our competitors. There are the people who are the software service providers in there. There's IT pros, whether those IT pros are internal or external. And then there's the people who actively fight the bad guys. We work together as a team to try to identify cyber criminals and work together to try to solve those problems. As new exploits are found, we work with each other. That's how it should be.

We also see a major role for law enforcement, for governments. Not only on the public policy front, but also in the active role of working together around protecting customers, identifying threats, and dealing with those threats. That's a combined role across a lot of different players. But the fact is, that's how it works. Done right, it means providing active protection against an active threat.

There's one other player that actually I haven't mentioned yet that's probably worth calling out here, and that's actually the role of the insurance providers themselves. Because I think here's a place where we have a couple of key factors that we need to call in. One is the role of insurance provider around identifying best practice: Here's what you should do, here's how you should think about it. That comes in everything from

the consulting that might happen from a brokerage, like Marsh, or it might be something that comes from an insurer with: Here's the list of things that actually matter to us.

And then there's also the constant updating and communicating with the customer: Here's what you should be doing — that natural signal-sharing that happens. And then the role of the insurer also has the traditional financial element to it of handling what happens when something goes wrong.

So it is a team. At different points, different players have to play different roles, but it is something we have to look at actively as a coordinated team sport.

Allison Pan:

I love that analogy, that as a team the sum is greater than even the addition of the parts, that there's additional value from that collaboration and that partnership. I really think it's interesting how you're describing the role of insurance as an industry, because it feels like there's an element of almost behavioral economics coming into play. How do we think about the incentive structure to incentivize the resilient metrics?

There's do good for the intrinsic value of good — there's always that impetus. But also, can you have incentive structures? Like, the availability of insurance given the implementation of certain controls. How does that build systemic resiliency as it gets implemented and shared across different carriers and the clients? So super interesting.

Gentlemen, I want to go back to the survey. Were there any of the findings or results that were surprising to you or that maybe have changed in importance over the years as we think about the change of the results over time?

Jim DeMarco:

I think perhaps I'll jump in here on that one, Allie. I think one of the things we've noticed is that the needles have moved over time. But in some respects, there are a lot of the same needles. If we look back to the very first survey that we put together a number of years ago, we saw that there was an issue and a concern in [the] cybersecurity world and so forth. The issue and concern has grown.

We also saw that there was a limited amount of security controls put into place. They've gotten better. Are they perfect? No. When I talked about the good guys and the bad guys, the bad guys have gotten better at what they do; the good guys have also gotten better at what they do. And so what we are seeing, I think, is a swelling of the size of the playing field and a growth of the capabilities on both sides of that equation, both good and bad. And what we're seeing now, though, is that the stakes also necessarily have increased.

If I did want to call out one thing, as those trends have moved, the importance of the coordination across supply chain is one that perhaps has moved a bit more than some of the others. Because we've seen in the field the need to actually have a coordinated view across your entire cybersecurity footprint, which means everything that you've got that's out there. That piece of understanding, where we're going after not just the traditional, easy exploits, but getting at the more narrow ways to penetrate into an organization, that means there's a need to actually have a better and further coordinated response. I think that's one of the things that we learned from the survey, is that that needle has moved maybe a bit more than some of the others.

Allison Pan:

That's reassuring.

Faizal, what are your thoughts on the state of controls and the state of cybersecurity resilience? You're the practitioner. You are the cybersecurity expert. Where do you see, in the clients that you work with, how are things moving in that space?

Faizal Janif:

As Jim pointed out, we are seeing improvements. But one of the key things to remember is, cyber isn't set and forget. So as you improve your cybersecurity posture and you implement additional controls and you improve your cyber hygiene, it doesn't mean that once you've put things in place that you're done. It's constant. You have to constantly review the controls; you have to constantly review the rules that are being written. As your organization changes and your technology changes, your cyber controls — each and every one — needs constant reviews and updates to keep them current. That's one part.

The other part that we are seeing, if you have a look at key trend #4: Adoption of more cybersecurity controls.

We are seeing organizations invest heavily in cybersecurity controls. But where we are seeing some of the shortfalls or some of the vulnerabilities that are coming up, is the implementation and the adoption within the organization of these controls.

Because cybersecurity isn't just technology. It's a business-wide approach. You've got your people and process. And all three — technology, people, and process — need to work in uniform to be able to appropriately secure your organization. So if you are implementing new cybersecurity technology which hasn't been adopted across your organization, then your vulnerability is still there, even though you have brought in new technologies to combat the threat actors that are out there.

So what we are seeing is, in some organizations, not all, it hasn't been implemented near the level it should be. And as Jim pointed out, it becomes that conversation that, if done right, then the impacts to your organization in terms of security is absolutely fantastic. You are building a lot of resiliency. But if not done right, then you have just spent a lot of money for some minor gains.

Jim DeMarco:

I'd like to jump back on something, Faizal, you said earlier, because I think it really is worth reiterating. Cyber insurance and cyber protections are more of a game of Whack-a-Mole than they are like a Ronco Rotisserie. It's not a set and forget. And one of the things that we see, the tool that we have in the insurance space, the tool that we typically have is: Let's write a policy. Well, policies are in duration for a year, and we're in this model of understanding, once a year: Oh, I've got to go do that again and get my insurance updated. That's not how cybersecurity works. It is an active risk. It is an active, bad-player risk.

And so to Faizal's point, that means we need to actually have active preventions in place. And while we are moving the needle, we're also seeing this as an excuse for the industry to also transform itself, to understand that we need to be in the active protection business as well. So from both an insurance perspective, a brokerage perspective — again, it's a team sport — the technology supplier perspective, and the customer perspective, we have to be looking at this as a continuous, ongoing not just conversation, but ongoing work together to make sure that we are continually monitoring and addressing those bad acts while we still use the facility of: Every once a year, we write a contract. And I think that's a key element to how we have to look at it. It is a cultural and business transformational shift we're seeing in the industry.

Allison Pan:

Can we end on an actionable note? Because I love what you gentlemen just said, because I think that this is how we should be. You used the words cultural transition. We're talking about the mindset shifts; we're talking about true long-term changes in organizational culture, individual culture, perhaps even national-level cultural practices when we think public-private sector.

But to close us out, can the two of you give our listeners a couple of actionable, immediate next steps you think that can get them started on this path that you're describing? Those are absolutely the long-term goals we need. What are some winnable first steps for our listeners to walk away with?

Faizal Janif:

I'll start on that. From my point of view, a couple of key things. Preparation. Make sure that you understand what you're trying to protect. Understand where your organization is headed, what is their strategy, where your business wants to be, as an example say in the next three years, the technology that's going to solution that to enable your business to get to where it needs to be. Therefore, the level of cybersecurity that's required as well. So understanding that journey would be one.

The other thing that you want to really have a look at is, what controls do you have in place? And how effective they are. The control effectiveness is very important, because a lot of the times when we do present to the board or do assessments, we're able to tick the box green that we have these controls. But how effective are they? And that vulnerability or that exposure, what does that mean to your organization?

And the last thing that I would you say is, be mindful of the next generation that's coming into the workforce, Gen Z. Because that is going to really shift the paradigm on what cybersecurity looks like. We're looking at generations that are grown up with technology, that might want to use a Facebook sign-on or a Google sign-on. A lot of these things are banned from the corporate networks, so how does cybersecurity look in that space as well?

So start to think ahead. Instead of what is now and how things were traditionally done, to more what is the next challenge that we're facing as well?

Jim DeMarco:

Those are great ones, Faizal. I'll add a couple of items from my own perspective. I think one is that you need to review where you are, constantly. I think it's worthwhile understanding, as this is a moving target, we need to be able to continuously flow not in a static way, but in a continuous monitoring way, to actually achieve our goal of keeping our businesses secure, up and running, and so on.

From that perspective, I think it's worth noting that we need to act like a coordinated team, not only with vendors. We need to stop thinking of people as vendors necessarily as much as they are business partners, when it comes to these types of things. We need to be coordinated across the organization, that the risk officer could be your friend, your quarterback for, how do we look at our business? And then that the business partners that we have, who provide us that advice, are in fact that business partner, adapting best practices along the way and understanding that if we continue to add those controls along the way, it means that we have to be able to continually evolve our business. And in our world, what we adopt, in the tech world, DevOps. That's been around for a while. We now think of it as DevSecOps. It's not just development and operations. Security is inherently in that system; that's how we have to look at it.

Last, I want to reiterate what Faizal said. We're also seeing a generational shift. As young people come into the workforce, they come in with a different set of ideas and expectations. They also come in with a tremendous amount of creativity, and that is an element that we need to look at. This is not just something we want to take the mindset of: Lock all the doors, raise the walls higher and make the moat broader. We need to think of this in a much more fluid way. And the fluid-level thinking we're seeing, coming in from people who are coming out of college today, that's a really, really strong element of how we're going to improve our footprints over time.

Allison Pan:

Such incredibly helpful advice. Thank you, gentlemen, so much for your time today.

Faizal Janif:

Thanks, Allie.

Jim DeMarco:

Thank you, Allie

Faizal Janif:

Thanks, Jim.

Jim DeMarco:

You too, Faizal.

=====

Allison Pan:

That's all for this edition of *Risk in Context*. We hope you enjoyed our discussion and thank you so much for listening.

You can rate, review, or subscribe to *Risk in Context* on Apple Podcasts or any other app you're using to listen today. You can also follow Marsh on LinkedIn, Twitter, Facebook, and YouTube.

In addition to your podcast feed, you can find more episodes of *Risk in Context* and more insights from Marsh — including the full *The State of Cyber Resilience* report — on our website, marsh.com.

Until next time, thanks again for listening.