**Cyber Risk: What You Should Know During COVID and Beyond**

**00:00 Host** Here at M&T, we understand these are unprecedented times and our goal is to provide you with insights and information that can help support you and your business. We are excited to present the latest in our webinar and content series to help you, your business and your employees manage many of the challenges you may be faced with. We're excited to discuss what you need to know about cyber risk during COVID-19 and beyond.

**00:26 Presenter** Hi, everyone, [I'll] be talking to you today about really the changes that have been wrought by COVID-19, and how your cyber risk—has really been impacted in connection in some related risk mitigation ideas you can consider. So that's really going to be the focus of my time here today. So just as to start off right, we're in now month five of COVID-19 and the kind of related impact and we're all I think collectively struggling with different aspects of it, as impacting our personal life, business and so on.

And I think it's no overstatement to say that really, business risk landscape has been completely transformed by COVID-19, right? And cyber risk, especially impacts business is really no exception. So I'm really going to highlight today's the what, the why of that and kind of give you some—we're going to burrow down into some kind of use case to the different business impacts and then some mitigation strategies for you to focus on in connection. So, I think to start off, when we think about how everyone in business perspective has been adjusting to COVID. And this is a crisis that has been just changing daily both in terms of the health impact and economic impact. And the impact in different countries, industry sectors.

**01:46** There's been favorites and has been unfortunate victims, and some sectors have been victimized pretty heavily by it like, like transportation or hospitality or others have come off, a lot better. So, there's really no clear kind of trajectory to COVID in that kind of related risk and economic impact of it. And I really think it's fair to say there's not an end in sight, through that uncertainty around treatments around vaccines, like arena, still in the first wave now we're stuck in wait, we just don't know, right? And I'm not an epidemiologist, to be able to share that with you, but I guess the point is, we're in the process of transition and change related to COVID.

Right now, businesses are going to be continually adjusting to this new reality. And so, we have to take that in mind, we talked about the impact of COVID on cyber risk and the nature of business services, business customers and what the scale and scope of that disruption is gonna look like. So from a cyber risk perspective in particular, right, we first are looking at organizations pretty much across the board that are really really rethinking and re engineering, the business practices that have been largely in place, for a long time. And that's not to imply that pre-COVID you had a static business environment, right?

**03:04** I think that especially here in the US our economy has been one of the kind of rapid transformation acceleration right in bracing new technologies in ways of sharing data, processing data, and really understanding information. So those processes were in place pre-COVID, but if anything, the reality is that that really devastating impact of COVID had made adjusting to these challenges even more acute, really as we're dealing with this crisis. So while companies deserve tons of credit, and deservedly so for all the changes they've made to the business practices, and really client needs in connection with COVID.

A lot of these changes at the same time they could result in new or really uncertain cyber risk issues, if made hastily or if made without fully implementing and thinking through the scope of cyber risk in connection. So, I guess now that a good example what I'm talking about is really the embrace of both cloud computing, and automation through remote work, right? So, for example, like the cloud can continue to bend really, like a life raft in many ways, there's so many businesses we've seen COVID did not start the transition to the cloud, right? We've seen then the major business story you would say for the last decade if not more of business transitions to and utilization of the cloud. And we've seen now post-COVID even more acceleration and dependency in the cloud for just conducting day to day services, like data storage needs, and so on.

**04:43** But, it's important to think through though the related cyber risk in connection with that because that kind of increased dependency reliance. It really does at the same time, while it enables greater business continuity and operational flexibility at the same time, you are warehousing more data in basically vendors hands.

And so that can make potentially a data breach or business interruption outage more damaging, because you have just a higher concentration of data storage and increasingly dependency on kind of that business continuity from a digitization perspective. So an example of what I'm talking about is thinking almost, from a data breach scenario, right you have a track record from 2013 on where large scale data breaches like Target like Home Depot and so on. Really showed the devastation that could be wrought by having, individual companies having their own corporate networks compromised, and having related event management and other legal liability costs in connection with the data breach.

**05:50** Now with more of that data in the hands of cloud computing companies, you have the capability and potential for, even more devastating events. Because, if one of those large cloud service providers gets compromised, the magnitude of cost could be like quadrupled if not more, because of the sheer number of companies that are using that cloud service provider, right? So just more data being concentrated in one area if things go haywire, and there's large scale incident in connection, those costs will be manifested and spread throughout more companies than they otherwise would have in a business environment where there's less utilization to cloud.

I think separately when we talk about remote work, we're also dealing with similar challenges, right? I think it's point out the obvious that if flexibility of using home tech devices and kind of work from home workstations and other ways of using VPN, other technologies to utilize your essentially to stay connected and be able to do your job at a like a full and kind at a full level has made it the remote work really lifelines many companies. But, at the same time, it's remote workers also kind of increased propensity for human error, right? Because, there's a lot of people that are working from home for the first time pre-COVID not everyone Was working from home.

**07:25** In fact, statistics kind of show across the board that less than 10% of all employees pre-COVID they're really working from home on a consistent regular basis. And so, now we're dealing with employees we're dealing with challenges, not only resolve it from working from home to the first time, then assess the blending work and childcare and personal time, right? And so you might be working from home, but you don't have the ability to give your full dedicated attention to your work the entire time, and related kind of security best practice in connection. So with that there is obviously a higher risk that the safeguards you're taking in terms of protecting your data, whether it's corporate data that

takes the sensitive business information or whether client data that you're having on your work device or on a personal device you're using for work purposes, that that data is now properly safeguarded.

**08:24** Too we have to think about the human error component of remote work as well, right. It's something separate from the onboarding implementation of remote work the first time because we have the human error piece. As companies are kind of cycling through their workforce and identifying new hires, new needs for talent, but also furloughing other workers, right. Where because of that changing dynamic of the economic impact of COVID we're using an employee knowledge, and with existing workers. And we're also increasing the possibility that this loss of tenured employees could erode employee loyalty which could then accelerate insider threat risk. By insider threat risk I'm alluding to the possibility that disgruntled internal employee, someone who either feels they're not fully appreciated or someone who's been notified that they're being let go or furloughed. Essentially takes out their frustration and seeks to really sabotage internally the company by stealing data, by sharing sensitive trade information and trade secrets, and so on. So the insider threats really a key concern and the kind of economic reality and business needs around COVID are making that a higher threat as certain employees are being let go or not utilize maybe their full capacity.

**09:45** We're also seeing on the flip side of onboarding new employees. There's a lot of really HR practices and corporate practices in terms of optimal ways of onboarding and training new employees. And despite best efforts there's just a lot more inherent challenges with remote onboarding, or with virtual only client and colleague interface. So you're not able to really hopefully plug in your employees, you're not able to fully get them up to speed on or optimally fully utilizing the suite of technological tools and capabilities at their disposal or fully understanding the ins and outs of the business through a virtual only capacity. So all those challenges are just what we have to deal with right now with this just remote work environment with COVID for the foreseeable future. I mean and then in turn just increase that human capital aspect of cyber risk.

**10:46** One other area to think about that's different from remote work capabilities and a little more similar to the cloud computing pivot that I described before is that many company in their kind of bid to stay relevant and also to optimal most beneficially serve their clients are becoming more and more dependent on e-commerce, right, in terms of ways of servicing existing clients and attracting new ones. And again, it's an accelerating trend that does, yes, company need to be doing it and they're right to be doing it to kind of increase and maintain the business operation and ability to service clients as mentioned. But at the same time, greater dependence in e-commerce is increasingly that organizational cyber risk, because theory of commerce, for example, companies are collecting more payment card data, right. They're also relying more on a digital platform to process orders, to execute orders for logistics standpoint. So that connectivity needs to be seamless, needs to be in time in order to properly process and really execute transactions. And if you have any disruption to that kind of capability, to that digital platform and ability to service your existing clients, that is in turn another challenge that from cyber's perspective could be very costly to companies if disrupted. So with these challenges in mind, it's no secret that many threat actors know of these challenges and are also taking advantage of them. So for example, there was a, I remember some statistics from this past spring at a firm on April or May where there was research done by Google where they basically witnessed increased volume of phishing attacks and malware attempts by many threat actors.

**12:34** By phishing attempts I'm referring to these really click bait schemes, where the individuals are basically induced to click on a bad link or an email that basically enables a threat actor to gain access to a corporate network in an unauthorized way that they otherwise wouldn't have access to. So essentially they're led in by the employee inadvertently by a successful phishing attack.

**13:02** I separately recall an article from late April of this year from Microsoft where their researchers noticed an uptick in ransomware attacks, right. Ransomware is a type of malware that is many times executed by basically successful phishing events or by also successful instance of compromising remote desktop protocol, RDPs. Where essentially they're able to basically take advantage of open ports that the companies have not protected by passwords or other safeguards, and are able to basically gain access to corporate networks and basically implement the malware that way. And so for malware and specifically, I think there's also a cost benefit calculation many criminals are taking into account where, if you think about it, we're already dealing with many companies across industries that are economically stressed and economically on edge by kind of the realities of COVID.

And so many of these cyber criminals are banking on the fact that these stressed companies are gonna be even more inclined to maybe pay a ransom to get back to normal, whatever normal is right now with COVID, to be honest, than they would be otherwise. So they're seeing incentivization around companies paying a ransom and getting back to where they can conduct business as usual because of those additional kind of stresses caused by COVID. So from my perspective at least, almost akin to kicking a guy while he's down, right, you're taking advantage of an already weak entity and already basically compromised company who's not basically functioning or operating at full capacity. And you are basically utilizing basically a cyber attack to induce them to pay that ransom.

**14:50** And I also know from a personal level based on my own conversations with many leading cyber insurance markets, all these threats and all these vulnerabilities, it's true that they have not maybe led to a corresponding significant uptick in claims, civilian lost, income or loss data. So even though we're dealing with a heightened threat environment, that heightened threat environment, I wanna stress, is not so far, at least as of July 2020, resulted in a correspondingly higher volume of claims. Of related financial loss that's being basically put on note as being the bigger carriers for the claims we're dealing with and other loss kind of loss claims, also lost data, business interruption loss and loss revenue, things like that.

But we're still very early on, right, and even though we've had businesses that have been dealing with the new realities of COVID the past few months, many times threat actors can embed in systems for months, even years. So it may not be clear right now at this juncture what the true threat and what the true cost of this increased threat activity is remains to be seen, maybe later this year early next to get a fuller picture of what that of what the cost of COVID-related cyber risk really looks like. So despite these challenges right whenever challenge does come opportunity. And like anything else, businesses do have opportunity now to watch and really manage cyber risks post-COVID in light of everything I've gone over. So example of this is, to go back to my first points around really that, that increased vendor lines and supply chain challenges.

**16:35** I think for many companies supply chain challenges. I think we've all dealt with this personally as we've shopped. And basically noticed that hey, certain store that products not there anymore, right? We're not getting the same volume and same kind of frequency usually is. So it's true there's been or are supply chain challenges that have been widespread, but businesses at the same time are now have

the incentivized to identify and engage alternative suppliers. So this can really limit certain aspects of contingent business interruption loss moving forward. So example, that I'm talking about before with a preset, smaller group of vendors, for example.

A business is arguably more vulnerable to certain contingent business interruption losses and by contingent business interruption loss, I'm referring to the financial loss they incur when one of their key vendors is suffers a cyber attack. So in essence, the company's bottom line is impacted by their key vendor being taken offline or being victimized by cyber attack.

**17:39** So post-COVID and given kind of the business necessity for companies to identify and basically onboard new vendors, maybe having a larger volume of potential vendors deal with less than that likelihood that a company will suffer that same degree of contingent business interruption loss. Because we'll have more other alternative vendors lined up and they can then send the process orders to deliver parts, and so on. Think another example is basically, the reality is many say companies in the pharmaceutical industry and others in terms of conducting medical research in the vaccine race, right? And there's been a lot of documentation so far by sources like the Wall Street Journal talking about how the efforts in terms of the related research for the vaccine have been compromised by nation state cyber espionage efforts. But at the same time, everyone's aware of these risks. So I think it also bears noting that this heightened risk environment around the racing vaccine is really starting to increase by necessity as well for threat information sharing, right?

**18:52** Companies are less inclined to maybe not share data, because the realizing that like hey, my key competitor, we need to conduct the same medical research activities me is taken down. I'm equally vulnerable, right? So it's prompting coming in to more optimally share information with one another around hybrid threats, and rather late activity, and also think it's worth bearing out, too, that, for companies across the board, we're dealing with these challenges of remote work on such a widespread level. It is making many companies either accelerate or think through for the first time. Am I appropriately really tearing, classifying and identifying which of my employees have access to certain pieces of critical data and who doesn't?

So in a way having everyone remote really helps to sharpen the kind of thought process around who has access to what. And so I think it's a very helpful thought process to go through for companies that by nature of restricting that certain employee access to data, you do by kind of naturally do draw down your cyber risk, because you're limiting the scope of that vulnerability as a result. So I would kind of just closing with other ways.

**20:10** In addition to this opportunity that just discussed around really what to say risk mitigation strategies around limiting some new cyber risks that then kind of heightened or accelerated by kind of COVID economic realities. The cyber insurance itself is something that companies can utilize in terms of optimally managing their cyber risk. Because it's a really essential components of any kind of broader cyber risk management strategy. It's not meant to be a replacement for more technical controls, but it's meant to really help companies manage that uncertainty. Especially in times like these to help too companies understand once the financial impact of cyber event looks like to minimize the scope of that financial impact by transferring that risk to someone else. And cyber insurance also helps to enhance overall awareness of what that risk looks like what different events could cost the company through cyber risk quantification. And if the sheer process that companies go through obtain insurance helps them really take a hard look at their existing security controls and help them identify areas for

improvement. And at the same time, cyber insurance can help them be introduced or made more broadly aware of very experienced technical individuals being an expert and others who can assist them with responding to and recovering to a wide variety cyber event.

**21:37** So I guess in a nutshell, cyber insurance really checks a lot of boxes to where not only provide that insurance risk transfer companies that have been are dealing with these these type of risks. But also gives them the kind of preparedness tools and greater insight into what they're actually risk looks like when it could cost them. And again, just to clarify the in the benefits of cyber insurance were there these were all true pre-COVID. But I also think at the same time, given that we've talked about the increase in remote work, digital dependency and just being really wide ranging scope of threats now.

**22:13** Cyber insurance can really help manage risk that it can be more complex and kind of hard to decipher than ever before. So I think just in closing, I just want to emphasize that we really believe that cybersecurity is critical and we'd highly encourage you to optimally manage this risk.