***Julia*:** **Hello and welcome to a DerivSource podcast.**

I'm Julia Schieffer, founder and editor of DerivSource.com

Cyber risk has sadly become more commonplace of late with incidents across various industries making headlines. So naturally financial institutions are getting more concerned.

In fact in DTCC's recent Systemic Risk Barometer Study respondents cited cyber security as their top concern with 80% of those surveyed rating it as their top 5 risk overall.

With me today I have Mark Clancy, Managing Director, Technology Risk Management and also Chief Information Security Officer (CISO) DTCC and CEO, Soltra. Mark is going to shed some light on cyber risk itself and explain how market participants can better protect their data, systems and organisations from cyber risk.

Welcome Mark to the podcast.

Mark: Hi Julia.

***Julia*:** **So firstly, as I've already mentioned, in the most recent study by DTCC, cyber security as a top concern among the respondents. I understand this was a rise from 2014 as well. Mark, what is the driver behind this rise in concern? Is this change really due to cyber security /cyber risk becoming more visible or are firms actually encountering real threats?**

Mark: There are a few reasons behind cyber threats being cited as the top risk: One, there is more awareness and visibility; these are incidents that are read about in the newspaper, and seen on the nightly news. They're not just happening in the back office of firms. Second is that there is a plethora of attackers that are going after infrastructures, not just trying to steal money (which is what the financial sector has been used to), but trying to express political views, respond to world events or cause other types of destruction because they have grievances against the financial sector or other parties.

The combination of all those has changed the risk profile, so it's not just monetary losses that we're concerned about.

***Julia*:** **Going back to basics here, Mark, can you tell us a little bit first about what cyber risk is exactly and how could it impact financial institutions?**

Mark: We break it down into essentially four main components:

1. Confidentiality
2. Integrity
3. Availability
4. Privacy

In the information security circle the confidentiality, integrity, availability (or CIA as we call them) have been the main factors that attackers are trying to compromise, in addition to privacy. If I'm a criminal I may be trying to steal information used for a credit card transaction, or perhaps information used for a derivatives trade; essentially, I want to exploit that information to put money in my pocket.

In most cases, criminals exploit confidentiality. Other attackers, known as 'hacktivists', are trying to express a political view, maybe they're concerned about sanctions. They're going to try to attack the availability of a system, and to do that they're going to launch a distributed denial of service attack, which knocks it off the internet so that it can't transact. We've seen that carried out against many financial institutions, retail banks, brokerage securities firms and exchanges. What they're trying to do is cause a disruption.

The other types of attacks which have been less frequent but more concerning are destructive attacks which really go after the integrity of a system to destroy the data and the underlying function. The attack against Sony Entertainment Pictures last year is an example of that. There have been attacks in the financial sector directed towards banks in South Korea. Historically we've assessed the risk to be primarily confidentiality loss, now we have the addition of denial of service attacks which impact the availability, and most recently we've seen these catastrophic attacks which impact integrity.

I also mentioned privacy in the beginning. If you can't ensure the confidentiality and integrity of data, then you can't ensure the privacy. And so there's an additional piece here which is ensuring that the data that's maintained by the institution is protected from disclosure and used for the appropriate purposes. This concerns how data is managed internally as well as preventing criminals, or hacktivists or cyber espionage actors, from taking the information and using it.

Julia: **What are some of the secondary risks (e.g. reputation damage) that a firm might encounter?**

Mark: There are a few additional risks. I think one of the more interesting dimensions is that every problem now is assumed to be a cyber attack. So if I'm running a market infrastructure on my corporate website and I have an IT problem, the very first thing that somebody is likely to Tweet about it is "*Hey, Institution X is under a cyber attack as their website is offline"*.

So the response is to assume a cyber attack first and then figure out what happened second.

There are also consequences of cyber attacks. For example, if you had data stolen that led to your customer being impacted, other customers are going to be concerned. It's very common that when you investigate an incident you do not understand its full scope. For example, the Office of Personnel Management in the US had a breach; it was widely reported in the media - they came up with a figure that it impacted hundreds of thousands of employees however a couple of weeks go by and now it's several million.

Unfortunately it's very common, because doing damage assessment in an incident response is quite difficult; it's very hard to tell what somebody stole because the impacted firm still has the copy of data that was stolen.

***Julia*:** **So looking at how to approach cyber security, Mark, do you think that the industry as a whole should be focused on addressing cyber risks? Do you think also that maybe some regulation might come out of this new concern to, for instance, require firms to introduce measures to protect themselves better?**

Mark: Yes, the industry must work co-operatively. What we've been very good at, particularly in the retail financial space, and which is now happening in the institutional market, is sharing information about what cyber attackers are doing. It is the market data of the cyber security domain. If I can tell someone what an attacker is doing, I increase the attacker's cost because they have to go out and come up with a new way to attack me, and if I can use standardization and automation as a defender, I can reduce my cost to defend.

If I'm informed about what the attackers are doing then I can be much more vigilant and agile in my response.

We've approached this as a community defense problem, because if somebody attacks one firm they'll probably use the same attack against another firm. If I'm the first victim, I'm able to tell you, as a potential victim, what to look for and how to get ahead of it. Therefore you can be much more effective at stopping it from being effective.

Regulators have also been more active by making firms aware that infrastructure operates under tight governance and 'hygiene'. Research carried out in by the Australian Signals

Directorate, looking at government intrusion found that if you do four things well you would stop 85% of the intrusions from succeeding. Those four things were:

1. Patching systems

2. Patching applications

3. Removing administrative rights, especially to workstations

4. White-listing software, so that only known, approved software is able to run on your system

If you combine that with information sharing you have a much better chance of preventing these attacks from happening. You're still going to have people who can get into your network and get through your first line of defense, but you can potentially thwart the significant impact and mitigate problems more quickly.

Regulators are encouraging firms to share information about cyber threats with their peers, which is very positive.

Julia: You mentioned those four measures. Mark, do most financial institutions already have these measures in place?

Mark: All firms face challenges. The issue is how firms respond to them. These are all measures that have been well known in the security industry for a while but firms are only really now starting to focus on them i.e. how do I get my performance and my hygiene to 99.9% as opposed to what a lot of infrastructures have, which is 70% or 80%.

The leading institutions are now focusing heavily on these measures which have become an important issue for management boards.

That said, no one is ever 100% safe, because the IT environments are so complex and there are so many moving parts. You'll have things, what I call in-flow and out-flow, so every second Tuesday of the month if you run Microsoft systems you get a new wave of issues you have to address, so there's always some backlog. The key is to have a backlog as minimized as possible, and to have the whole company focus on routine and periodic maintenance to maintain high performance. The more mature institutions have been focusing on that, but the lesser established firms don't really have the measurements in place to assess their cyber security efforts; they're not reporting to their management chain about these issues on a weekly or monthly basis.

Julia: **What are the main actions that you think financial institutions should really take on board to guard themselves against cyber risk? What are the main elements of a cyber security plan?**

Mark: A few things. Assume a breach; assume there's someone in your environment and operate your daily life like there might be somebody poking around. That change in mindset will help you. You have to then engage in what we call 'active hunting'; which is don't wait for some system or alarm to trip saying something happened, go through your environment, look at what is happening, take the knowledge you have about what attackers are doing and query your environment to ask what is going on'.

You should also recognize that you are going to have an incident that you are going to have to respond to, and that response plan needs to include both technical aspects of how you deal with an intruder in your IT infrastructure, and the business management and crisis aspect; making sure you have an incident response plan, that you've tested it and drilled it. That plan includes your general counsel, your public relations team, your regulatory relations team and your executive management. Even if you're lucky enough not to have any incidents, you should know how you're going to respond.

It sort of goes back to the military quote where 'planning is essential but plans are useless' - you want to make sure that you have that muscle-memory, and that you know how you're going to respond to an incident, so that you're not trying to figure it out at 3am in the morning over the weekend when it happens.

***Julia*:** **So we have an audience here at DerivSource of risk, operations, data and compliance professionals, Mark, what advice would you give them in terms of ensuring they take actions immediately to protect them and their data from cyber risk?**

Mark: It's very important to remember that every person in the company is a sensor. Everybody is a human detector of these attacks. Verizon published a study about breaches they investigated and the vast majority of them (91%) started with a phishing attack, where somebody sends an email to an employee and tries to get them to click on a link. That link then installs malware which then provides a foothold for the attacker to get inside a company's infrastructure.

So when you look at the operations area or the compliance team, or risk teams, these are all people who run inboxes, they get email, they deal with the outside world, they can be part of that sensor community - if you see it you report it to the security team for investigation.

Leading companies also test their entire teams by sending out messages that look like phishing attacks. An employee would click on the link and view a little training video that tells them what they did wrong and how to be more resilient to that in the future.

Firms should also look at what information they post in the public domain about the people who work for their company. This is because the criminals can harvest that information and use it to make these phishing attacks more compelling. So if they know that someone is a member of some society or professional group, they may create an email in the context of that group which may lead them to open it.

Having all of these teams engage internally and externally and consolidating the reporting of those events can help the security team be better prepared to respond to them.

***Julia*:** **Thank you Mark for sharing your insight with us today.**

If you would like to see the transcript of this podcast please see our podcasts notes page on DerivSource.com.

The podcast is also available via iTunes or the free DerivSource app.

This podcast is part of a Risk Podcast Series we are hosting this summer. So tune in every other Wednesday for more insight on risk related topics.

And if you have a risk related question or would like to suggest a topic please let us know by emailing us at Editor@derivsource.com or by commenting on the podcast notes page.

Thank you for listening. Join us next time.