Julia: **Welcome to this DerivSource podcast.**
I'm Julia Schieffer, the founder and editor of DerivSource.com

We've covered cyber security in the past on DerivSource and how financial industry should focus on preparing a response to a cyber attack as such attaches are on the rise.

In this podcast we dive a little deeper into what a cyber security plan should look like for financial institutions. With me, I have Tom Lemon, managing director and lead of the technology consulting practices in the UK at Protiviti.

Welcome to the podcast, Tom.

Tom: Thank you, Julia.

Julia: **Talking about a preparation plan, can you walk me through what a preparation plan tends to look like, and what the main elements of a plan would be?**

Tom: Sure. I would summarise it in the following way. Typically, nowadays, one of the more common ways of structuring a response plan is to think about six things. Firstly preparation, secondly identification, thirdly containment, fourthly eradication, fifth recovery, and then finally, lessons learned. Really that structure is intended to make sure that organisations that are preparing their response plans are really thinking about everything they need to do before, during and after an attack that impacts them.

Julia: **In your paper, you talk about crown jewels. Can you explain what they mean, and why they are very important in cyber security plans for financial services?**

Tom: Picking up on crown jewels, and I think this is really important when you think about what your response plan looks like, and really what your overall security protection measures look like. Fundamentally, it's all about understanding what's most important to you as a business. What are the targets that bad actors would go after? What would have the most impact if it were to happen? The way that we think about these crown jewels is by thinking about actually, what are those risk scenarios that we're most worried about, and what are the technology and/or data assets that are related to those risk scenarios?

For example, in a trading organisation, you talk to the front office, they would be very worried for example, if they lost their risk systems that gave them the ability to manage and monitor their risk and positions during the course of the trading day. If they lose those systems, then suddenly they're blind, and there's a potential huge risk for the missed opportunities or making the wrong decisions. If I'm a bad actor trying to do bad things, I might want to target those most risky systems.

Really, by understanding the crown jewels, it means that we can prioritise our security investments in the right way. We can put our strongest protection measures around those systems that are most important to the business, and around the data that's most important to the organisation as well. That goes just as much with response plans. We need to be very much focused on those risky systems, our crown jewels, when it comes to how we respond and how well rehearsed we are at those responses, because ultimately, if something goes wrong with those systems, we need to be responding quickly and effectively to limit the possibility of damage.

Julia: **Great. Tom, looking at executing a cyber security plan for prevention purposes, who's generally in charge of planning this, and also doing the execution side of this response plan? Is this role changing within financial institutions, as obviously, cyber attacks increase?**

Tom: It does vary, and it is changing I think, certainly from what we see. Typically, first things first, there should always be a team that's responsible for initiating a response. One of the common terms for that team is a cyber security incident response team, or a CSIRT. Now in organisations where it's really treated properly, those teams will have the authority to initiate a response, and to escalate where they're needed. What I've also seen is that, through the course of escalation, if something really serious does happen, there can be a crisis management team that is ready and invoked to make really important decisions if the incident is looking like it's going to have significant impact to the organisation, or at least needs to be dealt with, with that level of priority.

Those crisis management teams, once again, the chairmanship and makeup of those teams does vary, but the most important thing is that they have the right representation and the right authority to make decisions quickly. For example, I've seen the head of business continuity across a company be in that sort of chairmanship role. I've also seen chief operating officers and CSOs as well, within those roles. It's less about the person that's at the chair, it's more about the business giving that forum the authority to make quick and impactful decisions, to minimise the impact of any cyber security attacks that might happen.

Julia: Within financial institutions, as you said, it's usually a role that an existing person, like a CEO, would take on. Do you ever see a trend towards there being cyber risk experts in financial services, and people hiring these type of individuals, or is it more just individuals are obtaining the skillsets to instigate and initiate these plans?

Tom: There's absolutely a focus it, and hiring is included within that. Certainly, within financial services firms, there's been a lot of hiring activity to make sure that the capability is available in-house, to advise the executive team and the board around any cyber security protection measures that need to be taken, and responses that need to be taken if an incident impacts them.

Certainly that does happen, however, if a cyber security incident does occur and a response is invoked and initiated, it really does need decision makers across the business to be involved in that response activity. Partly because we can't think of cyber security as an isolated security or IT issue. Ultimately, it's going to impact the business if the worst happens, and therefore, that's why we need real business leaders involved in response activities, so that they can make the decisions that are necessary, and make them quickly. But also so that they can manage things like communication flows, which are really critical to make sure that people know what they can say, know what they can do, they know when they can say it and when they can do it, in order to manage a response most effectively.

Julia: We've talked about what's going on within the institutions themselves. Tom, how is the risk of cyber attacks becoming more real for financial institutions today?

Tom: Sure. I think there's a couple of things. One is the level of sophistication of the cyber attackers that are impacting financial institutions today, is increasing hugely. These are smart people. They are well run, well funded, very organised organisations, that are trying to perform these attacks. The situation nowadays is that there is money to be made from performing cyber attacks, and that is, in itself, driving a lot of organisations and individuals to perpetrate this type of crime. That's one side of it, the increasing sophistication of the attackers that we're trying to defend against.

Another side of it, which I think is very important as well, is the level of customer expectation is increasing accordingly as well. Customers are very much expecting organisations they do business with, to safeguard their data, to provide the services that they committed to provide. As a result of that, really it's, the cyber security question is one that is more and more commonly asked as customers look to do business with financial institutions. I think the combination of those two things, and the realisation and recognition internally that cyber security is a really important issue that

businesses need to focus on, is what is making it really real for financial institutions today.

Julia: **Finally Tom, what advice would you give firms looking to bolster their defences and create these response plans in 2017? Is there something in particular that they should be focusing on?**

Tom: There's a few things I would advise companies to do, and this is a lot of what we're helping our clients with at the moment. Firstly, do make sure that you understand your crown jewels, as we called them earlier. Understand and agree what you truly care about. That's what it's all about. Understand the business risk scenarios you're most worried about, and focus your defences and response plans there.

You have to start somewhere, and so focus on the things that really matter to your organisation.

Secondly, if you don't have a response plan, put one in place. There really isn't an excuse now. We need to be ready for these things to happen. We are in an age when it's a matter of when, not if. With the level of sophistication of attackers out there at the moment, if they really are minded to impact your organisation, they will find a way, and so we need to be very much ready for that.

If you do have response plans in place, make sure that you review them regularly. Reflect on whether they're sufficient across the steps that we outlined earlier in this interview, and if they're not, then do something about it quickly. As much as we can get to a place where our response plans are operating like a well oiled machine, all the better. In order to do that, not only do you need a rigorous response plan, but you also need to rehearse those response plans regularly, with all of the right stakeholders involved within your organisation, to make sure that you're ready to respond should the worst occur.

Secondly, or I should say fourthly at this point, within those response plans, do make sure that you've got sponsorship from senior leadership within the organisation. If you don't, then it's really critical that you make sure that that does happen. Ultimately, as an organisation, you need to have a team that is able to make decisions quickly when it comes to responding to cyber security incidents, should they occur.

Then finally I would say, just also make sure that within your response plans, you have quite well thought out communication protocols. I do see, very commonly, when cyber incidents occur within financial institutions, a breakdown of communications, as people aren't quite sure what they can

say, whether it's internally to other parts of the business, or externally to customers or even regulators, and when they can say it. It's really important that those protocols are established so that if and when something does occur, as I said previously, you can manage the message effectively, at the right time and with the right parties.

I would say that those organisations that respond well to cyber security incidents, really do stand above those organisations that don't. There's been some research that has been done over the years, and even customers and other parties that rely on financial institutions, do say that they look a lot more favourably on organisations that can respond decisively and effectively, should the worst occur. I think, really that's why incident response plans and their level of depth and their level of "testedness", it really is important and can make a big difference to your organisations.

Julia: **That's great advice to leave our audience with. Thank you for joining us and sharing your expertise.**

Listeners - you can find more on this topic in a recently reported DerivSource article on cyber risk and related links on the show notes page.

Thank you for listening. Join us next time.