SLAUGHTER AND MAY/

Managing Cyber Supply Chain Risk
Digital Horizon Scanning Podcast
November 2025

Natalie	Hello and welcome to our latest cyber podcast, which is part of our Digital Horizon Scanning series. My name is Natalie Donovan and I'm a counsel knowledge lawyer at Slaughter and May. In this episode, Richard Jeens, Head of our Cyber Hub, discusses supply chain risks with partner Laura Houston and associate Alex Buchanan. This is a fast moving area, and since the podcast was recorded, we've seen the ICO fine Capita for its supply chain breach and the government write to the chief execs and chairs of Britain's leading businesses, urging them to protect their businesses from cyber-attacks and manage their supply chain risk. So, a very timely episode, which I hope you enjoy.
Richard	All too frequently when we're called upon about cyber or data incident, it's not our client who has been directly impacted, but rather one of their suppliers. In some respects, that's entirely predictable as the expansion of digital estates and digital business arrangements means there are just more potential entry points for attackers, or some kind of social engineering to get at the humans. Indeed, a recent Argon security review found supply chain attacks grew by over three hundred percent in the last year or so, and a survey conducted in September by the Chartered Institute of Procurement and Supply revealed that almost a third of managers reported companies in their supply chains had been attacked in recent months. I'm therefore delighted to be joined today by Laura Houston, a partner in our digital and outsourcing team and a key member of our Cyber Hub, and Alex Buchanan, one of our specialist cyber and privacy associates. So, Laura, tell us a bit more about supply chain cyber incidents and why threat actors choose to go after suppliers rather than targeting customer organisations directly?
Laura	Yeah, maybe we should start with a quick refresher on what we mean by supply chain breaches. So as you mentioned, Richard, we're talking here about a scenario where a cyber attacker targets an organisation indirectly by compromising one of its suppliers who has access to its systems. So forgive the noddy example, but I like to explain it by analogy to robbing a bank. So rather than breaking into the vault and having to scale the walls and circumvent the bank's robust security arrangements aimed at thwarting intruders, the criminal instead steals the keys from the nighttime cleaning company, who may have left them lying around and gains access to the bank that way. That is likely to be easier, cheaper and probably quicker for the threat actor. And when we think about the strategy behind these attacks, we see different approaches being taken by the attackers. So sometimes we see them going for the big managed service provider. Now those providers may actually have very sophisticated security arrangements, but they hold the keys to lots of different organisations, so the challenge is worth the prize for the attackers. Other times you see threat actors targeting smaller providers who might not provide access to such a broad pool of customers, but who are less sophisticated, and they're targeting because they are the weak link in the chain and so

	attacking them provides a route for threat actors into much more heavily fortified organizations. And we've seen this happening time and time again in the headlines with the likes of the Capita breach from a couple of years ago, when Capita suffered a ransomware attack and sensitive customer information was leaked. We've also seen it in the Advanced breach where a healthcare software provider again suffered a ransomware attack, and that brought various NHS services to a halt. And likewise with the likes of the MOVEit vulnerability, which again triggered a wave of cyber-attacks.
Richard	Yeah, it's interesting you say that and obviously there's been much reporting around the M&S breach and others more recently, and the Synnovis one affecting the NHS trusts, um, supply chains clearly matter. But but what is it about these sorts of incidents that makes them so difficult for, for people to manage?
Laura	Yeah. So, I think there's a range of factors at play here. On one hand, they're often harder to identify, so they are often outside an organization's direct line of sight. Often, a customer can't see what's happening in its supplier's network, and the issue originates in systems that a customer won't directly control or indeed monitor. And so, it can hide undetected for extended periods of time. So that can make things more difficult. Also inevitably harder to prevent. Of course, diligence is important exercising audit rights. But ultimately this is about the defenses of third-party organization and not a client's own defenses. Again, that's difficult. And ultimately, when this happens, the organization is one step removed from the centre of action. So it's left relying on information from the supplier and how quickly and effectively they respond. So, for example, a customer is unlikely to be the one making the decision about whether to pay a ransom. And that's amplified by the fact that they can have a sort of multiplier effect, where one breach may impact hundreds of thousands of organizations all at once. And then from a legal perspective, we have the sort of blurring of the line of responsibility. I'm sure, as we'll come on to talk about, customers may still be accountable, even if it is third party defenses that have failed. And that can bring with it these sort of complex questions of liability.
Richard	So it's like a complicated game of Jenga. You never quite know who you're relying on and how it fits together. Um, so how a business is supposed to think about it is, is it just looking up the supply chain to see who you're most reliant upon?
Laura	Yes. And when we think about cyber and supply chain risk, that is absolutely our key focus is the inbound risk. So the risk of a supplier breach impacting client systems. So as you say be careful who you trust. But there's also the risk of how a customer cyber incident might affect its supply chain. So the outbound risk. And we've seen this in the widely publicized Jaguar Land Rover cyber attack, highlighting this outbound risk that a cyber attack poses to supply chains. So there JLR, subject to a cyber attack, has had to shut down its production. But that shutdown has directly impacted those in its supply chain, particularly some of the smaller suppliers who are reportedly at risk of bankruptcy. This clearly has an impact not only on those suppliers, but has a knock on impact back

	upstream to JLR's ability to restart production. And here the UK Government has stepped in with support. But of course this will not be the case for all organisations.
Richard	Right. So it's like Jenga, you're stuck in the middle and there can be debilitating consequences at the top of the tower and the bottom of the tower. Um, Alex, I suppose just just turning more to sort of regulatory and privacy side of things in what we're calling a supply chain breach. Is this different to a traditional controller breach? How do regulators tend to view this and what are the key legal concerns at play?
Alex	Well, it is different to a traditional controller breach. In our experience, data protection authorities like the ICO will still focus on whether the controller has exercised sufficient oversight over the suppliers handling of personal data. So when you use third parties or IT service providers to process personal data on your behalf, you should be satisfied that they have appropriate security and are complying with DP laws that you have some sort of assurance, usually via a contract. This all go towards that controllers accountability obligations and their proper management of third party relationships. Rights under contract serve as tools for oversight and mechanisms to support the controllers own accountability obligations under DP law by exercising their rights to request information and conduct compliance checks, the controller is able to monitor and evaluate the supplier's performance, ensure appropriate safeguards are in place, and respond effectively to regulatory inquiries. This also enables the controller to obtain clearer understanding of the processors current position, including any remedial actions taken since the breach, and to demonstrate that appropriate steps are being taken to manage and mitigate ongoing risk. The ICO expects evidence that these controls are effectively monitored, regularly reviewed and updated as needed to remain effective. So in this context, accountability does require a proactive and structured approach to compliance supported by clear governance, internal oversight, and traceable actions. Clear records here are key showing decisions are made and demonstrating accountability.
Richard	Thanks, Alex. I mean, that obviously fits with what we're seeing in a lot of the enforcement actions we're working on at the moment where the ICO or other regulators are demanding the documents and being, frankly, pretty disappointed when they can't be produced on a ready basis. Um, thinking, of course, in practice, how many organisations will be using suppliers and those suppliers will have their own suppliers? How far up and down does this sort of supply chain diligence and record keeping really have to go?
Alex	Well, common market practice is for organisations to only be aware of and conduct diligence on their first line of suppliers, but under certain regulatory guidance this is just not enough. So in the EU, EDPB guidance arguably rather unrealistically says that controllers should exercise DD in their selection of an oversight of all processes throughout the processing chain, no matter how long or complex that chain of processing is. The NIS2 directive similarly requires organizations to adopt a comprehensive risk

	management strategy for their entire supply chain, involving risk assessment, the implementation of security measures, continuous monitoring, and supplier accountability. Accompanying ENISA guidance sets out the DD on a list of all suppliers should be undertaken. But interestingly, where this is not possible, the identification of those suppliers that are responsible for products and services with security enforcing functions, the suppliers that have privileged access, or the suppliers that handle particularly sensitive data are the suppliers that should be prioritized in that diligence. This seems to take practice inspiration from the UK Cabinet Office's supplier assurance framework. In the UK, while there is no specific ICO guidance on how far down the supply chain organisations diligence should go, NCSC guidance recommends prioritising your organization's crown jewels, i.e. determining the most critical of a list of tiered supplier security profiles, which each represent an increased scale of impact. Now, the NCSC acknowledges that you may have to rely on your immediate suppliers and subcontractors to provide information about their subcontractors, and it may take some time to ascertain the full extent of your supply chain. Controllers will then need to determine whether or not their suppliers and subcontractors have provided the security requirements asked of them. Understand what access your suppliers have to your information and how you will control it, and understand how your immediate suppliers control access to and use of your information by any subcontractors they employ. Of course, it's important not to forget corporate governance code provision twenty nine, which is that we know boards of listed companies are expected to monitor and review the effectiveness of the company's risk management frameworks. And cyber is, of course, one of those risks. Therefore, there needs to be consideration of reasonableness, cost benefit analysis and about appropriate risk of the framework in place. The board should be holding the CISO to account re how far down the supply chain their diligence should go. So to resolve this tension between regulatory expectations and practical reality, organisations need to come up with a sensible policy in terms of how to target their resource, particularly focusing on key suppliers that may present the greatest risk.
Richard	Blimey, that's an awful lot for organisations to get through. Thanks, Alex. Um, I guess in practice then, um, what sort of provisions Laura, do we need to have in place to enable organisations to meet at least some of that shopping list of regulatory requirements?
Laura	Yeah. So it is a fair question. What can anyone actually do about any of this? I think there are sort of contractual points to consider, both from a prevention perspective, but also then if the worst happens from a sort of crisis management perspective. So I guess first up, mitigate the risk of the attack happening in the first place, or at least provide contractual recourse if it does, by imposing information security obligations on your on your counterparty. Now, I think it's important to say that this should apply to all

	information that a supplier holds on a client's behalf, and not just personal data. So we do still see security provisions that are scoped by reference to personal data exclusively, and that may well be too narrow. So imposing baseline security standards that might be by reference to specified standards, and then supporting that with obligations to maintain, to test and to report on those controls. Next up, I think it's important to ensure that the contract provides you, the customer, with a right to audit and assess those security controls rather than having to take the supplier's word for it throughout the duration of the contract. And that's particularly important in lengthier sort of longer term contracts. Depending on leverage, it might not be a full annual audit. It might instead be a right to ask questions. It might be a right to request reports or to see evidence of particular practices. Of course, the diligence at the outset of a relationship is absolutely critical, but it is important that you have this sort of self-help remedy of getting in and refreshing that during the term, because ultimately suppliers need to be treated like a shared risk surface alongside an organization's own cyber posture and not a separate one. And then pivoting to incident management. I guess here contracts should enshrine and enable cooperation and access to relevant information. If we do find ourselves in crisis scenarios. So robust incident notification regime again ensuring that that isn't only triggered by personal data incidents, but that then needs to be supported by ongoing information provision obligations. So you want information at the outset. You want a first report but then ongoing updates as the picture becomes clearer. It is worth here, bearing in mind that when there is a supply chain breach, as we mentioned before, it's likely that that breach might affect multiple customer organisations of your suppliers. So suppliers will be fielding calls from a whole host of customers, and you don't want to find yourself at the back of that queue. So again, depending on leverage, one way to address that issue is to consider including a teller's first obligation or a sort of most favoured nation regime, so that you are treated as a key customer in a large supply chain attack, and you are at the front, or at least towards the front of the queue if if the worst happens. One practice point that we have seen when advising on incidents. Some suppliers delaying the provision of information on incidents until a further separate NDA has been negotiated and entered into. Now to avoid having a standoff over the terms of NDA, when everyone really should be focusing their efforts elsewhere. We would suggest that a contract expressly deals with confidentiality around information provision as part of an incident and sets out, for example, that the confidentiality regime will apply to that information in the event of an attack. And then finally, when all is said and done and you're out the other side, think about what the contract says about post-incident action. So whether that's a regime around root cause or some sort of remediation report. What caused the incident? How has it been resolved? What steps are being taken to avoid recurrence? A customer shouldn't be left relying on sort of trust us, it's fixed. It won't happen again. Type reassurances and should be involved directly in understanding what what steps have been taken and indeed what mitigating actions prevent future future occurrence of the same issue.
Richard	So quite a lot to do there. Um, difficult enough when you've got a direct contractual relationship, presumably some ongoing commercial leverage

	as you, as you rightly raise. Um, how does this work out, actually, with your previous suppliers, you know, if they've hung on to your data, if they've not got rid of it or, you know, but you clearly need to help manage that risk.
Laura	Yeah. It's a it's a very good point. And it's one that came up in relation to the Capita breach, I think, to plan for this eventuality. Ideally, each of those contractual terms that we've just described in relation to security and relation to incident response notification. Those need to be drafted so that they survive termination or expiry of the contract for so long as the supplier still holds the data. So that should include all of the clauses that relate to audit rights, data security, data retention, deletion, including data subject rights and cooperation and information provisions. All of that good stuff really needs to survive for so long as there is any scenario in which that supplier continues to hold your data.
Richard	Wow. Okay, so Alex, coming back to you again here, there's obviously quite a range of notification obligations that exist under the relevant regimes. Um, and comms is obviously such a critical part of handling any incident. How does the fact that a breach doesn't necessarily originate within the organisation, and it's hard enough to know what's going on in those circumstances. But really flows from a supplier. How does that affect the obligations and broader communications strategy?
Alex	Well, in short, it usually makes it much tougher. Obviously under the EU and UK GDPR, if the breach is likely to result in a high risk to the rights and freedoms of individuals, and an organisation must inform those concerned directly and without undue delay. As the standard is high risk, the hurdle for informing individuals is higher than it is for notifying the ICO and other DPAs, so there is a need to assess the severity of the potential and actual impact for individuals, as well as the likelihood of this impact occurring. In our experience, regulators like the ICO will want to see the assessment as to which individuals are at high risk has been undertaken, and that comms have been sent to those individuals to put them on notice of the risk and setting out steps for them to keep their data secure. As mitigation for that risk, the regulator may penalise an organisation who has not done so or has delayed in doing so. Now, depending on the proximity and efficiency of your supplier, you may not be notified of the breach or may not be notified until many months later. And even if you are told and do your ongoing diligence, you may not necessarily be able to decide whether or how to notify data subjects. Therefore, in practice, you may need to notify either the earliest point, i.e. without undue delay from the point of awareness, or in a piecemeal fashion as information becomes available to you. It's always worth keeping an eye on the approach of any other organizations who also use the same supplier. Of course, it's important not to cast the net wider than necessary by notifying more individuals of the breach than those to whom high risk is posed, or to overstate the impact and or risk of the breach. The data subjects which may result in greater anxiety and possible reputational risk.
Richard	Thank you. Thank you both. There's clearly a lot to work through there. I suppose just to wrap up a few points to think about here. First, the

	regulatory regime is tough, has different standards, but from taking a commercial approach, the first thing is to think about what are the crown jewels, what really matters to your business and where does your risk relate? Think about that risk. Upstream and downstream you rely on people, but you don't want to have customers that you can't sell to. If you suffer an incident, think about cyber resilience as a core part of your procurement and contracting process. Is it worthwhile building in some redundancy? Can you mitigate and manage your risk in your contracting process? Think about how you engage. Who's going to talk to whom, when? How are you going to keep them informed? Build up trust so that they talk to you. And finally, given the regulatory challenges and oversight here, make sure you can demonstrate the accountability and the practical steps you've taken, have key documents, DPIA, contracts, etc., that you can get out of a drawer and show to the regulatory authorities when asked quickly.
Natalie	Thank you for listening. If you're interested in receiving more cyber, tech or digital content, you can subscribe to our blog, The Lens. Our Data Privacy newsletter and our Digital Horizon scanning series. Please also feel free to get in touch to discuss any of the issues raised in this episode.