HL INFLUENCERS: DIGITAL TRANSFORMATION

TRANSCRIPT

JOKE BODEWITS
PAUL OTTO

Leo von Gerlach	Hello everybody and welcome to another edition of *The Influencers*, our podcast conversation on Digital Transformation and Law. I'm Leo von Gerlach, and with me today are my Hogan Lovells partners, Joke Bodewits and Paul Otto. Joke and Paul are our top AI and data law experts, Joke in Amsterdam and Paul in Washington DC. Today, we want to speak about the hottest topic of their respective practices, and that's clearly about cyber-attack management in times of AI. With that, Joke, Paul, welcome to the show.
Joke Bodewits	It's great to be here Leo. Thank you.
Paul Otto	Yes, likewise. Delighted to be here.
Leo von Gerlach	Paul, let's jump right into your practice. Give us a sense of how AI is reshaping cyber-attack and cyber defence playbook. So both sides of the equation?
Paul Otto	Absolutely and let's start with the positive on the defence side. We're seeing a lot of new and exciting tools, platforms, technologies emerging that are leveraging artificial intelligence technologies and capabilities to support defending against all these cyber-attacks and attempted intrusions. One of the biggest problems in cybersecurity is simply the volume and so identifying what's real, what are actual signs of an attack, and honing in on that versus all of the noise, all of the activity that's happening within a network and on various systems that are false positives or appear anomalous at first glance, that's always been difficult and only getting more difficult. And so, AI type solutions are increasingly helping companies and organizations hone in on and identify better the patterns of actually malicious activity and identifying across the network, aggregating activity and honing in on what attackers are doing, helping defenders to more quickly respond. Unfortunately, AI tools and technologies are not only available to the good guys and so we see bad actors around the world also seizing upon these technologies. Also in a volume sense, problematic.

	First and foremost, the sheer ability of using AI tools to more quickly and more numerously attack companies more effectively, things as simple as feeding in the idea of different messages and appearing more to be an English speaker for phishing and other e-mail messages to be more convincing to would-be victims that they should click on a link or interact with a seemingly legitimate e-mail or bad actor, that's gotten easier. An d then, really problematic and difficult, Joke and I, and our global team have seen is simply the use of AI to imitate and simulate actual people, the kinds of deepfake or other similar technologies that very convincingly bring on someone onto a live video call even and seeming like it's your boss or it's your CEO telling you what to do or giving you authority to take certain actions where only after the fact do you come to realize that wasn't who you thought it was on the meeting or in that communication, that attackers instead were able to get enough insight to emulate real people and convince and deceive people to take actions or to give them access. Those attacks have been significantly on the rise.
Leo von Gerlach	Very interesting. So perhaps shifting the focus to the European Union and zooming in on the topic and the practicalities. Joke, I mean, speaking about the sectors most affected and the strategies most typically applied with a view to AI, just your views on that?
Joke Bodewits	Yeah, I would say there is no single industry that is under scrutiny from my experience. It is really industry agnostic. I see companies in the tech industry, but I see equally companies in the consumer, travel and entertainment industry. Obviously, automotive is a company under scrutiny from cyber-attacks heavily but also the industrial industry and medical devices. So, it is very industry agnostic and within those industries, I think there is a trend similar to what Paul already identified. And other social engineering, and other phishing incidents are all much more sophisticated than a few years ago.
Leo von Gerlach	So, we have a phenomenon that really applies to all industries and all they need to be at the watch out and with that, let's dive a little bit into the legal side of things, Paul and the teams that have to deal with that and specifically the legal teams. What main rail guards, would they need to observe to do it just right?
Paul Otto	In one sense, AI is a variation on a theme of the last 15 years, challenging legal teams to keep up with technology and understand the implications of new and evolving technology. And so, to that end, what I mean is, in part, where AI is a component either of the attacker's methodology or of the systems and data that was impacted, it's very important for the legal team to work with their technology, information security, engineering and other teams to understand what that means. And in particular, we see attackers interested in going after, where companies are using AI because they see that those platforms might be a source of rich data sets to target. And so that may trigger the same types of reporting obligations that we've always

	been concerned about in the US, the mix of whether personal data has been impacted or other regulated or sensitive information subject to reporting obligations, public companies with their reporting obligations, with the twist really being regulators generally in the US and worldwide are quite interested when AI is implicated in an attack and they may have a host of additional questions, including if it is affecting an AI tool or technology that company was using, how were you using that tool? and raise a host of questions around whether that was an appropriate use, somewhat unrelated to the attack even. So, in a sense, we're focused on the same core concerns that we have been and the challenge for legal teams is keeping up, that technology is shifting so rapidly and the way that attacks are happening and the way companies are using AI is shifting so rapidly.
Leo von Gerlach	That makes a lot of sense to remain adaptive and then to be very good organized in cross-team workflows and the interoperability of data across team, the whole organization. So that's all internal looking but there's of course also the external side, the requirements for notification under the, let's say, General Data Protection Regulation or NIS2 or even some more specific, industry specific regimes like DORA for the financial industry in the European Union. So Joke, with that, how does this whole big space of notification comes upon the organization that have to deal with it in very short time and under significant pressure?
Joke Bodewits	Now, this is a very good question, Leo. I think first and foremost, companies should consider that cyber is a legal issue, both in readiness and response. There is considerations that should be given to technical, organizational and legal questions. So then diving into those legal questions, that is much more legal obligations and higher expectations from regulators, but also legislators nowadays. And that is not only due to the new legislation. It is also due to the fact that cyber is a real threat facing companies for years now, and regulators, business partners, insurance companies, and other stakeholders require a much more sophisticated level of compliance from companies, but also cyber resilience. So looking at those pieces of legislation that you just highlighted, such as NIS2 and DORA, they come up with stricter notification deadlines. So basically putting companies under much more stress when they identify an incident because they need to act so quickly. We no longer have those 72 hours that now feel almost comfortable from a GDPR perspective, but need to act much more quickly. So what we do, we work together with those companies to identify what they need to do and how they need to do that in a way that still meets regulatory expectations, but also work for the business teams. And in order to do that, you need to know the regulators. You need to know what they expect from a company in a certain industry sector and translate that to a reality that you have in cyber incidents. And this is very important because what we see in the aftermath of the cyber events, regulators are much more active nowadays. They have many more questions. They reach out with

	questions for information, policies, decision-making, due diligence that companies have conducted during the incident response. So knowing what you need to do, when you need to do it, and how you need to do it is much more important now than a few years ago.
Leo von Gerlach	That's interesting. So building and maintaining a very good relationship with the regulator to be ready when disaster strikes, I think, yeah, that's a good piece of advice to drive this even a little bit further with one follow up. Is it possible to say, if there's one thing you should do just right in the very first hours, that's the one you should really double down on, or would that be an oversimplification?
Joke Bodewits	It's not an oversimplification. It's a very good question, but it's a difficult question to answer. I think from a technical perspective, companies should start immediate internal investigations and start to consider which measures they can implement for remediation. From a legal perspective, what companies should be doing is making sure that they identify their legal obligations, preferably before they have the incident, but at least immediately following the incident. So, you need to know what you need to do. To identify what you need to do, you do not only need to look at what is in the law, but also what is in your contracts. So, what does your insurance company expect you to do or the important business partners? But you should also look at the regulatory expectations that maybe come on top of legal requirements, because maintaining a good relationship with the regulator is very important. Then in addition to that, especially if you're subject to NIS2 or DORA, it is very important to also consider the involvement of your management body and your boards. These bodies have an important role to play in incident response and in keeping the entire cyber resilience posture of the company compliant with these obligations, which brings that in the first, I would say 24 hours after an incident, you also need to manage those stakeholders, bring them up to speed and guide them through the process in a way that they can be successful in their role and meet regulatory expectations.
Leo von Gerlach	Thank you. I have taken notes while listening to your very, very good playbook, Joke. Perfect. With that, let's shift the focus yet again a little bit further. Most of our clients operate on a multinational or on a global basis. And then there is the problem of moving data, moving logs across borders through different legal regimes. Paul, give us your take on that obvious challenge.
Paul Otto	So, it's a big topic. And I will borrow, as Joke emphasized a moment ago, the benefit of doing this in advance before an incident, before a response, to know where are the support teams, the centres of excellence, that are involved in cybersecurity incident response, that would be managing that kind of data, logs, indicators of compromise, needing access to systems and applications to better understand what happened and planning in advance. Where are they located? Do we have the right structures and permissions in place? Are there limitations including on the third-party

	vendors that we use for incident response? Do we have teams that can meet localization requirements if and where needed? Can they operate in only within certain jurisdictions or operate on data only housed in certain regions? This is an ongoing challenge, one that's, I won't say easily solved, but certainly when Joke and I spend a lot of time advising in advance of incidents to make sure there's a plan and a strategy and approach to do so. And to think through, in particular, if there's going to be external data sharing, one of the most common issues we run into is with law enforcement. Companies increasingly see value in cooperating with law enforcement, perhaps in multiple jurisdictions, and there remains the same concerns that have been in place for 20 years. What does it mean for a company headquartered in one country to be sharing information that might contain certain sensitive personal data, other information in it with law enforcement or government authorities in a different country? So knowing in advance who makes those decisions, what are the frameworks or procedures for approval and confirmatory review makes it a lot easier in the crisis phase of an incident to not be sitting around waiting for days for things to clear or setting up a new structure that wasn't already in place.
Leo von Gerlach	Given the complexity of this challenge with so many different regulatory regimes in place, so many data, so many stakeholders, are there any technology tools, reg tag, legal tag tools around that make this specific task easier?
Paul Otto	It is an area of a lot of innovation. I think what I've seen, and Joke and others are advising on this regularly as well, is a real emphasis on the kinds of tools that help companies understand more quickly their data landscape internally and their contractual landscape. For a lot of our clients, an incident may impact contractual limitations or restrictions on how they operate or who they share data with or information. So rostering those contractual provisions is still one of the hardest challenges we see companies working through to get their arms around and legal tech and advances in tools and technologies that more automate and pull and aggregate that information and don't rely on the manual input of relevant contract provisions and maintaining that manual database. Those are really helping our clients out significantly to be more quick and nimble in addressing the mix of contractual obligations and limitations and also knowing what they need to do in terms of data management.
Leo von Gerlach	Very good advice. Perhaps now move to the back end of the process. At some point, organization needs to ask the question, are they ready to make a ransomware payment yes or no? And that's obviously a question that just then triggers a lot of different considerations, but there are also legal considerations to that question. So Joke, what are the things that we should keep in mind from the legal side when it comes to making payments, yes or no?
Joke Bodewits	This is a question that we get a lot from our clients that actually go through a ransomware scenario. Let me start by saying that luckily, not all cyber

	events actually result in ransomware. So, we still have a lot of companies that, well, good for them, do not have to through this discussion. But if you encounter a ransomware scenario, it's important to consider that paying a ransom in itself is generally not illegal under EU laws. But you need to consider what the consequence of paying a ransom might entail. And that could have a consideration from a sanction perspective or potentially paying money to people that are on terrorism list. So, organizations should always consider, and I would suggest seek legal advice, on whether or not they are allowed to make a payment in this specific instance. There is a lot of companies that provide support in that regard to help you understand the better profile of the threat actor and also help you to identify where you potentially make your transfer of money to. Knowing that and then giving legal advice on that, will help you to identify whether or not your payment is legal. And if you translate that to regulatory expectations in that regard, it is important to consider that most regulators will consider a ransomware payment a confirmation that a breach has occurred and that you will need to notify regulators of the fact that the breach has occurred. Not all regulators ask you for details about ransomware payments, but some regulators do. And if regulators ask you that question, they tend to also ask you questions about the decision making about whether or not to pay that ransom. That could be asking questions about who was involved within the internal organization, but equally, what was the due diligence that you did to come to the conclusion that the payment is legal. So, there's a lot that you need to consider in that initial analysis of whether or not to make that payment and how you do that and how you document that is something that you should carefully consider.
Leo von Gerlach	Definitely a tough call to make and probably a call to make for the C-suite and something on board level and just staying there for a while, on board level, general risk management, Paul, I mean, aside from the incident situation in the general stream of risk management by any good governed organization? What would be the, let's say, two or three checklist points that every board should have on top of their mind when it comes to the general organization of cyber-attack preparedness?
Paul Otto	The first and starting point almost always on cyber preparedness and resilience is simply, have we tested? So, for a board level conversation, I would be encouraging the board to have that conversation with their leads on information security, legal, and others. Have we run through the kinds of preparedness exercises internally and with appropriate third-party support to test and simulate different attack patterns and understand at both the technical and management level, how we would respond? So, we, of course, have, we want to see in Disha that there is a documented plan, playbook, and program for incident response, but importantly, is it being tested? It's not doing anyone any good service just sitting on a shelf. It needs to be run through, and boards need to know, and we advise boards regularly to be aware how frequently are we testing and simulating these kinds of incidents and attacks and running relevant response teams through exercises and tests and simulations. I think AI specifically, if we

	think about that as an emerging area, we're calling out increasingly, how are boards understanding how their company is aware of all their uses of AI? Because to understand and manage the risk landscape and to manage risk, you need to know what you have. And that's both internal, what are the AI tools and applications that are in use? The associated data that's being pulled into those, which might be very large data sets, but also in their supply chain. Who are their service providers and others that are making use of AI with their data or connected to their networks? And then third, and really squarely at the intersection of AI and cybersecurity, I would say it's important to focus in on social engineering resilience and readiness as well. Knowing, as we talked about already, that attackers are increasingly benefiting from the use of AI to successfully initiate their intrusions, getting the kinds of metrics or insight into how is the company helping to build resistance and enhance awareness and lean on the most important, the human element of their workforce to help both prevent these kind of events, but almost as importantly, to alert people when they realize that they've been deceived as quickly as possible, because minutes actually can matter in incident response. And so, what kinds of metrics are showing that we're running through campaigns and awareness and testing our workforce, not because we want to penalize people, but because we want to help people understand this evolving threat landscape?
Leo von Gerlach	So incident testing is somehow key and building everything around it to be ready. I think that's a very good piece of advice. And as we draw this now to a close, Joke, and as we just, well, in addition to all the good guidance you have given us already, just want to get some further takeaways from this. Perhaps your typical best advice to clients, do this in the next, let's say, 90 days or so, just to improve your game, to be just even better ready than you were before, to have that level of excellence when it comes to responding to any incident.
Joke Bodewits	I think before you reach that level of excellence, there's one thing to consider in incident response, and that is your pre-litigation strategy. I think in that moment, that you become aware of an incident, the pre-litigation strategy should start. And as part of that, you also take your considerations in what you need to do in the next 90 days. Because in those next 90 days, it might be the moment that you actually have litigation starting. So, considering that from the outside is important. And looking what you need to do internally, it's definitely reviewing what has happened. It is an after-action review that you can do by just making sure that you understand what has happened, how were we prepared, how should have we responded to it, which we haven't done maybe, and how can we learn from that. generally, results in an improvement of policies and procedures, but also helping people to better understand what you expect from them in an incident going forward. We have developed role cards for clients to help the key individuals understand and their tasks and responsibilities in incident response, which turns out to be really helpful for the second incident that occurred. But it's also looking at your company

	communication plan. So what do you need to communicate to whom and how do you want to communicate? Making sure that you have templates ready should an incident happen again. But also managing the relationships with all those stakeholders should be something that you do in those 90 days after the incident. The internal stakeholders, which can be, or depending on the type of incident, your maybe your works council or your board members or maybe your shareholders, but also your external stakeholders such as the insurance companies, your business partners, the regulators to whom you have engaged, maybe law enforcement. Doing all of that is something that you traditionally do in your aftermath, maybe not in the initial 90 days, but definitely something to consider in that time frame. Then one thing to add to that is doing a tabletop exercise or a training in which you really help people to lift their knowledge of cyber incident response, the expectations that you have as a company and that hopefully that won't happen again.
Leo von Gerlach	Oh, I love that idea with the role cards in addition to the checklists and the playbook so that everybody really knows what to do when the moment has come. And as we speak about distilled pieces of advice, Paul, your one line that you would give clients to make it better next time.
Paul Otto	Joke and I regularly emphasize that where cybersecurity is viewed as a part of the culture and in support of the business and not a cost centre, time and again, that's where we see organizations be more resilient and more able to recover from these more significant cyber incidents.
Leo von Gerlach	That definitely makes a lot of sense. And thank you for this and thank you for the terrific insight that you have shared about your practice and all the good advice you give. Thank you indeed everybody for listening in and I hope you join us for the next edition of The Influencers coming up soon. Until then, take care, goodbye.