CLIFFORD
CHANCE

NAVIGATING CYBERSECURITY AND RESILIENCE IN 2024

— THOUGHT LEADERSHIP

MAY 2024

NAVIGATING CYBERSECURITY AND RESILIENCE IN 2024

Cybersecurity is not just a problem for the IT department. It is an enterprise-wide issue. In this extract from a recent Clifford Chance webinar, we explore global trends in cybersecurity and resilience and examine increasing levels of regulation which will impact a much broader range of businesses.

“Cybersecurity is difficult because there are lots of misconceptions. It's not about being totally secure or free from threats. It's about knowing what the right definition of security is. How much are you prepared to invest in protecting your systems? How can you properly prepare for a cyberattack? What types of policies and tools are required? Importantly, will regulators and counterparties agree with your definition of appropriate security?” says Oscar Tang, a Clifford Chance Senior Associate.

The US perspective

In the US, cybersecurity has been a board level issue for a long time, but it has recently become even more important. "The fines for security breaches are larger, the public expects companies to treat cybersecurity as a crucial issue and regulation is increasing – the US now requires US publicly listed companies as well as foreign private issuers to have a cybersecurity disclosure programme in place and a specific requirement for board involvement with cybersecurity," says Megan Gordon, a Clifford Chance Partner and co-head of the US data privacy and cybersecurity team.

"As a result, boards have become very active and are doing much more than just asking 'do we have a programme in place?'. They are looking at how third parties are used, digging into supply chain risk management and treating cybersecurity as a material issue," she adds.

What's happening in Europe?

The situation is similar in Europe and legislators have become much more active in response to increasing cybersecurity risks. For example, in 2022, the EU published the Digital Operational Resilience Act (DORA) together with the Network and Information Security Directive II (NIS 2) and the Critical Entities Resilience Directive (CER), which aims to reduce the vulnerabilities of physical and digital infrastructure in the EU. "We already have a pretty high level of regulatory requirements in the European Union, including the General Data Protection Regulation (GDPR), which, as well as focusing on personal data, requires controllers and processors to implement and maintain adequate technical and organisational security measures," says Holger Lutz, head of Clifford Chance's Tech/Digital practice in Germany. "In addition, the ECJ has ruled that the potential misuse of personal data, such as in the case of a cyber-attack, can constitute non-material damage. The consequence of this decision means that more and more data subjects are trying to get money out of companies after a data breach or cyber incident. So, companies are not only hit by the fallout from a cyber incident, they then have to fight with the data subjects with regard to damage claims," he added.

Requirements in APAC are expanding

Almost all jurisdictions in Asia have some sort of data privacy regulation and, increasingly, those regulations contain some kind of notification provision. Indonesia, Vietnam and Singapore, for example, have expanded and strengthened the scope of their notification requirements recently.

In Australia, for example, there is a proposal to change the existing cybersecurity infrastructure legislation to include telecommunications operators who are currently regulated under their own separate regime and a recent proposal to create a mandatory ransomware notification requirement in order to gather more information on this kind of incident. Meanwhile, in Singapore, the Cybersecurity Amendment Act significantly expands the types of regulated entities under the cybersecurity regime to include, for example, foundational data infrastructure providers and cloud service providers. These entities will now have to comply with a range of requirements, including notification of a cybersecurity incident.

The Middle East – safeguarding critical infrastructure, national security and data

Three things influence public policy development of cybersecurity frameworks in the Middle East – safeguarding critical infrastructure, safeguarding national security and safeguarding data as a national resource. In Saudi Arabia, for example, in March, a draft data sovereignty public policy was released for consultation and its first principle is recognition of data as a national asset.

"Oil and natural gas infrastructure entities are very attractive to threat actors and protecting them is a priority because any breach could have local and far-reaching consequences," says Alison Evans, a Clifford Chance Counsel who has worked in Qatar, Saudi Arabia and Dubai on data protection, cybersecurity and tech issues. "Recognition of data as a national resource underpins regulatory obligations, particularly around localisation. In providing advice to clients, we've had to address how client compliance programmes might need to adapt to stricter localisation requirements," she adds.

"Gathering information about regulatory activity can be difficult. Even if general announcements are made by ministries, they may not include specific details about the action, but I think that is going to change as data protection laws embed," Evans says.

Across the region, regulators are prioritising clear documentation for entities to align with international best practice and they are open to discussions with regulated entities and for collaboration with businesses. For example, the UAE Cybersecurity Counsel has collaborated with KPMG to explore the future of cybersecurity in the next 50 years, highlighting potential policy decisions that the UAE might consider to maximise its cyber resilience. "Staying on top of regional nuance is going to be really important, as it's going to be a continuing compliance challenge, especially for those global entities where compliance programmes are EU- or US-centric to begin with," she adds.

Meanwhile, fintech is rapidly expanding in the Middle East, bringing huge benefits for retail banking, but also some new challenges to ensure that adequate protections are in place for the large amounts of sensitive data that are now being exchanged.

Supply chain risk

One of the biggest issues for companies is when third parties or suppliers are subject to a cyber-attack. "It impacts a wide swathe of different clients and the issue they have when they speak to third parties is getting information about what data of theirs has actually been impacted so they can see if they themselves have disclosure or notification requirements. This is a huge issue and one of the most difficult to risk manage," says Gordon.

"The US perspective is that you are pretty much responsible for your supply chain, so you can't bury your head in the sand. The National Institute of Standards and Technology (NIST) guidance on cybersecurity says that security requirements should be included in the RFP and in every contract there should be an agreement that a security team will work with the supplier on site to address anyvulnerabilities. It's a 'one strike and you're out' approach," she adds. In addition, the US Securities and Exchange Commission (SEC) specifically states that companies have to disclose information about third parties in the cybersecurity process.

A particular issue in the US is in the "connected" automobile sector, where there are proposals regarding how data is collected by Chinese-made vehicles and whether those vehicles could collect sensitive data about US citizens and infrastructure. "Access to data, supply chain access to data and how the supply chain works will become increasingly important in the future across a range of sectors", she says.

"In Europe, there is an increasing focus on supply chain risk," says Holger Lutz. DORA, for example, contains an entire chapter dealing with the management of third-party risk. Financial entities, amongst others, are required to conduct audits and inspections of their third-party service providers of information and communication technology. DORA will be applicable from 17 January 2025 and imposes certain minimum requirements for contractual arrangements with third-party service providers relating to cyber incidents. "For a financial entity, this will involve many contracts that will need to be amended. The German financial services regulator, for example, is urging financial institutions to look at the biggest and most critical contracts to meet this tight deadline," he says.

And in Singapore, the Cybersecurity Amendment Act will also have an impact, but from the reverse perspective, as David Olds explains: "The Act increases the number of entities that may be regulated and imposes obligations on them in relation to cybersecurity. Those entities are going to need to renegotiate their contracts with their financial institution customers in order to make sure that they can comply with the new legal requirements. That is going to be a real challenge."

Incident management and response and its impact on global businesses

In the past, businesses that were affected by a breach of cybersecurity focused on two things – getting the issue under control and complying with applicable notification obligations from a legal perspective, to reduce the risk of any fines or contractual claims. "In the EU, under the GDPR, if you mess up the notification obligations and fail to notify the authorities about a personal data breach within 72 hours, you are taking a quite big risk," says Lutz. "That is a very tight deadline, but under DORA, the latest version of the notification obligations foresees an initial notification to be submitted within four hours from the moment of classification of the incident as a major incident, but no later than 24 hours from the time of detection," he says. "The tricky thing in the future will be to track down all the notification requirements in case a breach or an incident happens so the company can actually comply with as many of the different notification obligations as possible."

In China, the Cybersecurity Authority published some draft measures in 2023 which have a one-hour notification requirement for certain types of incidents (India already has a six-hour obligation in place). "They're only draft measures and we are not certain if they are going to come into force, but it is a very strict test," says Olds.

Enforcement

"The US likes to regulate through enforcement actions," says Gordon. Huge fines have been imposed for cyber breaches, including, for example, a US$5 billion fine levied against Facebook in 2019 by the Federal Trade Commission – one of the federal agencies that regulates cybersecurity – which was then reduced in court to US$725 million. Cyber security is regulated federally, as well as by the States and the New York Department of Financial Services, which has been at the forefront when it comes to the regulation of financial institutions' cybersecurity requirements. "If you think about how many US regulators can get involved in these types of enforcement actions, the sums can get quite large. The private bar is now very well established at dealing with cybersecurity breaches. There's a whole group of private plaintiff attorneys that will bring actions against companies," she adds.

The cost of fines in Europe has not reached the same level as in the US, but many have been issued, mostly under GDPR for insufficient technical and organisational security measures. "I think one of the main developments, in the coming months and years, is that companies will not only have to deal with the fines, but also with private claims from the data subjects for immaterial damage," says Holger Lutz.

Is AI changing the nature of cyber threats?

"AI is a double-edged sword. On the one hand, there are AI cybersecurity products that can help identify and root out threat actors; on the other hand, AI is able to mimic voices, videos and emails which will help those threat actors," says Megan Gordon. "AI is going to have a huge impact going forward and hopefully the good guys will outpace the bad guys."

In the Middle East, the UAE and Saudi Arabia are rapidly expanding their national AI capabilities as well as introducing regulatory frameworks for new technologies. "Abu Dhabi, for example, has established the AI and Advanced Technology Counsel which aims to collaborate across the region on AI security and building trust," says Alison Evans.

What should companies do?

- Cybersecurity is a company-wide issue. It's about planning, being prepared for an incident and ensuring that the right people in your organisation know what is happening, and that everyone understands their role and what they need to do.

- One of the trickiest things is to consider the different obligations, especially notification obligations across the globe. Companies should prepare an overview of notification obligations in order to actually match most of them or many of them if an incident actually occurs.

- Be prepared to address regional nuances across the different regimes. If your compliance program is EU or US centric, have systematic ways to undertake gap analyses to address these regional nuances, particularly around the regulatory environment that implements data sovereignty policies and may require localisation or result in restrictions on cross-border transfers for cybersecurity purposes.

- Financial entities in particular should start early with activities requiring cooperation from third parties – such as the obligation to amend the contracts with ICT third party service providers.

CONTACTS

Alison Evans
Counsel
Düsseldorf
T: +49 211 4355 5045
E: alison.evans@cliffordchance.com

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com

David Olds
Counsel
Hong Kong
T: +852 2825 8996
E: david.olds@cliffordchance.com

Oscar Tang
Senior Associate
London
T: +44 207006 3749
E: oscar.tang@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2405-010981