Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Cyber risk management, incident response and investigation solutions

Contacts

Ffion Flockhart
Partner, Global Co-Head of Data Protection, Privacy and Cybersecurity, London,
Tel +44 20 7444 2545
ffion.flockhart@nortonrosefulbright.com

Christoph Ritzer
Partner, Frankfurt
Tel +49 69 505096 241
christoph.ritzer@nortonrosefulbright.com

Jay Modrall
Partner, Brussels
Tel +32 2 237 61 47
jay.modrall@nortonrosefulbright.com

Anna Gamvros
Partner, Head of Data Protection, Privacy and Cybersecurity – Asia
Tel +852 3405 2428
anna.gamvros@nortonrosefulbright.com

Jurriaan Jansen
Of counsel, Amsterdam
Tel +31204629381
jurriaan.jansen@nortonrosefulbright.com

Julie Himo
Partner, Montreal
Tel +1 514 847 6017
julie.himo@nortonrosefulbright.com

Nick Abrahams
Partner, Sydney
Tel +61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

Marcus Evans
Partner, Head of Data Protection, Privacy and Cybersecurity, – Europe, London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Nadège Martin
Partner, Paris
Tel +33 1 56 59 53 74
nadege.martin@nortonrosefulbright.com

Adjou Ait Ben Idir
Partner, Dubai
Tel +971 4 369 6393
adjou.aitbenidir@nortonrosefulbright.com

Stella Cramer
Partner, Singapore
Tel +65 6309 5349
stella.cramer@nortonrosefulbright.com

Chris Cwalina
Global Co-Head of Data Protection, Privacy and Cybersecurity, Washington DC
Tel +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

John Cassell
Partner, Calgary
Tel +1 403 267 8233
john.cassell@nortonrosefulbright.com

Managing cyber risks

Our experience at a glance

Our global cyber risk practice advises many of the world's leading corporations on managing and mitigating their data protection, privacy and cybersecurity risks. This includes developing internal policies and procedures, drafting comprehensive cyber incident response plans and stress testing those plans by conducting simulated cyber incidents.

When cyber incidents occur, our global emergency response team co-ordinates the legal, regulatory, IT and PR response, drawing on our established network of experts whilst taking steps to help maintain legal privilege. Our response team's work includes co-ordinating internal investigations and dealing with external investigations arising as a result of the incident.

Our recent experience in dealing with the types of multi-jurisdictional cyber risk challenges and incidents facing large financial institutions and multi-national corporations includes the following:

Incident response plans and playbooks

Drafting and implementing an incident response playbook for a global financial institution in light of a number of high-profile adverse cyber incidents, with reference to the specific cyber risk challenges faced by the its various business units as well as the legal and regulatory obligations imposed on the institution in a range of jurisdictions.

Reviewing and optimising incident response plans and playbooks for a number of large organisations in multiple industry sectors, often in the context of impending GPDR implementation. Our work in this area frequently addresses data security and privacy issues affecting critical infrastructure, system availability and personal information breaches.

Incident readiness and risk management

Providing advice and training on an international basis to various boards of a global financial institution on a number of systemic and sector-specific cyber risk issues, including in relation for forthcoming legal and regulatory change in Europe and Asia.

Provided advice and training for to the Australian operations of an international financial institution in respect of compliance with mandatory data breach notification laws, data breach response plans, cyber security and management of IT vendor security issues.

Advising a global financial institution on its legal obligations arising out of the cyber risks that it faces in a number of Asian jurisdictions including India and Singapore.

Conducting a privacy and cyber risk review of existing apps and apps in development for a multinational financial services company.

Liability risk

Co-ordinating the multi-jurisdictional response to incidents involving the compromise of our clients' customers' personal data, including one incident which resulted in data being compromised in 120 jurisdictions following a targeted spear-phishing attack. In each case, our global team and network of correspondent counsel provided advice within a short window which contained the incident and minimised the liability risk to our client.

Representing our clients in third party claims arising from cyber incidents, including, by way of example, defending a financial institution in a number of class actions alleging privacy violations for collection of personal data in credit card transactions and defending a large multinational organisation against claims of misappropriation of confidential information.

Outsourced vendor risk

Representing multiple clients in bringing business-to-business claims against third party vendors, including companies such as website developers, software companies and point-of-sale vendors, to seek recovery of losses arising from cyber incidents.

Losses from malicious acts

Co-ordinating the response to a number of distributed denial of service attacks and ransom demands which temporarily impact our clients' systems and online client services (including one such incident affecting a Swiss financial institution). Our recent work in this area has included advising a large financial institution on mitigating business interruption and preventing further attacks by assembling a team of forensic consultants to implement improved IT security, as well as extortion negotiators to advise on the bitcoin ransom demand.

Advising clients following the hacking of systems and accounts resulting in direct financial losses of several million and taking additional steps to successfully freeze payments and effect recoveries.

Regulatory risk

Representing a number of organisations in respect of serious data breaches requiring urgent drafting of communications to affected employees and data subjects in multiple jurisdictions, regulator notification letters and FAQ documents. Assisting with settlement negotiations with regulators, largely resulting in avoidance of fines and other sanctions.

We are experienced in advising clients on the planning and execution of internal investigations following significant cyber incidents. This work often includes implementing appropriate communications protocols to safeguard legal privilege and confidentiality, managing the investigation process and stakeholder engagement, advising on notification requirements and management of legal risks throughout the investigation, working with forensic experts and IT teams to assist with containment and remediation, and stress-testing all investigation findings.

We also assist clients in the event that they have become the subject of a government or criminal investigation or related litigation. We are experienced in providing and coordinating jurisdiction-specific advice to clients on how best to liaise with government and national crime agencies as well as providing an overarching global strategy.

Reputational risk

Successfully containing major international personal data breaches, including one breach involving the finance records of some 5,000 data subjects, which involved working closely with the client's senior management team, IT and PR consultants, managing the regulatory notification process and setting up call centre support as well as credit monitoring facilities for the affected data subjects. The incident was contained without any media attention, thereby minimising the reputational risk to our client.

Losses from error and malfunction

Providing emergency incident response following leaks of highly sensitive confidential information and intellectual property due to employee error and other causes. On a recent matter, this involved urgently assembling IT specialists to block the server containing the leaked information and ensure no personal data had been compromised. We also conducted a review of the contractual notification obligations and co-ordinated the PR and communications with the third parties whose IP had been leaked, thereby containing the incident with no resulting loss to our client.

Our approach to incident response

Example cyber incident

"An employee in your organisation has been spear-phished by hackers and has inadvertently introduced malware into your systems.

As a result, the hackers have compromised your networks and obtained access to large quantities of personal data, including employee and customer data and key business information to third parties. Via a series of servers, the hackers have exfiltrated the personal data to an externally-hosted server. Data has been stolen in large volumes belonging to data subjects located in the UK, Singapore and the US.

The hackers are demanding the payment of a Bitcoin-denominated ransom for the return of the data. If the ransom is not paid, the hackers are threatening to post the data publicly via the internet."

Norton Rose Fulbright's response

01 | Gathering necessary information as swiftly as possible

To ensure an effective incident response, information needs to be gathered as quickly as possible, while maintaining privilege over sensitive communications.

The information gathering process will involve considering questions such as the following:

What forensic steps have been taken to date? How have these steps been documented and are they evidentially sound? How are your technology systems structured in the affected jurisdictions?

What is the nature of the affected personal data? Who are the affected data subjects/corporations and where are they located? What is the contractual position in relation to affected corporations?

Who knows about the incident at present? Have any external agencies such as law enforcement been made aware of it? Might any employees/other insiders be involved and has this been discussed with HR?

Do you have a policy on dealing with incidents involving extortion?

02 | Involving other service providers

We would involve other service providers in the incident response, with whom we have well-established working relationships. Given the nature of the incident, this would include:

IT forensics and security specialists, in order to isolate the incident and prevent further losses of data from a technical perspective

Extortion management/negotiation specialists where necessary to deal with the ransom demand

PR/reputation management specialists to deal with reputational impact

We co-ordinate the work of these specialists in order to ensure that work product retains privilege to the extent possible, so as to protect those documents from disclosure in future legal action or regulatory investigations.

03 | Establishing the notification position to regulators and data subjects

A key element of the response to the incident will be determining how you will need to engage with regulators, data subjects and other entities such as stock exchanges in connection with the incident.

This would be done in each affected jurisdiction by Norton Rose Fulbright or by one of our correspondent law firms (or a preferred law firm of your choice).

04 | Co-ordinating the response

We would co-ordinate the response on an on-going basis in order to mitigate the impact of the incident.

This will involve co-ordinating notifications and engaging on an ongoing basis with regulators, data subjects, contractual counterparties and relevant stock exchanges in all affected jurisdictions. We also co-ordinate any investigations arising out of the incident and work closely with the IT forensic experts. We stress-test their findings in order to comprehensively advise our clients on both regulatory and litigation risk and to ensure that appropriate steps have been taken to mitigate the impact of the incident and to prevent any recurrences.

We will draft the necessary correspondence and FAQ documents, set up call centres and arrange credit monitoring services.

We will also defend any claims brought by data subjects or contractual counterparties and actions by regulators, as well as take formal steps against those responsible for the incident to seek recovery of any losses.

Cyber risk management solutions

Cyber risk management

Assist in the development and/or review of checklists, policies and procedures.

Drafting and stress-testing of cyber incident response plans or “playbooks”.

Cyber academy

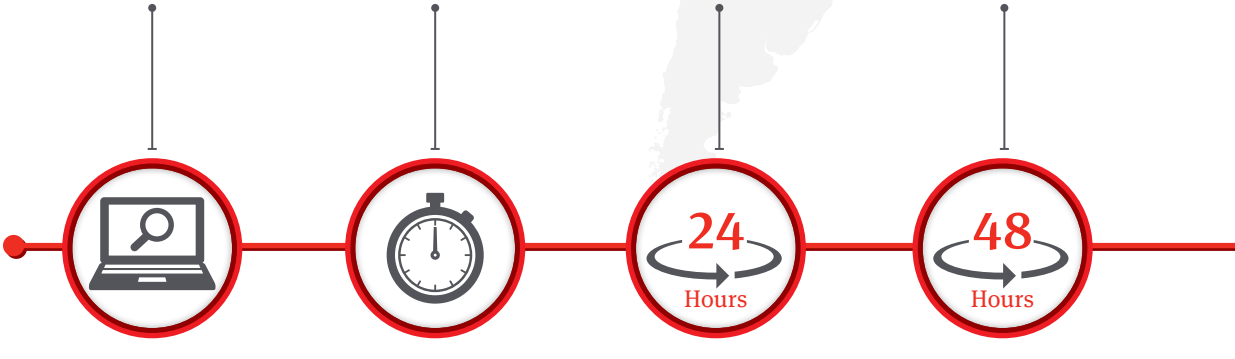
A tailored bespoke pre-incident readiness training by way of a Cyber Academy, to test policies, procedures and playbooks and incident preparedness.

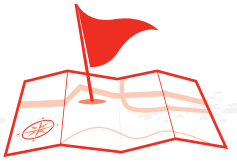
First response

Within 24 hours of a cyber incident being reported to us, we will provide initial advice and an urgent action plan on next steps, including emergency notifications and engaging with other service providers, e.g. IT specialists.

Interim updates

We will regularly contact and work with your internal incident response team to provide any updates to our initial advice.





Strategic plan

Within 72 hours of a cyber incident being reported to us, we will

- Provide or procure legal advice in relation to all jurisdictions affected by the cyber incident
- Prepare a comprehensive response plan
- Engage further with other advisers, e.g. IT and PR experts, to assist with the cyber incident response
- Coordinate continued engagement with regulators, such as the data protection authorities, as well as the financial regulator and stock exchanges, as may be necessary at this stage.

Continued engagement

We will continue to engage with other parties assisting with the incident response process.

Ongoing support and investigations

Following the Strategic Plan, we will provide ongoing support. In particular, we will

- Make further notifications to regulators and professional bodies as may be necessary
- Provide advice on communications with data subjects, where necessary
- Continue to engage with the other service providers assisting with the incident response process
- Provide further advice on lost data and recovery
- Plan, co-ordinate and stress-test incident response investigations, including internal investigations and investigations by third parties
- Represent you in legal and/or regulatory proceedings that may arise as a result of the cyber/data breach incident
- Provide jurisdiction-specific advice to clients on liaising with government and national crime agencies (as required)

Global resources

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3700 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

People worldwide

7000+

Legal staff worldwide

3700+

Offices

50+

Key industry strengths

- Financial institutions
- Energy
- Infrastructure, mining and commodities
- Transport
- Technology and innovation
- Life sciences and healthcare

Our office locations

Europe
- Amsterdam
- Athens
- Brussels
- Frankfurt
- Hamburg
- Istanbul
- London
- Luxembourg
- Milan
- Monaco
- Moscow
- Munich
- Paris
- Piraeus
- Warsaw

United States
- Austin
- Dallas
- Denver
- Houston
- Los Angeles
- Minneapolis
- New York
- St Louis
- San Antonio
- San Francisco
- Washington DC

Canada
- Calgary
- Montréal
- Ottawa
- Québec
- Toronto
- Vancouver

Latin America
- Mexico City
- Rio de Janeiro
- São Paulo

Asia Pacific
- Bangkok
- Beijing
- Brisbane
- Canberra
- Hong Kong
- Jakarta[1]
- Melbourne
- Port Moresby (Papua New Guinea)
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa
- Bujumbura[3]
- Cape Town
- Casablanca
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]
- Nairobi[3]

Middle East
- Dubai
- Riyadh[2]

1 TNB & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright US LLP
3 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.