Cybercrime attacks: Before and after –12 things to think about in the regulated sector

大成 DENTONS

October 26, 2018

Before

1. Policies and procedures

All businesses are at risk of cyber attacks. Having in place appropriate policies and procedures, however, helps to mitigate the risk of a cyber attack. Policies to consider putting in place include an acceptable use policy, a clean desk policy, a monitoring policy and a BYOD policy. It is also important that these policies are circulated and that regular training is offered to staff on how to avoid and spot cyber attacks. The sooner they are spotted, the easier they can be to shut down. Maintain awareness campaigns to ensure staff can identify cyber risks and follow good practice.
Risks relating to personnel are highest when they are leaving your business. To guard against this it is essential to have strict protocols in place to protect the integrity of your data, and your confidential information and trade secrets, when an employee has resigned, is being suspended or is dismissed.

2. Know your data

Ensure you know what data is stored on which systems. This likely requires an audit and data mapping exercise. You'll need to have this at your fingertips in order to deal with a breach quickly and efficiently. This should also cover data held by processors and vendors.
In addition, operators of essential services and digital service providers outside the financial services sector may be required to report certain cyber incidents to competent authorities under the Network and Information Systems Regulations 2018.

3. Incident response plan and business continuity plan

Implement an incident response plan and a business continuity plan to ensure that attacks are handled as swiftly and efficiently as possible. Ensure that all key stakeholders are aware of their roles and responsibilities.

4. Cyber insurance

Check if existing insurance would provide any cover. If not, consider investing in cyber insurance to assist with covering the financial costs of an attack and its fallout. After an attack, make sure you notify your insurer early on and get their buy-in to your response.

5. Governance and leadership

It should be clear who has overall responsibility for cybersecurity (both policies and plans and responding to incidents). In particular, responding to a breach may involve both internal personnel, such as CISO, CIO, Legal, Compliance, HR, Comms and Risk, and external agencies, such as IT forensic providers. Ensure that it is clear exactly who is in charge of coordinating their efforts.

6. Templates

Have template reporting notifications ready to deploy in the event of a breach. This would include notifications to individuals and steps they can take to protect themselves (like changing passwords/monitoring their accounts).

After

7. Find out what happened and identify key data

It is important to determine the nature of the breach, the data compromised and the cause. Was this a confidentiality breach (where data has been accessed by unauthorised parties) or also an availability breach (where access to data was lost) or an integrity breach (where data has been corrupted) or a combination of these? This will inform your response to the attack, in particular whether you need to notify customers, and ensure that losses are mitigated. If a written report is being prepared consideration should be given to legal professional privilege.

8. Communications

Often, the most harmful aspect of a cyber attack can be the reputational damage and loss of customer confidence that follows. This is even more so where the business is a listed company. It is therefore essential to control both internal and external communications relating to an attack. Having a clear communications strategy in place, which sets out the types of information that will be shared and with whom, will help keep reputational harm to a minimum.

9. Insider threats

Employees are often a business's biggest asset. But they can also be your biggest liability, especially when it comes to cyber attacks. Ensuring that comprehensive employee screening is carried out pre-employment and training staff on basic data security protocols (such as using alphanumeric passwords and use of encryption) can significantly reduce the risk of an attack occurring. Monitoring tools can also help identify an attack based on threat vectors. It is also important to ensure that any employees involved in a cyber attack are dealt with promptly and appropriately, and that proper investigations are carried out to determine their accountability. Disciplinary action may be required and (for firms subject to the Senior Managers and Certification Regime) this may also give rise to a need to consider (i) an individual's fitness and propriety; and (ii) whether there have been any Conduct Rules breaches, making notifications to the FCA/PRA and disclosing the matter in an individual's regulatory reference accordingly. Ensure you have a whistleblowing line in place, to ensure that employees and others can raise concerns to minimise the risk that they go directly to the regulator instead.

10. Liaising with law enforcement

It may be necessary or appropriate to liaise with law enforcement in relation to the attack. Law enforcement may wish to speak to you as victims of the attack or it may be linked to a wider investigation. Ensure that you consider the possible implications of law enforcement involvement and that you understand the nature of their requests.

11. Reporting to the Information Commissioner's Office

If the cyber attack involves personal data there may be a duty to report it to the relevant supervisory authority such as the ICO. This applies to confidentiality, integrity and availability breaches (the "CIA triad"). You need to assess the risk to individuals to determine whether there is a duty to notify the ICO and/or data subjects. Notification to the ICO is required within 72 hours and all breaches must be recorded in a breach log in any event.

12. Regulatory reporting requirements

Regulated entities will have reporting duties over and above those of other entities. Relevant considerations may include notifying the FCA (or PRA) under Principle 11 and SUP 15.3 or making a Suspicious Activity Report to the National Crime Agency. If you decide it is not necessary to make such a report you should clearly document the rationale for that decision. When making a notification this should be done with the understanding that the various bodies may well share information so it is advisable to ensure that all notifications are co-ordinated and consistent.

Your Key Contacts

Nick Graham
Partner, London
D +44 20 7320 6907
M +44 7795 618 315
nick.graham@dentons.com

Katharine Harle
Partner, London
D +44 20 7320 6573
M +44 7795 618213
katharine.harle@dentons.com

Marija Bračković
Senior Associate, London
D +44 20 7246 7485
M +44 79 2050 4734
marija.brackovic@dentons.com