
LexisNexis®

# LexisNexis In-house Advisory Board

## Cybersecurity and how organisations can best protect themselves

# Cybersecurity: how can organisations protect themselves?

On 21 June 2016, the LexisNexis In-house Advisory Board met to discuss the challenges of cybersecurity and the threat that an attack poses to an organisation in terms of financial and reputational risk. The discussion focused on the role of education and communication across the organisation and practical tips on how to be better prepared for a cyberattack. Highlighted in particular were the benefits of doing simulations and the challenge of privilege.

The session was facilitated by Marc Dautlich, partner in the TMT group and Head of the Information Law team at Pinsent Masons.

## Key topics discussed and covered in this paper:

- How cyberattacks can range in scale
- Education and communication
- Measuring the outcomes of a campaign
- The challenge of privilege
- How to prepare for a cyberattack
- Conclusions: the key measures to set in place

## Introduction

Marc Dautlich opened the session with an explanation of the ways in which a cybersecurity attack can range in scale and how that affects the evaluation of the risk and how an organisation responds.

On one end of the scale, the example was given of a dating agency website, where, because of a fault in the configuration of the website, information that was entered by members to be able to search by location in fact, in some cases, narrowed people down to the street where they lived. A risk assessment quickly identified that it was not difficult for a user who wanted to track an individual down to do so by using the location information and the rest of the member's profile. This placed the member at risk of physical harm should there be a criminal intent. In this case, the response was quick and clear – interrupt the service to reconfigure the website, even though this could be inconvenient for members using it.

To demonstrate the other end of the scale, the example was given of a malicious hacker who had been in an organisation's domain for nearly two years. Understanding the motivation of the attack is important and helps inform how an organisation responds. Forensic experts were appointed, but there was no obvious motivation driving the hacker. There had been no evidence of financial consequences or activism and no apparent damage. It was concluded that, owing to the nature of the business that the organisation conducted, the motivation must be espionage and gathering of competitive intelligence.

An operation was put in place which took several months with the objective of creating a robust plan to eradicate the hacker from the system. In cases such as this, an organisation only has one opportunity to ensure the hacker is definitely eliminated from the system, otherwise malware is likely to remain in the organisation enabling the attacker to reappear in the future. Once there was confirmation that the operation had been successful, the organisation could start to address the legal aspects in terms of how customers, regulators, and stakeholders, etc, were informed.

> "Understanding the motivation of the attack is important. It helps inform how an organisation responds"

## Education and communication

The discussion moved on to the question of how effectively an organisation can plan a response for when a cyberattack happens. The Board agreed that when it comes to cybersecurity it is not a question of 'if' but 'when' an attack will happen. It is crucial to be able to deal with the attack in such a way that financial and reputational damage to the company is kept to a minimum. In some instances, the crisis can even be used to enhance a company's reputation and build on brand equity.

The Board members discussed the value of running simulations and raising awareness of cybersecurity to educate employees as the first line of defence. One example shared with the Board was a multi-pronged approach among employees across a global organisation. The initiatives included:

- Education focused, multimedia initiatives: 15 second video guides, one-page reference guides, ongoing email communications with top tips on how to spot a phishing email and how to respond.
- Consistently emphasising that raising a concern will never be frowned upon – even if the employee has been over cautious, reporting the concern is the right action to take.
- Running activities to help the organisation prepare as much as possible for when a cyberattack happens, including for example sending fake phishing emails to ascertain whether employees are in a position to help protect the organisation in the event of an attack.

> "Employees are the front line of defence in cybersecurity risk management"

The organisation learned three key lessons from their approach:

1. Education and communication have a definite impact – you can statistically see a better outcome when you run a campaign. An organisation will in all likelihood never get rid of the threat overall – possibly never getting lower than 10% as a threat level – but it can minimise the threat through education and communication.
2. Phishing emails are becoming more and more sophisticated. When running a test, the more personal and sophisticated you make the phishing emails, the more likely employees are to respond. For example:
    - Create an email from the CFO or CEO asking for budget within their budget limit during a period when an important merger and acquisition is going through.
    - Create an email which goes out to all employees stating that an error on the HR system has meant that their performance related ratings have been altered and they need to click through to check if they have been affected. This taps into an emotional and personal point of interest.
3. Every 'test' phishing exercise has the opportunity to be used as a further education and awareness raising tool. They can be used as training to educate people on what they should have looked out for in the email.

## Measuring the outcomes of a campaign

Marc Dautlich shared recommendations with the Board about how organisations can monitor the outcomes of a campaign on an aggregate level by measuring:

- The number of people that report the emails to IT.
- The number of people that click through from the email.
- The number of people that simply delete the email.

Employees are the front line of defence in cybersecurity risk management. Information governance is a team sport. Measuring the outcomes of a campaign will help an organisation understand its employees better:

- Is the culture among employees to take responsibility to act against an attempted cyberattack and inform the correct people – or simply ignore it?
- Do employees know how to recognise a possible cyberattack?
- Do employees know how to respond to a possible attack – who to inform, what to do, etc?

Two key challenges for dealing with a threat effectively were highlighted:

- An organisation may have a lot of the technical kit but if it is not configured for that organisation then it will not be as effective.
- The IT team may not have within their remit the full set of tools and abilities required to deliver a secure environment (which can require a cross departmental approach involving all stakeholders). They aren't necessarily experts in information security and it is wrong to assume they have all the answers. Furthermore, technical matters are only part of the information security challenge. It is generally easier for a hacker to exploit an individual than to exploit a technical vulnerability, such as a corporate firewall.

> "Privilege is a huge issue and needs to be considered early on"

## The challenge of privilege

When a cyberattack occurs, organisations often need the assistance of a third party to support the preservation evidence. For example, a server needs to be imaged, isolated and investigated to help identify the nature and scale of the problem.

An organisation might also commission a report to fully understand the incident and its ramifications.

↑ Back to contents page

Those commissioned to produce the report need to demonstrate that it delivers value for money and an audit trail is therefore created as the report gets circulated and commented on. This can be very unhelpful in terms of the content and its vulnerability to future disclosure to third parties.

In these situations, privilege is a huge issue and needs to be considered early on.

The Board considered the question of whether the in-house legal department should throw the cloak of legal privilege over such commissioned reports. Often, in-house counsel have no understanding at first of what has happened and, even if they think they understand the scale of the incident, it can mushroom. What starts as 1,000 records can quickly become hundreds of thousands or millions records. The issue of privilege isn't appreciated because the underlying facts or extent of the incident isn't understood at the very early stages when the decision around privilege needs to be taken.

The Board also commented that the whole issue of privilege is a bigger challenge because of European legal challenges in recent years to privilege attaching to communications between in-house counsel and the organisations by which they are employed. In practice, many organisations struggle to ensure that privileged status is retained.

One suggestion from the Board was to retain outside counsel to appoint the forensic experts, pursuant to an engagement under which outside counsel obtains the report from the forensic expert (or other similar expert) for the purpose of giving legal advice to the organisation which has suffered the cyberattack. This approach does slow down the process but if, as an organisation, you have prepared and have thought about it in advance, the cumbersomeness of the process can be minimised and it is more likely to secure privilege.

"Finding a working definition on what constitutes an actual breach is vital"

## Further challenges

The Board noted that Legal are often advised quite late on when an attack has happened. In a large organisation it can be particularly complex to catch the starting point. It can often take a week, or even longer, before anyone lets Legal know what has happened. Time may have started running and any delay may breach deadlines for disclosure to regulators (eg to the ICO in the case of a data breach).

The Board felt that the regulators haven't taken into account that for many organisations there are thousands of near misses every day in terms of failed cyberattacks. As such, finding a working definition of what constitutes an actual breach is vital. Here, money laundering was given as an example. As the consequences of not reporting an incident are severe, ie criminal prosecution, the regulator needed to introduce materiality thresholds because too many incidents were being reported and there was not the budget or resources to deal with the number of reported incidents.

Similarly, the ICO don't appear to have the funding and resource to manage the anticipated volume of reported incidents. However, it was noted that currently the ICO do take a very practical approach in dealing with the reporting of incidents.

*Brexit*

If Britain leaves the EU, the question of who will make the law around data protection is raised. The government will need to consider whether and to what extent it can depart from GDPR while at the same time ensuring that the UK remains adequate (in data protection terms) for the purposes of cross-border data flows.

Brexit would mean a mind blowing task of reviewing all the law in detail. However, the basic framework of the UK's relationship model with the rest of Europe is needed before this exercise can be embarked upon in any detail. For example, will the UK follow a model relatively close (for these purposes) to full membership such as Norway (the EEA model)?

"Consider the question 'What do you want your customers to do in response to notification of the problem?'"

## How to prepare for a cyberattack

The main recommendation discussed by the Board was to run simulations for the executive response team. Knowing what to expect and how people react can help the organisation be prepared in terms of communication and reporting process.

From a simulation, an organisation can set in place the proposed stakeholders, for example Head of Legal, Compliance and Risk, IT, Information Security, PR (internal and preferably external crisis PR), and, depending on the organisation, HR and the COO. A decision making framework can then be put in place.

Enough preparation should be done to ensure plausibility in terms of the exercise so that stakeholders agree that the facts of the scenario could well apply to that organisation. The simulation needs to cover the sorts of consequences that the organisation would be most concerned about.



↑ Back to contents page

In many cases, a cyberattack involves an organisation's supply chain and it is important to understand the implications of this. It is one of the most vulnerable channels and presents significant risks. Having a supply chain also means there will be multiple agendas should a threat occur:

- Customer organisation – Is the provider at fault? Have they caused the breach?
- Provider's agenda – They will want to demonstrate they are not responsible but only supplying a service and that the onus is on the customer organisation.

The cyberattack on TalkTalk in 2015 was raised as a discussion point by the Board. The attack led to the theft of credit card and bank details of up to 4 million customers. The following comments were made:

- The general consensus was that the project management of the TalkTalk crisis was poor.
- The Board all agreed that the approach to such an attack needs to be simple.
- One recommendation was to appoint a chair so that the decision maker is a single voice. They must consult and gather a multidisciplinary team and then act as the final decision maker after listening to the team's opinions.
- In the early stages, there is no need to commit to an explicit timetable. Instead, commit to report updates. Explaining that you do not have all the facts but are investigating them with the intention of sharing relevant information as soon as you have it, is often sufficient.
- In the event of an attack, it is better to sit on your hands until you have a good understanding of the situation rather than make a fast and uninformed response.
- Organisations need to be cognisant that a claimant bringing legal proceedings no longer needs to show financial damage but only distress in order to claim damages.

Conducting simulations will help an organisation know, for example, how long it takes to get FAQs up on the website, what these should broadly cover and how long to establish a captive call centre to handle calls with a basic script. These are all elements that can be pre-prepared. It was agreed that there is no 'one size fits all' option but that Legal are in a strong position to look at all the aspects, ask questions and come up with a working plan.

The Board raised the question of whether it can be damaging to make a canned PR response if customers are already aware of the issue. For example, social media adds a level of complexity where customers often take to Twitter and as an organisation you have to respond quickly. Organisations need to be prepared for and plan for this. Is it in fact a better approach to come forward and take the flak?

One suggestion was to consider the question 'What do you want your customers to do in response to notification of the problem?'. Is there an action they should take (for example, a recommendation that they change their password) or is it the case that they just need to be informed? The organisation's PR message should address what you expect your customers to do so that their questions are answered.

*Johnson & Johnson – Tylenol*

The Board discussed the incident in the 1980s involving Johnson & Johnson as a good example of how to deal with customers and engage with the media. Several people died after Johnson & Johnson's bestselling painkiller product, Extra-Strength Tylenol, was sabotaged and laced with cyanide.

The company's objective was to protect their brand and preserve customer confidence in the most critical of situations. An estimated 31 million bottles of the drug were recalled and Johnson & Johnson offered to exchange all the capsules that had been purchased by the public. They also advertised in the national media warning people not to consume the product. Because of the upfront way in which they dealt with customers and the media, the brand was protected and Tylenol is still on the shelves today.

The Tylenol incident demonstrates how important it is to judge how much you share. Johnson & Johnson were honest about what they did and didn't know and they gave recommendations and guidance that considered the wider audiences that were affected. The Board agreed that advice provided to the public should be reassuring. In addition, advice needs to take into account not just the customers but also the regulators, shareholders and the board. This is exactly what multi-stakeholder simulations are good at identifying, enabling the organisation to prepare a much more effective response plan.

The Board also discussed the example of TalkTalk again with reference to the impact it had on banks and customers. TalkTalk advised customers to contact their banks to check for illegitimate transactions, which was potentially unnecessary and placed an unwelcome burden on the bank infrastructure and created an unnecessary anxiety for customers. This wider impact is something that organisations need to be fully aware of when making a response.

*PR responses*

Often the PR team want to tell the world and HR have a preference to inform all parties too, however Legal wants to assess risk. This can lead to different stakeholders wanting to take conflicting approaches.

*PR responses* can be written in advance, but there still needs to be an outline response plan. If the Daily Mail calls at 5pm and in-house counsel aren't available, who is next in line to respond? Organisations should prepare for a cyberattack in the same way they would for a product recall or a health and safety issue. If the focus is only on the technical IT side then this is generally the wrong approach.

The Board commented that it is not just about the plan if something goes wrong, it is also about looking at the culture of the organisation. It will be able to make a much more credible

↑ Back to contents page

PR statement in an emergency if it can show that it had not been careless, but had taken the appropriate precautions (eg by ensuring that the company has a compliant culture, the right policies and training).

> "Don't waste a crisis! An organisation won't get every response correct but you can gain critical learnings to take forward."

## Conclusions

The overwhelming takeaway from the Board's discussion was that organisations can never rehearse or prepare too much for the threat and aftermath of a cyberattack. It is also important to have an audit trail to prove that the preparation has been done.

The most important measures that a simulation can help set in place include:

*Identifying key stakeholders*

In practice, organisations in crisis need a very simple and clear plan to identify whom to contact and how to keep communications flowing. In a severe crisis, email or telephone systems may not be available so how to contact the relevant people (for example via personal telephone numbers) needs to be identified during a preparation exercise.

*Identifying an overall decision maker/lead*

Appoint someone within the stakeholder group who is the final decision maker. They need to be able to take on board everyone's comments, opinions and advice and then make the final call balancing risk and commercial considerations.

*Creating a risk register*

It can be difficult to ascertain if an incident is a severe crisis if the 'tech speak' is completely unintelligible. In a simulation you can work with technical colleagues to develop and understand cyber-risks and record them in a risk register, when there is time and space to do so. A risk register is a standard document that records risks, mitigations, risk proximity, likelihood, severity and actions – it is normally used in board contexts to manage material business risks.

*Ascertaining legal liability of third parties (for breach of contract and/or negligence)*

Although it is rarely a high priority at the very beginning of a cyber crisis, identifying fault on the part of a service provider in your supply chain involved in the incident may emerge to be important at a later stage. If Legal are not involved at the start, a forensic report won't be able to identify if what has happened is 'normal' and therefore the extent to which it is your supply chain that is at fault in relation to the security breach. Acquiring evidence to conclude whether the supply chain have been in breach may have other outputs such as sharing learnings with your service providers to reduce risk in future.

*Making time to assess the situation and your organisation's response*

At what point do you tell the stock exchange, financial regulators and customers? Having an outline plan helps ensure time is created to analyse just how serious the issue is and how the organisation should respond in different scenarios. This can be critical in how effective the response is.

*Being custodians of reputation*

People have a psychological need to need to know some information in a crisis. Being prepared gives you the ability to share information in a way that protects or even enhances your brand equity. The trick is to provide relevant and timely information. Don't give unnecessary information but do keep people informed in a timely fashion, and in the case of customers, try to be as clear as possible when identifying the recommended actions that they should take.

An important point to remember is this: Don't waste a crisis! An organisation won't get every response correct but you can gain critical learnings to take forward.



↑ Back to contents page

# The LexisNexis In-house Advisory Board

The Advisory Board meets 4 times a year to discuss a pre-agreed topic. This paper was produced as an overview to one of these discussions. You can view additional papers here.

**Jamie Barnard**
General Counsel, Unilever

**Lizzie Bayley**
Director, Shanks Waste Management

**Jeremy Berenzweig**
General Counsel and Senior Vice President - Legal, Flint Group

**Antony Braithwaite**
Vice President & Associate General Counsel, GSK

**Luscinia Brown-Hovelt**
Head of Legal, Westbury Street Holdings Ltd

**Sophie Carter**
Global Co-head Legal & Risk and Company Secretary, Christie's

**Steve Cowden**
Former General Counsel (retired), Reed Elvesier

**Clive Davies**
Senior Counsel, Fujitsu Ltd

**Kent Dreadon**
Head of Legal, Telefonica

**Duncan Gibbons**
MD and Legal Counsel, Royal Bank of Canada

**Sue Gozna**
Apple

**Toby Hornett**
Legal Director, Canon Europe

**Manu Kanwar**
General Counsel, Magine TV

**Ian Leedham**
Senior Counsel, Thames Water

**Victoria Lockie**
Associate General Counsel, Pearson

**Greg Morris**
Group Head of Legal and Compliance, Spencer-Ogden

**Kerry Phillip**
Legal Director, Vodafone Group Enterprise

**Matthew Redding**
Director of Joint Ventures and Partnerships
Legal Affairs, Everything Everywhere

**Seftton Samuels**
Operations Director, SMMT Ltd

**Hank Udow**
General Counsel, Reed Elsevier

**Suzanne Wise**
General Counsel and Company Secretary, Network Rail

**Melanie Wiseman**
Senior Legal Advisor, SMMT Ltd

**Roger Wiltshire**
European Legal Director, Euro NGC

---

### About Marc Dautlich

Marc is a partner in the TMT group and Head of the Information Law team at Pinsent Masons specialising in providing strategic advice to clients in both the private and public sector in relation to data protection, freedom o=f information, technology and e-commerce matters.

Marc speaks regularly at industry events on a range of data protection and technology issues, and is rated by Chambers UK 2015 as a top tier practitioner in relation to data protection, with a "depth of compliance knowledge" and "good commercial insight".



↑ Back to contents page