# Lawyer Insights

## Cyber threats are increasing – are you prepared?

Sarah Pearce and Ashley Webber of Hunton Andrews Kurth advise how organizations can take an active role in preparing for the worst, and learning from the past.

By Sarah Pearce and Ashley Webber
Published in Privacy Laws & Business UK Report | May 2024


The threat of cyber-attack is at an all-time high for businesses. The frequency of cyber-attacks continues to increase, both at the state and non-state level, while the nature of the attacks are becoming more intelligent and advanced, aided by the support of AI. Cyber-attacks can take many forms, for example phishing, password attacks, denial of service and, particularly common in recent years, ransomware attacks. Ransomware is a type of malware which prevents a business from accessing systems and data, usually by encrypting the files, resulting in the attacker demanding a ransom in exchange for decryption. While we are seeing increasing activity from legislators, regulators and law enforcement authorities globally to tackle the increasing risk of cyber threat, the first defense a business has is itself. This article explores some of the ways in which businesses can prepare for the threat of a cyber-attack, focusing on organizational measures a business can implement. However, we do not detail the kinds of technical security measures businesses could maintain in this respect.

**INCIDENT RESPONSE POLICY**

The foundation of any decent cyber threat defense is an effective incident response policy. A good incident response policy provides clear guidelines for responding to different incidents, such as personal data breaches, insider threats, and other security incidents. An incident response policy aims to identify incidents at the earliest stage and then manage and reduce the effects of the incident which should, in turn, limit or lessen operational and financial impact. The guidelines should, amongst other things allow a business and its personnel to:

- Recognize and respond to an incident;
- Assess the incident within strict time
- Constraints;
- Inform relevant stakeholders within.

The business such as senior members of the business;

- Comply with legal notification requirements including to regulators and impacted individuals;

This article presents the views of the authors, which do not necessarily reflect those of Hunton Andrews Kurth LLP or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article. Receipt of this article does not constitute an attorney-client relationship. Prior results do not guarantee a similar outcome. Attorney advertising.

- Identify remediation requirements; and
- Support the business in its recovery efforts.

There is no "one-size-fits-all" approach to preparing an incident response policy, and it may vary from company to company, but it is important to have one in place. Certain key components include defined terms to explain what commonly uses words and phrases mean, such as specific kinds of incidents, or personal data and an escalation process and requirements, starting with how to identify a potential incident and who to inform. Once an incident response policy is developed, or ideally before it is finalized and made available within the organization globally, it should be stress-tested to ensure it is in fact suitable for the business (see below for further information on tabletop exercises).

**RANSOMWARE PREPARATION**

With the significant increase in ransomware attacks, it is becoming more common for businesses to prepare and implement a dedicated ransomware protocol. Ransomware attacks present certain unique characteristics which require specific attention and action.

As with the incident response policy, ransomware protocols should also be tested before implementation is urgently required in the face of an
attack.

**TABLETOP EXERCISES AND TRAINING**

An extremely beneficial and effective way to prepare for incidents, to stress test and practice an incident response policy and any form of playbook, is to conduct a tabletop exercise. Tabletop exercises see relevant personnel respond to a hypothetical cyber-attack that has been prepared to reflect a potential reality for the relevant business.

Tabletop exercises are often conducted for selected groups of personnel. Participation by members of the incident response team is of course critical. Such individuals need to fully understand their responsibilities and rehearse their roles to allow successful implementation of the incident response procedure.

Training on cyber threats and how to respond is vital across all levels of the business for cyber threat preparedness. Business-wide training on cyberattacks usually discusses "incidents" in the broader sense, covering also noncyber based incidents. Such training should be provided to all employees upon onboarding and on a regular basis, and at least annually thereafter.

**THIRD-PARTY VENDOR MANAGEMENT**

Over recent years, there has been a significant increase in the number of supply-chain attacks. These are cyberattacks directed at third-party tools or services used by multiple businesses, i.e., in a supply chain. By targeting a third-party tool or service, the impact can be catastrophic, affecting hundreds or even thousands of businesses that use the targeted tool or service. While the root cause of a supply-chain attack cannot be clearly foreseen, there are steps a business can take to be prepared and limit the potential impact. For example:

© 2024 Hunton Andrews Kurth LLP

1. Implementing and maintaining a sophisticated third-party vendor onboarding process which includes due diligence of the third-party vendor;

2. Conducting a periodic review of the results of the onboarding due diligence; and

3. Having a set of technical an organizational measures which all third-party vendors must adhere to, or that can be used as a benchmark against the measures proposed by the third-party vendor.

**MONITOR TRENDS AND OTHER SOURCES**

Cyber-attacks often follow trends which are impacted by many things, such as global pandemics or financial crises, technological advancement and politics. While it will not be possible to predict a cyber-attack, a business can make efforts to monitor occurring trends to ensure it is prepared to face what other businesses in its industry or otherwise are experiencing. Another source to monitor is the guidance of regulators and other relevant bodies in the field. For example, many countries have cyber-crime “centres” or “bodies” which are not necessarily designed to supervise compliance of businesses by enforcing obligations but are designed to help in the case of an incident and to educate business on how to handle incidents if/when they occur. Such sources can provide very useful insights.

**LEARNING FROM EXPERIENCE**

While it is important for a business to be as prepared as possible in advance of a large cyber-attack using methods such as those described above, one of the best, albeit bittersweet, ways to prepare for future attacks is to learn from those which have already occurred. As part of the remediation process of a cyber incident, the incident response team, together with the legal team, should be responsible for reviewing and revisiting their approach to the incident against the incident response policy. The review should identify where the procedure worked well, and where it did not. If certain steps or requirements of the policy were found to be unnecessary, causing progress to be inefficient, or otherwise not effective, these should be flagged.

In addition to the policy, post-incident analysis is also, at times, valuable in the context of third-party vendor management. Being prepared for a cyber-attack is not achieved by simply preparing an incident response policy or conducting training. It is achieved by enterprise-wide awareness and engagement. This article sets out some examples for cyber preparedness but there are many other ways a business can prepare itself. As the risk of cyberattack continues to increase, now is the time to revisit and review existing frameworks of protection to ensure your business is truly prepared.

© 2024 Hunton Andrews Kurth LLP

**Cyber threats are increasing – are you prepared?**
By Sarah Pearce and Ashley Webber
Published in Privacy Laws & Business UK Report | May 2024

***Sarah Pearce*** *is a Partner in the firm's Global Technology, Outsourcing & Privacy group in the firm's London office. Sarah's practice covers a broad range of data privacy and data security issues in the UK and across Europe. She can be reached at +44 (0)20 7220 5722 or spearce@HuntonAK.com.*

***Ashley Webber*** *is an Associate in the firm's Global Technology, Outsourcing & Privacy group in the firm's London office. Ashley focuses her practice on all areas of UK and EU data protection, privacy and cybersecurity law. She can be reached at +44 (0)20 7220 5715 or awebber@HuntonAK.com.*

This article was published in Privacy Laws & Business UK Report, May 2024, www.privacylaws.com.

© 2024 Hunton Andrews Kurth LLP