THOMSON REUTERS

REGULATORY INTELLIGENCE

Cyber incident response: regulatory reporting and notification obligations

Published 23-Jul-2020 by
Ashurst LLP and FTI Consulting

Regardless of the size or nature of an organisation, cyber incidents are now a serious and constant threat. At some point all organisations will have to deal with some form of cyber incident and therefore adequate preparation for such an eventuality is imperative.

This article explains the key phases of a cyber incident response from a technical and practical perspective, and summarises the regulatory reporting and notification obligations which may be triggered where a cyber incident involves a personal data breach. In addition, it outlines specific reporting obligations for organisations regulated by the Financial Conduct Authority (FCA).

Cyber incident

The UK's National Cyber Security Centre (NCSC) defines a cyber incident as "a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorized access or attempted access to a system or systems".

The NCSC lists the following activities as commonly recognised breaches of a security policy:

attempts to gain unauthorised access to a system and/or to data;
unauthorised use of systems for the processing or storing of data;
changes to a system's firmware, software or hardware without the system owner's consent; and
malicious disruption and/or denial of service.

Incident response

Actions taken within the first 48 hours typically dictate how effectively an organisation will manage a cyber incident. It is important to mobilise the appropriate internal teams as soon as possible to make timely decisions, supported by external experts including technical, legal, and communications specialists.

Prior preparation and planning are essential to increase the efficiency and success of an incident response. Predicting the precise nature of potential incidents is not always possible and therefore plans must provide strategic direction and practical guidance while also facilitating an agile response where necessary.

The phases of responding to an incident can be fluid, but are typically broken down into the following five phases:

Triage

Once an incident has been detected and reported, both the incident's significance and the appropriate next steps are assessed through triaging, which aims to establish:

known impacts, such as the extent of ransomware encryption;
potential impacts, such as whether the ransomware perpetrators may publish client data to force payment;
business priorities, such as corporate stance and decision-making on ransom demands;
whether regulatory reporting and notifications obligations are triggered;
additional expertise required (e.g. external counsel, technical and communications);
immediate next steps and options (e.g. focus for forensics and containment, leverage of insurance policies); and
need for communications (internally as well as externally).

Containment

This phase focuses on ensuring that the incident does not get any worse and is contained as far as possible. From a technical perspective, this may mean isolating networks or devices that are both known and potentially affected. From a communications perspective, this means handling stakeholders and involving legal teams to assist with assessing regulatory reporting and notification obligations as well as providing advice on maintaining privilege.

Eradication

This involves an iterative process of ensuring cleanliness of infrastructure, software and data, as the cordons of containment are gradually lifted and operational teams look to identify "patient zero" (the initial infection). The process looks to ensure no technical infection or leakage. Experience also shows that this is a good time to ensure no technical "piggybacking" attacks or "persistence" (i.e. manipulation of for example administrative accounts to allow future access even after an infection has been removed) take place.

Recovery

During the recovery phase, systems are brought back up to speed and checks are made to confirm they are working normally. This typically requires a period of on-going monitoring to ensure systems are properly interacting, in particular where certain systems have been contained for a period, and any residual indicators of either targeting or compromise are identified.

During this phase, decisions about communications and assessments of regulatory reporting or notification obligations (as discussed below) will need to continue to be evaluated, as technical investigations conclude.

Learn lessons

A critical final phase of an incident response is to complete investigations and identify areas to improve future responses. For more significant breaches, which require regulatory reporting, notifications to individuals or significant insurance claims, investigations can be significant and lengthy exercises.

Personal data breach reporting and notification requirements

Throughout each of the response phases discussed above, consideration will need to be given to an organisation's regulatory reporting and notification obligations. Not all cyber incidents will involve personal data, but where personal data is involved additional obligations may arise under data protection and other sector-specific regulations. It is critical therefore to assess from the outset of the triage phase what systems and underlying data may have been compromised as a result of a cyber incident.

Under the General Data Protection Regulation 2016/679 (GDPR) and Data Protection Act 2018 organisations acting in the capacity as a "controller" of personal data may need to notify (i) a data protection supervisory authority ("SA"); and (ii) the affected individuals, in the event of a personal data breach.

A personal data breach under the GDPR is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Reporting to an SA

Controllers are required to report to an SA not later than 72 hours after becoming aware of the personal data breach "unless a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

In determining whether the reporting threshold is met, a risk assessment of the likelihood and potential severity of the impact on the affected individuals is required.

Recital 85 of the GDPR sets out that the negative impacts of a personal data breach should be considered. Examples given include: "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

The guidelines of the Article 29 Working Party on "personal data notification under Regulation 2016/679" refer to recommendations from ENISA, which set out a number of considerations when assessing the severity of the consequences of a personal data breach, such as the context of processing, the ease of identification of the affected data subject(s) and the circumstances of the breach.

Organisations will need to carefully assess and document the analysis of the impact of the personal data breach to individuals.

Notifying individuals

Notification to affected individuals is mandatory and must take place without undue delay where a personal data breach is "likely to result in a high risk to the rights and freedoms of natural persons".

This is a higher threshold than notifying an SA and requires an assessment of both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. The main objective of notification to affected individuals is to provide specific information about steps they should take to protect themselves and, therefore, it is important that the potential impact on the affected individuals is fully understood prior to any notification.

Other potential reporting obligations

For organisations regulated by the FCA, a personal data breach may also need to be reported to the FCA under FCA Principle 11, which requires disclosure of anything relating to an organisation which its regulators would reasonably expect notice of.

Under FCA Principle 11, an organisation must notify the FCA immediately if it becomes aware of, or has information which reasonably suggests, that any of the following has occurred, may have occurred, or may occur in the foreseeable future:

any matter which could have a significant adverse impact on the organisation's reputation;
any matter which could affect the organisation's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the organisation; or
any matter in respect of the organisation which could result in serious financial consequences to the UK financial system or to other organisations.

Cyber resilience guidance (Resilience Guidance) published by the FCA clarifies that a material cyber incident must be reported under FCA Principle 11 and advises that an incident may be material if it: "results in a significant loss of data, or the availability or control of your IT systems; affects a large number of customers; or results in unauthorised access to, or malicious software present on, information and communication systems."

The FCA also notes in the Resilience Guidance that dual-regulated organisations should also contact the Prudential Regulation Authority when making a notification under FCA Principle 11.

Closing remark

It is no longer a question of if, but when a cyber incident will occur. Understanding regulatory reporting obligations and early incident response preparation are crucial not only to ensuring compliance with legal obligations but also to managing operational and reputational impacts.

Gita Shivarattan, counsel, Jake Green, partner and Tom Brookes, associate at Ashurst LLP. Paul Reilly, managing director and Patrick MacGloin, partner at FTI Consulting

Complaints Procedure

Produced by Thomson Reuters Accelus Regulatory Intelligence 23-Jul-2020