Chapter 2

Types of cyber incidents and losses

This chapter provides an overview of the different types of cyber incidents, based on a categorisation approach developed by the CRO Forum, as well as the types of losses that may result from these incidents. Where available, data is presented on the magnitude of losses from past incidents including trends in the magnitude of losses and some of the drivers of cost variations across different countries (such as differences in terms of notification requirements).

There is significant literature on the nature and evolution of cyber risk as well as the magnitude of potential costs - although limited consensus in terms of definitions, categorisation or the reliability of the data that has been made available on the frequency and impact of cyber incidents. For example, there is no prevailing definition of cyber risk or prevailing taxonomy for categorisation of different types of incidents and losses.

Much of the data that is publicly available on cyber incidents and costs is provided by security and consulting firms and is perceived by some as potentially biased due to the commercial incentives that these firms may have to inflate the significance of cyber risk. For example, Romanosky (2016), using data collected mostly by Advisen, questions a number of commonly cited statistics and trends including the typical cost of a third party confidentiality breach, the share of companies that have been impacted by cyber incidents and the rise in the relative share of incidents that are malicious relative to accidental.

Conversely, the lack of reporting of cyber incidents by affected companies (particularly certain types of cyber incidents) have led some to suggest that the publicly available data underestimates the true significance of cyber risk. In the United Kingdom, for example, a recent survey found that only 26% of respondents had reported their most serious breach incident to an external party (of which only 19% of those that reported their most serious breach incident reported it to police and only 8% to customers) (Department for Culture, Media and Sport, 2017). Other estimates suggest that 60% to 89% of incidents are likely to be unreported (Edwards et al., 2014). While it is difficult to know which tendency may be stronger - it is clear that "existing cost estimates are far from perfect" (The Geneva Association, 2016).

A description of the main categories of incidents and losses, based on definitions and a taxonomy developed by the insurance sector, is included in Box 2.1. This is followed by a description of the types of incidents that could be included under each category and some illustrative examples and data, where available (which are also summarised in
Figure 2.6 at the end of this chapter). The purpose of this overview is to provide context for the subsequent sections of the report and support a better understanding of the range of potential incidents and how these incidents can translate into costs that can be transferred to insurance markets. It should not be interpreted as providing a comprehensive taxonomy of cyber incidents or a measure of the impacts of cyber incidents (which are beyond the scope of this report).

**Box 2.1. Definitions and categorisation of cyber incidents and losses**

**Definition of cyber risk**

Neither a standard definition of cyber risk nor a common definition used broadly within the insurance sector currently exist. A couple of definitions have been put forward by associations of insurance companies:

- A group of insurance company Chief Risk Officers (CRO Forum, 2014) has defined cyber risk as encompassing: "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks".
- The Geneva Association (2016), an international insurance think tank whose members include large insurance and reinsurance companies, has suggested a similar definition: "any risk emerging from the use of information and communication technology that compromises the confidentiality, availability, or integrity of data or services."

Both of these definitions broadly define cyber risk to include risks related to the use of information and communications technologies, which could include both risks related to human error as well as intentional/malicious attacks, whether generated by internal or external parties (nation states, terrorists, industrial competitors, organised crime, hacktivists or lone hackers/criminals). The Geneva Association (2016) definition usefully narrows the scope of cyber risk to incidents that lead to a compromise of data or service, which captures the types of incidents that are normally considered as within the potential scope of cyber insurance coverage.

**Types of cyber incidents**

There are a number of different possible approaches to categorising the different types of incidents. For the purposes of this study, the categorisation developed by the CRO Forum (2016) is used which includes four broad categories: (i) data confidentiality [breach]; (ii) system malfunction/issue; (ii) data integrity/availability; and (iv) malicious activity. These categories are described in the sections below, including examples of real-life (where existing) or hypothetical scenarios as well as any available data on the frequency or impacts of incidents for each category. It should be noted that the CRO Forum (2016) taxonomy is evolving based on an evaluation of an ongoing incident reporting exercise (see Chapter 5) and an effort to incorporate metrics commonly used for threat and security incident reporting ("VERIS" and "STIX").

**Types of cyber losses**

Cyber incidents can potentially lead to a number of different types of losses, including damages to tangible and intangible assets, losses related to business disruption and theft, as well as various forms of liability to customers, suppliers, employees and shareholders (amongst others). The CRO Forum (2016) has developed a set of "incident type groups" that provides a useful categorisation of the different types of losses that could be incurred as a result of cyber incidents. The categories of losses put forward by the CRO Forum are described in Table 2.1.

<table>
<thead>
<tr>
<th>CRO Forum (2016) &quot;Incident Type Group&quot; (loss types)</th>
<th>CRO Forum (2016) &quot;Coverage Scope&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business interruption interruption of operations</td>
<td>Reimbursement of lost profits caused by a production interruption not originating from physical damage.</td>
</tr>
<tr>
<td>Contingent business interruption (CBI) for non-physical damage</td>
<td>Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage.</td>
</tr>
<tr>
<td>Data and software loss</td>
<td>Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted or encrypted.</td>
</tr>
<tr>
<td>Incident Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Financial theft and/or fraud</td>
<td>Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g. shares). It covers both pure financial losses suffered by the observed company or by related third parties as a result of proven wrong-doing by the observed company.</td>
</tr>
<tr>
<td>Cyber ransom and extortion</td>
<td>Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g. access to data is locked until ransom is paid).</td>
</tr>
<tr>
<td>Intellectual property theft</td>
<td>Loss of value of an intellectual property asset, resulting in pure financial loss.</td>
</tr>
<tr>
<td>Incident response costs</td>
<td>Compensation for crisis management/remediation actions requiring internal or external expert costs, but excluding regulatory and legal defence costs. Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences costs; (ii) public relations and communications costs; (iii) remediation costs (e.g. costs to delete or cost to activate a &quot;flooding&quot; of the harmful contents published against an insured); (iv) notification costs.</td>
</tr>
<tr>
<td>Breach of privacy [compensation]</td>
<td>Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incident response costs.</td>
</tr>
<tr>
<td>Network security/security failure [liability]</td>
<td>Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network, but excluding incident response costs. The policyholder/observed company may not have any damage but has been used as a vector or channel to reach a third party.</td>
</tr>
<tr>
<td>Reputational damage (excluding legal protection)</td>
<td>Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company.</td>
</tr>
</tbody>
</table>
| Regulatory & legal defence costs (excluding fines and penalties) | A: Regulatory costs: compensation for costs incurred to the observed company or related third-parties when responding to governmental or regulatory inquiries related to a cyber attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties).  
B: Legal defence costs: coverage for own defence costs incurred to the observed company or related third parties facing legal action in courts following a cyber attack. |
| Fine and penalties                                     | Compensation for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed. |
| Communication and media [liability]                   | Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel or slander of third parties including web-page defacement as well as patent/copyright infringement and trade secret misappropriation. |
| Legal protection - Lawyer fees                         | Costs of legal action brought by or against the policyholder including lawyer fees and costs in case of trial (e.g. identity theft, lawyer costs to prove the misuse of victim's identity). |
| Assistance coverage - psychological support            | Assistance and psychological support to the victim after a cyber event leading to the circulation of prejudicial information on the policyholder without his/her consent. |
| Products [liability]                                   | Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber event, excluding technical products or operations (Technology errors and omissions) and excluding Professional Services errors and omissions. |
| Directors and officers (D&O) [liability]               | Compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber event. |
| Technology errors and omissions (E&O) [liability]      | Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber event. |
| Professional services errors and omissions (E&O)/Professional indemnity [liability] | Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber event, excluding technical services and products (Technology errors and omissions). |
| Environmental damage                                   | Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber event. |
| Physical asset damage                                  | Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber event at this company. |
| Bodily injury and death                                | Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g. sensitive data leakage leading to suicide). |

Note: The classification described in this report involves an interpretation of the CRO Forum categorisation which may not reflect what was intended by those that designed the classification.

Source: CRO Forum (2016)
Data confidentiality

Incidents involving the compromise of confidential data (also commonly referred to as "data breaches") are among the most common forms of cyber incidents. The CRO Forum (2016) classification sub-divides data confidentiality incidents into two types: (i) incidents involving own confidential data (e.g. financial data, trade secrets, intellectual property); and (ii) incidents involving third party confidential data (e.g. customers' personal information). Usefully, the classification of an incident in this category is based on the detection by a company of the confidential data "outside of its data perimeter" rather than the specific incident that led to the unauthorised release of data. This means that the scope of this category includes the many different underlying causes of the release of confidential data, ranging from improper disposal of company records to unauthorised access to a company's internal networks (often referred to as a "network security breach").

The release of confidential data through employee error (e.g. through the loss or improper disposal of a portable device containing confidential data) has historically been the most common form of data confidentiality incidents (and still accounted for 25% of all "data breaches" in 2016 according to some sources (Ponemon Institute, 2017)). However, incidents caused by malicious attacks have accounted for an increasing share of data confidentiality incidents, particularly as encryption of portable devices has become more common (reducing the risk of confidential data releases from lost portable devices and therefore the share of all incidents involving employee error) (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). Malicious attacks aimed at compromising data confidentiality would normally be motivated by financial gain (e.g. the sale of personally-identifiable information or the sale and/or exploitation of trade secrets) but could also be driven by political or social motivations, such as the desire to harm a company (e.g. the data confidentiality breaches at Ashley Madison and Sony Pictures) or political party (e.g. the data confidentiality breaches that affected the United States’ Democratic National Committee and Emmanuel Macron’s presidential campaign in France).

Third-party data confidentiality breaches

Most publicly reported breaches of data confidentiality have involved the loss or theft of third party data, and particularly personally-identifiable information (Gemalto NV, 2016). A data confidentiality incident involving third-party personal data is more likely to be reported than other types of data confidentiality incidents due to the notification requirements imposed in many jurisdictions related to the release of personal information (see Box 2.2). However, the availability of data (particularly comparable data) on data confidentiality incidents remains limited (even in countries with notification requirements) - resulting in uncertainty even in terms of whether the number of such incidents is increasing or remaining stable. Some reports have found a general upward trend in the number of reported incidents and the records exposed (see Figure 2.1) although there are other reports of a decline in such incidents in recent years (particularly serious incidents) - potentially attributable to the implementation of effective prevention measures and/or the declining black market value for some types of personally-identifiable information (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). One recent analysis found a measurable decline in the frequency of smaller (less than 100 000 records) data confidentiality breaches and a small decline in the frequency of larger incidents (for 2016 only) (Risk Management Solutions, Inc. and
Cambridge Centre for Risk Studies, 2016). However, for respondents to the OECD questionnaire, the existence of a black market for this type of information remains one of the most important factors driving the overall level of cyber risk.

Figure 2.1. Third party data confidentiality breach incidents and exposed records

Third party data confidentiality incidents involving the loss or theft of personally-identifiable information are most common in sectors that collect such information, such as health care, financial services, educational institutions, retail and the public sector (Identity Theft Resource Center, 2016; Howard and Gulyas, 2014) although there has been a significant recent decline in the frequency of incidents in the financial services sector, potentially as a result of increasing investment in security and data protection (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017). A particular target are companies that process debit and credit card payments through point-of-sale (POS) terminals that collect and transmit details on payment cards and PIN codes. Healthcare providers were also becoming an increasingly significant target due to an increase in the black market value of health care records relative to other types of records. However, there has been a recent shift in the types of incidents affecting health care organisations away from data confidentiality breaches towards cyber extortion (such as the recent WannaCry ransomware attack in May 2017 which widely affected the United Kingdom’s National Health System - see Box 2.8).
Box 2.2. Notification and disclosure requirements and related fines and penalties

Data confidentiality breaches involving unauthorised access to personally-identifiable information may be subject to notification and/or disclosure requirements (either to a regulator or to those affected) and fines and penalties in several countries:

* In the **United States**, there are prompt notification requirements established at the state-level in all but three states as well as federal privacy requirements that require notification (to regulators and affected individuals) if health or financial information is stolen (*Health Insurance Portability and Accountability Act* and *Graham-Leach-Bliley Act*, respectively). The requirements in 36 states as well as the federal requirements related to health information allow for the respective authorities to impose penalties on organisations for the release of that information. In addition, regulatory actions can be brought by a number of federal and state agencies, including the Federal Trade Commission and state Attorney Generals (Allianz Global Corporate & Specialty, 2015). The US Securities and Exchange Commission (SEC) requires disclosure by public companies of cyber incidents, where an incident is "reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition" and where an incident is likely to "materially affect a registrant’s products, services, relationships with customers or suppliers, or competitive conditions" (SEC, 2011). Data breach incidents could be included within the scope of this disclosure requirement although a number of significant breaches have not been disclosed by public companies (Tsukayama, 2016).

* In the **European Union**, notification requirements are currently less prevalent although there are potential notification requirements in some sectors. The *Payment Services Directive 2*, for example, allows for the possibility of public ("payment service user") notification in cases where "an incident has or may have an impact on the financial interests of its payment service users". There are also notification requirements related to incidents that are operationally disruptive to critical services (see the section below on system malfunction). This will change as a result of the General Data Protection Regulation (GDPR) (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data*) which will come into effect in May 2018 and will include more generalised notification requirements. The GDPR will require prompt notification to the supervisor in cases where there is a risk to the "rights and freedoms of data subjects" (and to affected individuals if there is a high-risk) and will impose administrative fines in the case of breaches that are deemed intentional or involving negligence (Steptoe and Johnson LLP, 2016).

* In **Australia**, **Canada** and **Japan** fines may be imposed although only in the context of non-cooperation with an investigation or non-compliance with a specific order (BakerHostetler, 2015) (although, in Australia, changes to privacy legislation will lead to broad notification requirements and the potential for penalties of up to AUD 1.8 million for "serious or repeated interferences with the privacy of an individual" to be imposed by federal courts (Lui, 2017)). In Japan, financial sector businesses are required to notify the supervisory authority of data breaches while companies in other sectors may be required to notify supervisory authorities, depending on the nature of the data breach, the type of data involved and the number of data subjects affected, along with other relevant factors. In **Singapore**, the *Personal Data Protection Act* introduced requirements for the protection of personal data that is collected and fines of up to SGD 1 million can be imposed (Allianz Global Corporate & Specialty, 2015). An amendment to the **Republic of Korea**'s *Personal Information Protection Act* allows for fines of up to KRW 100 million (and a prison sentence of up to ten years) (PwC, 2016). **Mexico** also imposes monetary penalties related to violations of the *Ley Federal de Protección de Datos Personales en Posesión de Particulares* (Federal Law on the Protection of Personal Data held by Private Parties).
Data confidentiality breaches involving third party (personal) data can lead to different types of losses, including (in particular) data and software losses, incident response costs, breach of privacy compensation, reputational damage, regulatory and legal defence costs, fines and penalties, legal protection - lawyer fees and directors and officers (D&O) liability. In its 2017 Cost of Data Breach Study (based on estimates from the 419 companies that participated in its annual survey), the Ponemon Institute (2017) estimates that the average total cost (excluding breach of privacy compensation) of a data breach incident (defined as a breach which puts an individual's name and either a health or financial record at risk; i.e. a third party data confidentiality breach) to a company was USD 3.62 million (down from USD 4.0 million in 2016). This is generally consistent with the findings of a 2015 annual survey of companies in the United Kingdom which estimated that the cost of addressing the worst breaches impacting large companies ranged from GBP 1.5 million to GBP 3.14 million (Department for Business, Innovation and Skills, 2015) and with estimates by Verizon of an average cost range of between USD 5 million and USD 15.6 million for large privacy breaches (100 million records or more) (Verizon, 2015). The average cost of data breaches varies significantly across countries, ranging from USD 1.52 million to USD 1.68 million in India and Brazil to USD 4.31 million in Canada and USD 7.35 million in the United States (as cost is significantly affected by notification requirements, penalties and compensation practices, as described below) (Ponemon Institute, 2017).

The limited available data on cyber insurance claims identifies an average cost (i.e. sum of claims paid and self-insured retention) of USD 650 000 to USD 675 000, although with higher average costs in certain sectors such as retail, health care and financial services and among large companies (USD 4.8 million to USD 5.9 million for companies with USD 10 billion to USD 100 billion in revenues) (NetDiligence, 2015; NetDiligence, 2016).

An important driver of the differences in cost across countries and sectors is differences in the legal frameworks related to privacy protection. As an illustration of this, data breach claims incidents account for close to 90% of all insurance claims in the United States (NetDiligence, 2015; NetDiligence, 2016) where notification requirements are widespread but were found to account for less than 25% in Europe (AIG, 2016). The major components of the costs of a third party data confidentiality breach across jurisdictions are:

- **Fines and penalties**: As noted in Box 2.2, a number of jurisdictions may impose fines and penalties as a result of a data confidentiality breach involving personally-identifiable information. The magnitude of these fines varies by jurisdiction and sector. In the United States, organisations affected by a data confidentiality breach involving health records have been fined as much as USD 5.5 million (Department of Health and Human Services, 2017). In Europe, the scope of potential fines and penalties currently varies across member states. For example, in the United Kingdom, the Information Commissioner's Office can issue fines for up to GBP 500 000 (Information Commissioner’s Office, 2015). The GDPR, effective in May 2018, will allow for fines of up to EUR 20 million or 4% of worldwide annual turnover (whichever is greater) and will apply to all entities that process personal data of EU citizens.

- **Incident response costs**: In some jurisdictions (notably, the United States), individuals affected by a data confidentiality breach must be notified that their personal information has been compromised, particularly when there is a risk that
the release of that information could cause harm. Notifying individuals can be costly (on average, 5% of total costs - see Figure 2.2), especially in the case of breaches that affect large numbers of individuals. In addition, affected organisations are likely to incur public relations and communications costs once the data confidentiality breach is made public. An analysis of the breakdown of costs related to data confidentiality breach claims in the United States found that 75% (USD 375 000, on average) of costs incurred were related to "crisis services" including forensic investigations, notification costs, public relations (as well as credit/identity theft monitoring which is classified in this study as breach of privacy compensation) (NetDiligence, 2016). A report by a legal firm that supports US companies in responding to third party data confidentiality breaches found that a forensic investigation was undertaken in approximately one third of incidents at an average cost of USD 102 806 (BakerHostetler, 2016).

Figure 2.2. **Breakdown of data confidentiality breach costs by type (2015)**

Source: Ponemon Institute (2015). Losses resulting from a data confidentiality breach are classified in the study as: (i) "Ex-post response costs" which includes some components of breach of privacy compensation costs (credit-watch services) and incident response costs (public relations and communications costs and remediation costs) as well as regulatory and legal defence costs and fines and penalties; (ii) "notification costs" which include incident response costs related to informing customers that their information has been compromised; (iii) "lost business" which includes both the disruption to business that directly results from responding to the event (i.e. business interruption) as well as the loss in revenue resulting from reputational damage after the event; and (iv) "detection and escalation" which includes the IT investigations and forensic analysis component of incident response costs. Large breaches (involving more than 101 000 compromised records) are excluded from the scope of the study.

- **Reputational damage**: Where data confidentiality breaches are made public, affected organisations may face a loss of profits due to a loss of confidence in the company among its customers (see Box 2.3). The Ponemon Institute (2015) found that, on average, the most significant costs for organisations affected by data confidentiality breaches are due to lost business (abnormal customer turnover, increased customer acquisition costs, reputation losses). However, there is some evidence that the reputational impacts of a data confidentiality breach may be declining (or may be lower than expected). An analysis by PCS (an insurance claims data provider) of 12 major US data confidentiality breaches found that companies did not always face a share price decline after the disclosure of an
incident and that the impact on share prices have declined over time (Artemis, 2017). A 2014 study on consumer responses to companies affected by data confidentiality breaches found that 44% of respondents would end or reduce their business relationship with a company affected by a data confidentiality breach (where informed by media coverage) although 71% of those actually affected by an incident maintained their business relationship with the affected company, mainly because of a lack of alternatives or the perception that most companies are affected by such incidents (Ponemon Institute, 2014).

Box 2.3. The implications of lost business: Target data confidentiality breach

In the fourth quarter of 2013, Target, a major US retailer, discovered a significant data confidentiality breach that led to the theft of approximately 40 million payment card records (along with 70 million other information records such as addresses and phone numbers) (Phillips, 2014). As of 30 January 2017, the company had reported USD 292 million in incurred expenses as a direct result of the privacy breach, including settlements with four major payment card networks, affected customers and financial institutions (as issuers of the payment cards). In May 2017, the company reached a USD 18.5 million settlement with numerous US State Attorneys General that had launched investigations into the breach (Hurtado, 2017).

While the direct expenses incurred were significant, the company also faced an initial decline in sales and shareholder returns in the aftermath of its data breach disclosure. Subsequent growth in sales and shareholder returns also lagged behind the performance of its peers, suggesting that the company may have faced longer-term reputational damage as a result of the incident (see Figure 2.3).

Figure 2.3. The business impact of a major data confidentiality breach

- **Breach of privacy compensation:** Individuals (and organisations) whose information has been affected by a data confidentiality breach may seek compensation from the organisation that was breached, usually based on a contractual obligation of the company to protect that data (either explicit or implicit) (Alder, 2015). Some privacy and data protection legislation may also explicitly establish (or reaffirm and/or define) private rights of action to seek
compensation (e.g. European Union member states through the GDPR, some
Canadian provinces). With the implementation of the GDPR, companies operating
in Europe will be liable for breaches of confidential data for which they have
responsibility, even if the source of the breach was a third party. There is a strong
expectation among consumers that companies will provide some compensation if
the personal data that they have collected is compromised. A 2014 study found that
between 58% and 67% of respondents in the United States expected some
combination of monetary or in-kind compensation, identity theft insurance or credit
monitoring services from a company affected by an incident (Ponemon, 2014) and
many companies will provide this type of compensation or services.²

The most common forms of compensation provided by companies to those
affected by data confidentiality breaches are credit monitoring services and
identity theft protection.³ In many cases, those affected by a data confidentiality
breach will also seek monetary compensation although this would normally
require a demonstration that they have been harmed as a result of the breach (e.g.
that their identity has been stolen and their credit or reputation has been
negatively affected as a result).⁴ In practice, breached companies and/or their
insurers have reached settlements with affected consumers in order to avoid a
costly legal process with an uncertain outcome, particularly in jurisdictions
where collective redress actions are permitted.

In the United States and Canada, individuals affected by a release of their
personal information may cooperate through a class action lawsuit to seek
compensation (although class action lawsuits have been less successful in Canada
due to more stringent requirements and because the right of action only arises
after a full investigation by the Privacy Commissioner (BakerHostetler, 2015)).
According to an analysis of third party data confidentiality breaches by a legal
firm providing response services in the United States, litigation resulted from
only 6% of all incidents involving the company's response services
(BakerHostetler, 2016) while available claims data found that legal settlements
accounted for approximately 10% of costs incurred (with legal defence
accounting for a further 3%) (NetDiligence, 2016). Where class actions have
been pursued, the average settlements ranged from USD 0 to USD 13.63 per
person with a tendency towards higher amounts for breaches involving personal
health information, lower numbers of claimants and fewer non-cash benefits
(such as identity theft monitoring) (Phillips et. al, 2017). However, there have
been a number of cases where settlements (or amounts sought) have been outside
that range, including:

- the theft of 45 million payment card records from TJ Maxx (a US retailer) in
  2007 led to reported settlements with customers of USD 11 million
  (equivalent to approximately USD 30 per claimant with evidence of
documented losses) (Insurance Information Institute, 2014);

- a 2013 lawsuit related to the theft of medical records sought damages of
  USD 1 000 and 10 000 per person under health privacy legislation in
  California (Aschkenasy, 2013); and

- in a recently settled class action suit related to the breach of data at Anthem,
  an alternative settlement of USD 50 per person was agreed to for individuals
  who did not want to enrol in the services offered as part of the settlement
  (MacLean, 2017).
Consumer class actions are less common (and more restricted) in the United Kingdom and continental Europe. In continental Europe, consumer class actions (collective redress) are possible although affected consumers can only be represented by a qualifying non-profit consumer association (rather than a fee-earning law firm as in the United States and Canada). In addition, in some European members states (e.g. France and Germany), collective redress actions related to data protection will only allow injunctive relief (i.e. corrective action), not compensation for damages (Swiss Re, 2017). The GDPR will leave it to member states to determine whether to maintain these restrictions or allow for compensation for damage awards. In the United Kingdom, collective redress actions are not restricted to consumer associations and it is possible to seek compensation for damages suffered (i.e. not just injunctive relief). A 2015 Court of Appeal ruling allows individuals to bring claims for distress without having to demonstrate that a financial loss has occurred (De Freltas, 2016). A June 2016 settlement awarded GBP 2,500 to GBP 12,500 per person to asylum seekers whose personal information was released (Swiss Re, 2017).

In the particular case of data confidentiality breaches involving payment card details, specific (contractual) penalties may be imposed by the operators of payment card networks on the basis of contractual obligations where non-compliance with the requirements of the Payment Card Industry Data Security Standard was a causal factor (Goodman, 2016). Fines for non-compliance with the standard range from USD 5,000 to USD 50,000 (BakerHosteler, 2016). In addition, an acquirer (retailer) that suffers a breach involving payment card information may face assessments (or legal action) by the entities that issued the payment cards (or the payment card networks acting on their behalf) to cover the costs of re-issuing cards and covering any losses due to fraudulent use of the affected payment cards. These costs can be substantial with one study finding costs that range from USD 7 to USD 65 per set of card information (with an average of USD 30) (BakerHosteler, 2016). For example, the theft of 1.5 million payment card records from Global Payments Inc. in 2012 led to USD 35.9 million in fraud losses, fines and other charges (i.e. fines and assessments) expected to be imposed by the payment card networks (Information Security Media Group, 2013). The massive breach of payment card information (up to 100 million cards) at Heartland Payment Systems in 2007 led to over USD 100 million in assessments/settlements with the payment card networks (see Table 4.1). Target's assessment/settlement with Visa (on behalf of issuing financial institutions) was reported to be up to USD 67 million (Insurance Information Institute, 2014). According to a study of insurance claims paid in the United States, Payment Card Industry (PCI) fines and assessments were incurred in 5% of insured incidents and involved average insurance payouts of just under USD 500,000 and up to USD 3 million (NetDiligence, 2016).

The magnitude of losses from a data confidentiality breach also varies significantly by sector. Highly-regulated sectors (including sectors faced with specific notification requirements) incur higher costs per stolen record than less regulated sectors and the public sector (although this could also be due to better reporting of breaches in highly-regulated sectors). In 2016, the total reported cost per stolen record averaged USD 380 in the health sector, USD 245 in the financial sector and USD 200 in the education sector compared to USD 71 for records stolen from the public sector (Ponemon Institute, 2017). However, this figure varies substantially based on the country as well as the total size of...
the data confidentiality breach. Breaches above 101 000 records are excluded from the Ponemon Institute estimates and would generally involve a lower cost per stolen record given that some costs are fixed (as low as USD 5 per record in some cases (Sclafane, 2015)). For example, the cost per stolen record of a breach involving more than 50 000 records is significantly less\(^6\) than the cost per stolen record of a breach involving less than 10 000 records (Ponemon Institute, 2017). Some examples of the reported costs of selected data confidentiality breaches are provided in Table 2.2.

**Table 2.2. Costs of data confidentiality breaches: selected examples**

<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
<th>Reported costs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Equifax</strong></td>
<td>On 7 September 2017, Equifax, one of the largest credit reporting bureaus in the United States, reported that the names, addresses, social security numbers, birth dates and some driver license numbers of 143 million individuals in the United States (along with some personal information for residents of Canada and the United Kingdom) had been breached. In addition, credit card numbers for approximately 200 000 individuals were also accessed.</td>
<td>• In the five trading days following the disclosure, the company lost USD 3.5 billion in market value (Reuters, 2017) and the stock price remained 30% down at the end of September (Petterson, 2017). • The company is expected to face multiple state and federal investigations into the breach (Basak and Surane, 2017). In addition, at least 100 lawsuits had been filed including consumer class actions, a securities class action and also multiple lawsuits by municipal authorities (Reuters, 2017; Petterson, 2017). In many cases, the company was accused of violating its responsibility under the Fair Credit Reporting Act to keep the information it collects private. The company has agreed to provide credit monitoring services to all US consumers for a period of one year (the company is a provider of such services). The potential cost of settling the consumer lawsuits is estimated at USD 200 million (Petterson, 2017). The data confidentiality breach has also led to new regulatory proposals related to the protection of information by credit reporting bureaus (Insurance Journal, 2017a; Insurance Journal, 2017b). • Several senior executives (including the Chief Executive Officer) have resigned or taken early retirement and some reports suggest that a clawback of executive compensation is being considered (Advisen, 2017c; McCrank, Voltz and Mukherjee, 2017). • The company reportedly has USD 100 million to USD 150 million in stand-alone cyber insurance coverage (Basak and Surane, 2017).</td>
</tr>
<tr>
<td><strong>Yahoo</strong></td>
<td>In 2016, Yahoo disclosed two separate breaches involving approximately 1 billion and 500 million users in 2013 and 2014, respectively (with some accounts affected by both incidents). The incidents involved a breach of confidentiality of names, email addresses, telephone numbers, dates of birth as well as encrypted or partial information on passwords and security questions and answers. In October 2017, Yahoo reportedly increased its estimate of the number of users affected to 3 billion (all of its users at the time of the breach) (Harrison, 2017).</td>
<td>• A decline in the acquisition price of the company of USD 350 million relative to an offer made prior to the disclosure of the breaches (The Associated Press, 2017). • As of March 2017, the company had reportedly incurred USD 16 million in direct costs in response to the breaches (Goel, 2017). • Investigations with potential penalties have been launched by the Securities and Exchange Commission and the Federal Trade Commission (The Associated Press, 2017). • The company faces 43 consumer class action lawsuits as a result of the breaches (Goel, 2017). • A shareholder lawsuit was filed in January 2017 seeking compensation for the loss in share value (and loss in acquisition value) resulting from the data confidentiality breach (Lacroix, 2017). • The company’s CEO did not receive a USD 2 million cash bonus or a share bonus with a USD 12 million approximate value (Goel, 2017). • The company’s CEO did not receive a USD 2 million cash bonus or a share bonus with a USD 12 million approximate value (Goel, 2017).</td>
</tr>
</tbody>
</table>
| **TalkTalk** | In October 2015, TalkTalk, a UK telecommunications company, disclosed that the personal information of more than 156 000 customers (names, addresses, dates of birth and contact information) had been breached. Among the affected customers, more than 15 000 also had their bank account information accessed. | • In its 2016 Annual Report, the company reported exceptional costs of GBP 42 million attributable to the data breach, including direct incident response costs and customer management costs including additional call centre agents, communication and marketing costs, restoration with enhanced security features and increased retention costs including the cost of providing free upgrades. The company reported that the cost of credits to retain customers was approximately GBP 3 million (TalkTalk Group, 2016). • The company’s pre-tax profits fell to GBP 14 million in the year ending **ENHANCING THE ROLE OF INSURANCE IN CYBER RISK MANAGEMENT © OECD 2017**
<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
<th>Reported costs</th>
</tr>
</thead>
</table>
| Ashley Madison | In July 2015, a hacker group made a public claim that it had accessed confidential data on clients of Ashley Madison, a Canadian online dating website targeting people in relationships with others, and threatening to release the data unless the website was shut down. In August and September 2015, the hackers published names, usernames, encrypted passwords, addresses and phone numbers of 32 million Ashley Madison clients. | March 2016 relative to GBP 32 million in the previous period (Rodionova, 2016). Total revenue growth fell to 0.2% in the second half of fiscal year 2015 from 4.7% in the first half of the fiscal year, partly as a result of the data breach (TalkTalk Group, 2016). The company attributed a loss of 95 000 broadband customers to the data breach incident (TalkTalk Group, 2016) and may have lost 250 000 customers overall (IDT911, 2016).  
- Executive directors annual bonuses were reduced from 6.4% to 4.0% of base pay as a result of the data breach incident (TalkTalk Group, 2016)  
- The company was fined GBP 400 000 by the UK Information Commissioner's Office for failing to take appropriate measures to protect personal data (Rodionova, 2016).  
- There were reports that customer information was used in subsequent phishing attacks that led to the disclosure of banking details and the transfer of funds from their bank accounts. At least one law firm was examining whether there was cause for seeking compensation from the company on behalf of affected customers (Leigh Day, 2016).  
- The company reportedly had USD 100 million in insurance coverage against cyber attacks (Advisen, 2017b).  
- The company also reportedly faced a CAD 578 million lawsuit from its customers (Lord, 2016). It settled a US class action lawsuit involving approximately 37 million affected users for USD 11.2 million in July 2017 which provides users with up to USD 3 500 depending on documented losses (Stempel, 2017) |
| Anthem       | In February 2015, Anthem (health insurance provider) disclosed that an unauthorised access had allowed hackers to obtain various types of personal information, including names, birthdays, health care identification/social security numbers, street addresses, email addresses, phone numbers and employment information, including income data. According to the company, there was no evidence that financial or health-related information was obtained. The incident reportedly affected 78.8 million “members” (i.e. insureds) and employees (Herman, 2016). | The company reportedly spent USD 12 million initially on forensic investigation and remediation costs, including an assessment of needed cybersecurity enhancements. The company invested a further USD 130 million in 2015 and 2016 to improve its level of protection against cyber attacks (Advisen, 2017b).  
- The company indicated that they are providing credit monitoring and identity protection services to those affected (reportedly for two years) and that they have incurred expenses related to forensic investigation and remediation.  
- In its most recent Annual Report (Anthem Inc., 2017), the company indicated that there were ongoing investigations by various state and federal regulators that could lead to fines. In June 2017, the company reportedly agreed to a USD 115 million settlement to resolve consumer claims from the breach (MacLean, 2017).  
- The company reportedly had USD 100 million in insurance coverage although reports suggest that this amount was unlikely to cover more than the cost of notification and credit monitoring (Osborne, 2015). |
| JP Morgan Chase | In September 2014, JP Morgan Chase (US bank) disclosed that the confidential information of 83 million clients (76 million individuals/households and 7 million small businesses) had been accessed, including names, addresses, phone numbers and email addresses (not usernames, passwords or financial information). | The company indicated that it has increased its investment in cybersecurity defences from USD 250 million per year in 2014 to an expected USD 600 million per year in 2016 (JP Morgan Chase & Co., 2016).  
- Investigations by government agencies were reported although there is no indication that fines or penalties were imposed.  
- According to one report, credit monitoring services were not offered to affected customers (as only contact information had been breached and the company reported no increase in fraudulent activities) (Kerner, 2014b). |
<p>| eBay         | In May 2014, eBay (a US online retailer) disclosed a breach involving all of its 145 million users. The company’s network was accessed by an unauthorised party using employee credential(s) and led to a breach of the confidentiality of username and encrypted passwords as well as | The company reported reduced activity among its users and reduced its revenue projections for 2014 by USD 200 million after the disclosure of the breach (i.e. from USD 18.0 to USD 18.5 billion range after Q1 to USD 18.0 to USD 18.3 billion range after Q2) (Drinkwater, 2014). |</p>
<table>
<thead>
<tr>
<th>Incident</th>
<th>Description</th>
<th>Reported costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea Credit Bureau</td>
<td>In January 2014, it was reported that a contractor working for the Korean Credit Bureau, a private organisation that manages credit information for financial institutions, had stolen 105.8 million personal information records from three issuing banks involving the confidential personal information of 20 million individuals. The stolen information, which included credit card numbers and validation dates, credit ratings, resident registration numbers, and contact details (but not passwords or personal identification numbers) was sold to marketing firms.</td>
<td>In its Q2 investor relations calls, the company reported a 1.9% decline in operating margin that was attributed to expenses related to the breach incident (and subsequent investments in network security improvements) (Kerner, 2014a). As of 31 January 2017, eBay had received information requests from various regulatory and other government agencies although no payments of fines or penalties had been disclosed. A putative class action lawsuit had been filed against the company in July 2014 although was dismissed (with leave to amend) (eBay Inc., 2017).</td>
</tr>
<tr>
<td>Sony Play Station Network</td>
<td>In May 2011, Sony disclosed that some personally identifiable information from each of its 77 million Play Station Network (video game) user accounts had been breached, including usernames, passwords, email addresses, home addresses and some credit card information in encrypted form.</td>
<td>A class action lawsuit was reportedly filed on behalf of 130 cardholders seeking KRW 110 million in compensation per victim (Lee, 2014). Within the first two weeks after the disclosure of the breach, 2.28 million requests for cancellation and 3.84 requests for reissuance of the affected credit cards were made (Kim and Cha, 2014). The Financial Supervisory Commission fined the three issuing banks whose cardholders were affected (KB Kookmin Bank, Lotte Card and NH Nonghyup Card) KRW 6 million each and banned them from issuing new credit cards for three months (Vaas, 2014).</td>
</tr>
<tr>
<td>Heartland Payment Systems</td>
<td>In 2009, Heartland Payment Systems (US payments processor) disclosed that confidential payment card (debit and credit) information had been breached for up to 100 million cards issued by more than 650 financial services companies. The information that was accessed reportedly did not include unencrypted personal identification numbers or cardholder social security numbers or contact details (McGlasson, 2009)</td>
<td>The company provided USD 1 million in identity theft insurance protection for each user. In late May 2011, the company estimated that it would incur USD 171 million in costs for the identity theft programme and various promotional offers provided to customers in response to the breach (Hachman, 2011). In 2012, a judge dismissed one of the US class action lawsuits filed on behalf of those affected (Kerr, 2012). Other lawsuits were filed in the United States and Canada (seeking CAD 1 billion in the Canadian lawsuit (Rose, 2011)). As of May 2015, the company reported that US class action suits had been settled (amounts were not disclosed) although a non-US lawsuit remained pending (Sony Corporation, 2015). The UK Information Commissioner's Office fined the company GBP 250 000 for security failures related to the incident (Halliday, 2013).</td>
</tr>
<tr>
<td></td>
<td>The company provided a detailed breakdown of many of the expenses that it incurred as a result of the data confidentiality breach in its 2010 Annual Report. The company incurred approximately USD 31.4 million in legal fees, investigative costs, remediation and crisis management services. The rest of the company's expenses (USD 114.7 million) were incurred for the settlement of claims/assessments, including USD 3.5 million to settle with American Express, USD 59.3 million with Visa and related parties, USD 34.8 million with MasterCard and USD 5.0 million with Discover (likely related to the cost of re-issuing cards and any fraudulent transactions resulting from the breach) (Heartland Payment Systems, 2011). USD 31.2 million was recovered through insurance.</td>
<td>The 2010 Annual Report also identified a number of ongoing class action lawsuits on behalf of cardholders and financial institutions. The company also faced a number of regulatory investigations and enquiries from a number of agencies in the United States and Canada. The company's share price reportedly declined by 77.6% in the six weeks after the disclosure of the breach and remained 50% down almost six months after the breach relative to the price before the breach was announced (King, 2009). Approximately 5 000 of the company's 250 000 merchant clients reportedly left in the weeks after the data confidentiality breach was disclosed (SecureWorks, 2012).</td>
</tr>
</tbody>
</table>
A data confidentiality breach of third party data could involve third party corporate (rather than personal) data, the release of which could be deemed defamatory, involve a copyright infringement or disclose third party trade secrets. In such cases, the company affected by the data confidentiality breach may be liable for compensating the third party whose information was disclosed. The CRO loss classification defines such losses as communications and media [liability].

First-party (own) data confidentiality breaches

There is more limited information on data confidentiality breaches involving unauthorised access to own data (e.g. trade secrets or financial data) as there are no (or limited) notification or disclosure requirements related to these types of incidents (with the exception of US Securities and Exchange Commission disclosure requirements which may apply in some instances). There are some estimates of the prevalence and impact of intellectual property theft. For example, in the United Kingdom, a survey of firms in 2015/2016 found that 1% of those surveyed had been affected by intellectual property theft in the previous 12 months (Department for Culture, Media & Sport, 2016) while an older report suggested that intellectual property thefts may account for one-third of the total estimated economic cost of cyber crime (Detica and Cabinet Office, 2011). In Europe more generally, a report by a cyber security firm found that, in 2016, 19% of all data that was exfiltrated as a result of malicious cyber incidents involved trade secrets (FireEye, 2017). An annual study on US insurance claims payments included one payment in 2016 for loss of trade secrets for an amount of USD 4.9 million and three payments in 2014 for amounts ranging from USD 150 000 to USD 900 000 (including self-insured retention) (NetDiligence, 2016).

These types of breaches are most commonly targeted at the public sector, manufacturing industries and professional services sector (Verizon, 2016). In December 2016, for example, ThyssenKrupp, a German industrial engineering conglomerate, disclosed that it had been the victim of a significant cyber attack that led to the theft of confidential business information from its steel production and manufacturing plant design divisions (Auchard and Käckenhoff, 2016). The value of the stolen trade secrets was not disclosed. A more recent target for intellectual property theft has been the media industry which has faced a number of ransom demands in recent months to prevent the early release of films and/or television episodes (Smith, 2017).

System malfunction/issue

The CRO Forum classification includes five sub-categories of system malfunction/issue: (i) own system malfunction; (ii) own system affected by malware; (iii) network communication malfunction; (iv) inadvertent disruption of third-party system; and (v) disruption of external digital infrastructure.

Own system malfunction/own system affected by malware/network communication malfunction

The CRO Forum classification identifies three categories of system malfunction/issue involving a company's own systems or software:7 (i) own system malfunction (i.e. where a company's own systems create system errors, freeze completely or are otherwise rendered inoperable); (ii) own system affected by malware (i.e. where an intrusion of a company's systems is suspected due to the detection of malware or the abnormal behaviour of systems and software);8 and (iii) network communication malfunction (i.e.
where a company's systems cannot communicate via the internet or other digital network). Two practical examples of own system malfunctions are a malfunction in a core business system (either due to human error or a malicious attack) and a denial-of-service attack. These types of own system malfunctions and the kinds of losses that may be generated are described below.

Companies depend on digital systems and software for a wide-range of corporate functions, from internal communications to payroll and financial reporting to control systems for the operation of machinery and equipment. A malfunction of any of these systems or software can lead to important consequences for business operations. For example:

- Business interruption/interruption of operations: An internal disruption to the provision of digital services, particularly a core digital service, could lead to an interruption of operations, extra expense and/or lost profits;
- Data and software loss: A malfunction of a system or software would likely lead to costs for restoring or replacing data and/or software;
- Product liability or professional services errors and omission (E&O) liability/professional indemnity: Depending on the nature of the companies' business, a system or software malfunction leading to a defect in the company's product or a failure to provide adequate professional services could lead to a liability claim or class action by its customers;
- Physical asset damage: If the system that malfunctions is involved in controlling the functioning of machinery or equipment (i.e. operational technology), damage to physical assets is possible (see Box 2.4). Damages to system hardware (whether or not as part of an operational technology failure) would also normally be considered physical asset damage.
- Technology errors and omissions (E&O) liability: If the system or software that malfunctions was acquired from a third party technical services provider, the provider may face a liability claim related to the malfunction.

There is very little information on the frequency or impact of systems malfunctions as notification and disclosure requirements are much more limited than in the case of third party data confidentiality breaches. In the European Union, under the Network and Information Security Directive, operators of "essential systems" must notify the competent authority or computer security incident response teams of "incidents having a significant impact on the continuity of the essential services they provide" with a possibility for public disclosure in certain circumstances (European Union, 2016). In addition, under the Payment Services Directive, payment services providers must notify the competent authority in the event of any major operational or security incident and payment system users (i.e. the public) where the incident "may have an impact on the financial interests of its payment service users" (European Union, 2015). In the United States, major operational incidents could be covered within the scope of the US Securities and Exchange Commission disclosure requirements.

A denial-of-service (DoS) (or distributed denial-of-service, DDoS if a network of computers is involved) attack could be considered as a form of system malfunction, specifically a network communications malfunction under the CRO classification. A DoS attack is aimed at bombarding a web server with traffic in order to disrupt its
2. TYPES OF CYBER INCIDENTS AND LOSSES

functionality. There are various sources of data on the volume of DoS and DDoS attacks. According to one estimate, half of all major US corporations experienced a DoS attack in 2015 and one-in-eight of those attacks led to a disruption of website services (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). A survey of UK firms in 2016/2017 found that 8% of those surveyed had been affected by a DoS attack in the previous 12 months (relative to 15% in 2015/2016) (Department for Culture, Media & Sport, 2016; Department for Culture, Media & Sport, 2017).

Box 2.4. Physical asset damage due to cyber attacks on operational technologies

There is significant concern about the potential losses that could result from a cyber attack targeted at control systems, particularly control systems used in the operation of critical infrastructure such as electricity networks, water supply, or communication infrastructure. There is also some evidence of increased frequency of attacks on some critical infrastructure sectors, such as the energy sector. For example, the US Industrial Control System Cyber Emergency Response Team registered 303 reported incidents affecting industrial control systems in 2015 relative to 138 in 2012 (NCCIC/ICS-CERT, n.d.). A recent report found that, in 2016, 18% of all data that was exfiltrated as a result of malicious cyber incidents in Europe was data related to industrial control systems, building schematics and blueprints (FireEye, 2017).

There are a few documented examples1 of cyber attacks that have led to physical damages, usually as the result of a malware infection that led to system malfunctions or allowed for the takeover of systems through remote access:

- In August 2008, an explosion occurred along a pipeline in Turkey which has been linked to a cyber attack that increased the pressure of the crude oil flowing through the pipeline while disabling the alarms and communications systems that would normally trigger a response to such an event (Robertson and Riley, 2014).

- In 2010, a computer worm (malware) aimed at sabotaging the operation of centrifuges used for uranium enrichment was discovered in the industrial control systems operating enrichment facilities in Iran. The worm reportedly led to damages to a number of the centrifuges (Kelley, 2013).

- In 2014, an unnamed steel mill in Germany was affected by a cyber attack that disabled the ability to shut down a blast furnace, leading to significant physical damages (Zetter, 2015).

- In 2015, a cyber attack against power distribution control centres in the Ukraine led to approximately 30 substations being taken offline and a loss of power to more than 230 000 residents for a period of one to six hours (Zetter, 2016). A further attack on a control centre that disabled capacity equivalent to about 20% of the city of Kiev's night time energy use was reported in December 2016 (Condilffe, 2016). It has since been reported that the malware used in the latter attack (known as "Crash Override" or "Industroyer") could also be effective in attacks against power grids in Europe and potentially the United States (Finkle, 2017).

Lloyd's (2015) has published an industrial control systems sabotage scenario (developed by the University of Cambridge Centre for Risk Studies) based on an electricity blackout affecting 15 states in the Northeastern United States (including New York City and Washington, D.C.). The scenario is based on a malware infection that causes electricity generators to overload and burn out leading to widespread short-term blackouts with rolling restoration of power over a number of weeks. While deemed improbable, the scenario is reported to be technologically feasible. The scenario estimates economic impacts ranging from USD 243 billion to more than USD 1 trillion and insured losses of USD 21.4 - USD 71.1 billion depending on the severity of the scenario (which, under the more extreme scenarios, involve insured losses that are higher than the most costly ever natural catastrophe - Hurricane Katrina). Insurance claims would be incurred across a number of business lines, including property damage and business interruption at power generation companies, property (cold storage) and business interruption losses at companies in the blackout area and contingent business interruption at companies with suppliers in the blackout area.

1. A series of fires at petrochemical plants and facilities in Iran between June and September 2016 have been reported as potentially caused by malware although this has not been publicly confirmed (Gambrell, 2016).
A specialty provider of DDoS mitigation services for large traffic customers publishes statistics on the number of DDoS attacks, the number of "mega-attacks" (i.e., attacks of over 100 Gbps (gigabytes per second)), average duration and the maximum traffic volumes against websites using its services. According to its estimates, there was an increase in the number of DDoS attacks by a factor of 7.5 between 2014 (Q2) and 2017 (Q2). The number of mega-attacks (i.e., attacks capable of disrupting a website with the infrastructure necessary for 1 billion visits per month (the top 100 global websites)) has been more variable on a quarterly basis (although the number of mega-attacks in 2016 was close to double the number of mega-attacks in 2014, before declining in 2017). The size of the largest attack per quarter has generally increased over time and reached over 600 Gbps for one incident in Q3 2016 (see Figure 2.4). The DDoS attacks on OVH in September 2016 and on Dyn in October 2016 (see Box 2.5) reportedly reached more than 1.0 Tbps (terabytes per second, or 1 000 Gbps) (Paganini, 2016; Woolf, 2016). The sectors that are most commonly targeted by DDoS attacks include government, gaming, software and technology, media and entertainment, internet and telecommunications and financial services (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016; Akamai, 2016d).

Figure 2.4. Denial-of-Service attacks

The main losses from a DoS attack (for the company directly attacked) are likely to be due to business interruption/interruption of operations, including lost profits as well as extra expenses. The magnitude of losses will depend on the length of the disruption as well as the importance of the disrupted website in terms of the impacted company's business (and particularly its revenue generating impact, such as online sales and/or online advertising). Seasonal and time-of-day factors are also likely to have an impact (i.e. a disruption during peak sales times would be more harmful). A recent survey by Arbor Networks (2016) provides estimates of the cost-per minute of downtime across a range of companies (see Figure 2.5). Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016) have provided average per event estimates of USD 52 000 for small to medium businesses and USD 444 000 for larger businesses. A study of US
claims found that insurance payouts for most incidents in 2016 were below USD 35 000 although at least one claim involved USD 750 000 in damages, including self-insured retentions (NetDiligence, 2016). Payouts of over USD 1 million (and up to USD 5 million) have been reported in previous years (NetDiligence, 2014).

Box 2.5. Distributed Denial-of-Service attack on Dyn

On 21 October 2016, a huge DDoS attack against the servers of Dyn, a provider of domain name system (DNS) services, led to the disruption of a number of major websites in the United States and Europe, including Twitter, the Guardian, Netflix, Reddit, CNN and many others (Woolf, 2016). As a DNS service provider, Dyn translates requests for internet content into the IP addresses used to access that content. Therefore, a DDoS attack that overloads the capacity of Dyn to properly direct internet traffic will have a knock-on impact on the companies to whom it is providing its DNS services (i.e. the companies that depend on Dyn to direct traffic towards their content).

According to Dyn, the company was impacted by two DDoS attacks. The first attack initially targeted Dyn servers directing internet traffic in Asia-Pacific, Eastern Europe, South America and the Western United States and then shifted to servers directing traffic in the Eastern United States. The first attack took just over two hours to mitigate (although the actual time disruption to Dyn client websites would have varied). The second attack was targeted more diversely at servers directing internet traffic for users around the world and was mitigated in just over one hour (Hilton, 2016).

The DDoS attacks were reportedly implemented using the "Mirai" botnet which is able to generate requests to targeted servers by internet connected devices (webcams, wifi routers or even baby monitors) as well as computers. The use of such a broad range of devices allowed for an attack strength that apparently reached 1.2 Tbps using tens of millions of different IP addresses, approximately double the strength of the previous most powerful DDoS attack (which also used the same botnet) (Schneider, 2016). The attack on Dyn caused an estimated USD 110 million of (contingent) business interruption losses although very little was expected to have been insured given that most insurance policies use time deductibles that would normally be longer than the disruption caused by these incidents (Calversbert, 2016).

Figure 2.5. Cost-per-minute of website downtime

<table>
<thead>
<tr>
<th>Share of companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>USD 1-1 000</td>
</tr>
<tr>
<td>USD 1 001 - 5 000</td>
</tr>
<tr>
<td>USD 5 001 - 10 000</td>
</tr>
<tr>
<td>USD 10 001 - USD 20 000</td>
</tr>
</tbody>
</table>

Source: Arbor Networks (2016). Cost-per-minute was not defined in the survey question although a related question on business impacts considered a wide-variety of potential costs, including operational expense, reputation/brand damage, revenue loss, remediation and investigation, loss of customers, loss of executive or senior management, regulatory penalties and/or fines, extortion payments and increases in cyber insurance premiums.
DoS attacks are increasingly used as a distraction aimed at occupying information technology security resources in order to reduce their ability to detect a simultaneous cyber attack (such as an attempt to access the company's internal network). In such cases, the DoS attack might lead directly to some business interruption losses as well as a data confidentiality breach or extortion payment (for example) and the various types of losses associated with those types of incidents. The survey by Arbor Networks (2016) found that extortion payments were made by 4% of respondents as a result of one or more DDoS incidents.

**Inadvertent disruption of third-party system**

The fourth sub-category of system malfunction identified by the CRO Forum is an inadvertent disruption to a third-party system. This type of malfunction refers to instances where a company's systems or networks are accessed by an unauthorised attacker in order to use those systems and networks to target a third party, for example through the spread of malware or as a botnet involved in a denial-of-service attack. In such cases, the company whose network was used as a botnet or for the transmission of malware could face a third-party liability claim from the company that was affected by the denial-of-service attack or faced damages or losses due to the malware. Under the CRO Forum's loss classification, these losses are defined as network security/security failure [liability] losses. No public information on the magnitude of losses from these types of incidents (or examples of such incidents) has been identified although information security experts report this as a common occurrence (although it is not clear how frequently liability is established). A particular exposure could emerge as a result of the increasing use of connected devices as botnets in DDoS attacks. For example, it is conceivable that a producer of routers used as botnets in a DDoS attack could face a liability claim by those affected by the attack based on an allegation of insufficient security protections.

**Disruption of external digital infrastructure**

The fifth type of system malfunction incident under the CRO classification is a disruption of external digital infrastructure. This would involve a disruption to a company's business resulting from a disruption to the information technology services provided by a third party (such as a cloud service provider (see Box 4.1) or a DNS service provider such as Dyn, as described in Box 2.5). In such cases, companies that depend on these service providers will face contingent business interruption losses, i.e. business interruption losses that are caused by an interruption at a related third-party (a supplier of information technology services). No public information on the magnitude of losses from these types of incidents was found. It is likely that companies that depended on Dyn to direct traffic to their internet content would have faced some contingent business interruption losses during the period when Dyn's servers were unable to direct traffic as normal (although, as noted, it is likely that these losses did not reach the time threshold for insurance coverage). Some of the disruptions to cloud service providers described in Box 4.1 might also have led to contingent business interruption losses. For information technology service providers, such disruptions could lead to technology errors and omissions liability (for example, if it is determined that the provider was negligent in protecting its systems against disruption).
2. TYPES OF CYBER INCIDENTS AND LOSSES

Data integrity/availability

The CRO Forum classifies incidents involving the deletion, corruption or encryption of either own or third party data into a category on data integrity/availability. Similar to the data confidentiality category, the classification of an incident in this category is based on the detection of deleted, corrupted or encrypted data, rather than the underlying cause. The CRO Forum classification also establishes separate sub-categories for own and third party data. For the purposes of this report, two illustrative examples will be examined: (i) the deletion or corruption of own or third party data due to a software error; and (ii) the encryption of own or third party data as a result of an intrusion by ransomware. There may be some differences in terms of consequences between incidents where the underlying data is own data or third party data although this is most likely valid only in a minority of cases (e.g. where the impacted company has some kind of obligation to maintain a complete and accurate catalogue of third party data).

Deletion or corruption of own or third party data

The data held by a company, whether its own or belonging to a third party, may be deleted or corrupted as a result of human error or malicious attack. There is limited information on examples of this occurring as this kind of incident would normally only have implications for the company whose data holdings were affected (i.e. there would be no need to notify a third party if their own data had been deleted or corrupted unless the affected data holder is the only source of that data). The one well-known example of a malicious attack that resulted in the deletion of data was the 2015 attack on Saudi Aramco (Saudi Arabian state oil company) which led to deletion of data affecting over 30 000 computers (see Box 2.6).

Box 2.6. Malware attack on Saudi Aramco

On the morning of 15 August 2015, a malware developed with a "timebomb" set to go off at a specific time began deleting the data on the computer hard drives connected to the internal network of Saudi Aramco, the state oil company. The choice of 15 August - a holy day in Saudi Arabia (Lailat al Qadr) - meant that a large proportion of Saudi Aramco's employees were not in the office (potentially slowing the response to the incident) (Perlroth, 2012). The malware succeeded in deleting data from approximately 75% of all of Saudi Aramco's corporate computers (approximately 35 000 affected computers) and led to days without internet and corporate email access as the network was shut-down to end the spread of the malware. Many of the company's business functions, such as shipping and contracting, were severely affected - although the company's oil production was managed through a separate unaffected network. While the overall cost to the company of the incident is unknown, reports suggest that the company brought in information technology security experts from around the world to respond to the incident and purchased 50 000 computers to replace those that were affected by the malware (Rashid, 2015). In addition, the disruption to business functions apparently led the company to give oil away for free in order to maintain the continuity of domestic supply (Pagliery, 2015).

In terms of data corruption, there are few (if any) known example of incidents although a scenario has been developed by the University of Cambridge's Centre for Risk Studies (Ruffle et al., 2014) which provides one approximation of the magnitude of potential losses from a significant software sabotage leading to the corruption of data over time (see Box 2.7).
Box 2.7. Loss potential of a data corruption incident: a scenario

The Centre for Risk Studies at the University of Cambridge (Ruffle et. al., 2014) developed a sabotage scenario to estimate the loss potential due to the corruption of a widely-used database software. The scenario is based on the corruption of a relational database (i.e. a database structured to recognise relationships between data items) by a malicious (disgruntled) insider which produces small (and therefore less likely to be noticed) computational errors in the stored data over time. In the scenario, computational errors (or a "logic bomb") begin to impact various types of algorithmic processes in various sectors, including, for example, the design of manufactured parts, trading and pricing models, management information systems used for regulatory filings, process control systems used for managing equipment and logistics systems related to the management of supply chains. Broad use of the database across many sectors and processes along with the incremental corruption of data over time (which also means that database backups are corrupted) leads to significant and widespread uncertainty about data integrity. Losses are incurred by the database vendor as a result of the need to compensate their customers for their losses related to data integrity (technology errors and omissions liability) as well as by database users who may face compensation demands and/or lawsuits from customers that have purchased final products developed based on corrupted processes (product liability) and shareholders affected by the declining value of the affected companies' business (directors and officers liability). While the scenario does not include an estimate of losses faced by companies, it does provide an estimate of the share of global GDP at risk, ranging from 8% to 26% depending on the severity of the specific scenario.

Encryption of own or third party data

The encryption of own or third party data by an unauthorised external party would normally only occur as the result of a cyber extortion attack. In such incidents, an attacker will use malware known as "ransomware" to make data unavailable to its users through encryption until a payment is made to the extortionist. In most cases, the encryption is sufficiently strong to ensure that the data is not recoverable without the payment of a ransom (Stransky, 2017). Some have suggested that ransomware may be replacing the sale of stolen data as the most effective way for cyber criminals to profit from network security breaches (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). There is some evidence that the frequency of ransomware attacks is on the rise while the recent WannaCry and NotPetya ransomware attack demonstrates the potential for broad scalability (see Box 2.8). Beazley (2017a and 2017b) reported a quadrupling of ransomware incidents among its clients in 2016 and an increase of 50% in the first half of 2017 (relative to the first half of 2016). AIG's operations in Europe, Middle East and Africa reported that 16% of all cyber claims it received between 2013 and 2016 (up to September) were for encryption ransomware extortion (AIG, 2016). Similarly, the number of worldwide users of a specific ransomware protection software that encountered ransomware rose by 17.7% to over 2.3 million users in the period April 2015 to March 2016 relative to the previous twelve months (April 2014 to March 2015) (Kaspersky Lab, 2016). Among respondents to the OECD questionnaire, the proliferation of ransomware remains among the most important factors in driving the level of cyber risk.

These types of incidents lead to losses classified by the CRO Forum as cyber ransom and extortion losses, including the cost of experts to manage the incident and the amount of any ransom payment made. Information on past losses related to extortion is not generally available as there are almost no disclosure or notification requirements, and important incentives for not disclosing ransom payments (such as the aim of not encouraging further extortion demands). In the United States, an estimated USD 209 million in ransoms was paid by businesses and individuals to hackers in the first
quarter of 2016 alone (compared to a total of USD 25 million in 2015) (Twersky, 2016). For individuals and small organisations, payments related to ransomware are generally below USD 1 000 while most company payments are in the range of USD 10 000 to 50 000 (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). There is some evidence of ransom inflation with reports that the average ransom demand tripled in 2016 to just over USD 1 000 (Sharp, 2017). There are a handful of examples of much larger payments (in USD millions) by large corporations including a reported payment of "several million" by a European telecommunications company and several payments in the USD 3 million to USD 7 million range by companies and financial institutions in Greece, India and the United Arab Emirates (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2016). Recently, there has been an increase in attacks on hospitals in the United States and Europe, aimed at capitalising on their particular dependence on timely access to patient data (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017). A study of US insurance claims found a range of costs from USD 12 500 to USD 75 000 with an average cost of USD 32 000, classified as forensic investigations costs and legal guidance including self-insured retentions (it is not clear whether ransom payments were made and/or reimbursed by insurance companies), (NetDiligence, 2016).

Box 2.8. WannaCry and NotPetya

In May 2017, a massive global attack using a ransomware worm known as "WannaCry" reportedly infected more than 300 000 computers in 150 countries around the world, including at the UK National Health Service, the Russian Ministry of Interior, the DeutscheBahn railway and global companies such Nissan, Renault, and FedEx (Robertson and Penty, 2017; Risk Management Solutions, 2017). The ransomware took advantage of a known vulnerability in the Microsoft Windows operating system for which a patch had been released in March. Files on infected computers were deleted and replaced with an encrypted version which could only be unlocked upon payment of a ransom of approximately USD 300, with the ransom amount increasing over time (Sherr, 2017). While the overall losses in terms of ransom payments were not significant, a number of organisations faced operational disruptions. For example, some hospitals in the United Kingdom were forced to divert patients while production at some Renault factories was halted in order to stop the spread of the malware (Robertson and Penty, 2017).

In June 2017, a second ransomware attack, known variously as "Petya", "NotPetya" and "GoldenEye" affected companies in North America, Asia, Latin America, Australia and particularly Europe, including large companies such as Maersk and FedEx's TNT subsidiary. Similar to "WannaCry", the ransomware accessed companies through a "backdoor" vulnerability (this time, through an accounting software commonly-used in the Ukraine), encrypted data and sought a ransom payment of approximately USD 300 in bitcoin in order for the data to be decrypted (Harman, 2017; Satter, 2017) (although access to a decryption key was apparently disabled soon after the attack (Schlangenstein, 2017)). The attack led to disruptions in the operations of major ports in New York/New Jersey and Rotterdam managed by a Maersk subsidiary (Verbyany, Kravchenko and Turner, 2017) with some lasting more than two weeks after the initial attack (Schlangenstein, 2017). Maersk reported to investors that it expected to face costs of USD 200 million to USD 300 million as a result of the operational disruptions (Advisen, 2017d). FedEx's European subsidiary TNT was still reportedly using manual processes for some operations into July (Schlangenstein, 2017). In September, the company reported a USD 300 million reduction in quarterly profits as a result of the disruptions (Johnson, 2017). For manufacturing companies, the main impact was in terms of lost sales, including EUR 35 million for Beiersdorf AG, GBP 90 million for Reckitt Benckiser and EUR 250 million for Cie. de Saint-Gobain (Ricadela, 2017).

While neither event led to significant insured losses (partly due to limited impacts in the United States where more companies are insured against cyber risk), the global reach of "WannaCry" and the disruptive force of "NotPetya" are seen as illustrations of the potential for large losses from ransomware attacks (Suess, 2017a).
Malicious activity

The CRO Forum incident classification includes three sub-categories of malicious activity: (i) misuse of system (i.e. misuse of a digital system to distribute defamatory or embarrassing messages); (ii) targeted malicious communication (e.g. phishing attempts aimed at securing confidential information); and (iii) cyber fraud, cyber theft (e.g. an unauthorised financial transfer). For the purposes of this report, two illustrative examples will be examined: (i) the misuse of a system for defamatory statements; and (ii) cyber fraud/theft based on unauthorised network access and/or unauthorised use of financial credentials. One of the most common forms of targeted malicious communications ("CEO-phishing") is usually aimed at cyber fraud/theft and will be addressed in that section.

Misuse of systems for defamatory purposes

This sub-category of malicious activity would cover incidents that involve the misuse of digital systems to distribute defamatory or embarrassing statements/information. In the CRO Forum classification, it specifies that the information that is distributed would be defamatory or embarrassing to the victim, suggesting that this category is meant to cover first party damages and losses, not liability (the section on third party data confidentiality outlines an example of how the release of defamatory confidential information as the result of a breach could lead to third party liability for the organisation that is breached). The description specifically refers to "cyber bullying" and "cyber mobbing" suggesting that this category of incidents is mainly focused on individuals affected by defamatory or embarrassing statements on digital systems such as social media (see Box 3.2 for a brief overview of cyber insurance for individuals). In the case of individuals, losses might be incurred as a result of reputational damage related to distribution of defamatory or embarrassing statements.

Companies could also be affected by defamatory or embarrassing statements on digital systems (including social media) with potential consequences in terms of reputational damage. For example, in 2016, a fake press release claiming that Vinci (a French construction and engineering company) had dismissed its chief financial officer due to accounting irregularities was distributed to financial news outlets, leading to a fall in the company's share price of 18% (although the price later recovered after the company denied the information (Nussbaum, 2016)). In this case, there was no major loss to the affected company (Vinci) although the example provides an indication of the type of defamatory information that could be distributed and the potential for reputational damage.

Cyber fraud/cyber theft

Cyber fraud or theft (i.e. unauthorised or fraudulent transfer of funds) could occur as a result of an intrusion into a company's network, the use of financial credentials to make an unauthorised transfer of funds or through deception (for example, by impersonating a company officer in an email seeking to initiate a transfer of funds). In these cases, the cyber fraud or theft would lead to pure financial losses (categorised as financial theft and/or fraud under the CRO Forum loss classification).

There are a few examples of cyber theft that appear to have resulted from some form of network intrusion, including through unauthorised inter-bank transfers (such as the USD 101 million transferred from the Bank of Bangladesh's account at the New York
Federal Reserve (along with a number of other transfers and attempted transfers attributed to the same criminal gang (Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies, 2017)) and the creation of bank cards (with manipulated limits) to withdraw cash from Automated Teller Machines (ATMs) (e.g. USD 45 million was withdrawn using pre-paid travel cards from Indian credit card processors in 2013 while JPY 1.8 billion was stolen from ATMs in Japan based on credit card data from the customers of a South African bank in 2016). In 2016, Tesco Bank in the United Kingdom was affected by a cyber attack that resulted in GBP 2.5 million in funds being fraudulently transferred from approximately 9,000 customer accounts (although the details on how this was done have not been publicly disclosed) (Leyden, 2016). There is at least one example from Thailand of thieves loading malware directly onto ATMs in order to withdraw funds from these machines (Lewis, Wieland and Peel, 2016). A number of real estate companies in the United States (amongst others) have also been the victims of unauthorised transactions, usually involving escrow accounts and transfers of USD 1.5 to 2.0 million (Krebs, 2014a; Krebs, 2014b; Krebs, 2013). There are also a number of examples of major thefts of crypto-currencies due to network intrusions. According to one analysis, since the creation of bitcoin in 2009 (up to March 2015), 33% of all bitcoin exchanges that have operated have been hacked, in many cases leading to significant losses for customers of those exchanges (Chavez-Dreyfuss, 2016).

Another approach that is being used to commit cyber fraud or theft is through the use of social engineering (i.e. sending targeted email impersonating a legitimate person) aimed at initiating a financial transaction for the benefit of the attacker. For example, one common approach is to send an email impersonating the CEO or other senior officer of a company and demanding that payment be made to a specific account ("CEO-Phishing"). In 2016, the US Federal Bureau of Investigation (FBI, 2016) issued a press release to warn businesses of this fraud (which they termed "business email compromise") citing USD 2.3 billion in fraudulent payments by 17,642 victims between October 2013 and February 2016 (an average of about USD 130,000 per victim, although with a potential for significant variation). According to one report, the amount of lost funds has increased to USD 5.3 billion up to December 2016 (CNA Financial Corporation, 2017) with a 1300% increase since 2015 (FBI, 2016). In one case (Ubiquiti Networks), USD 46.7 million in fraudulent transactions was disclosed in one quarter as a result of this type of social engineering (Wickliffe, 2016). In Europe, there have also been several transfers of significant funds as a result of this type of social engineering fraud, including a USD 75 million transfer from a Belgian bank, a USD 50 million transfer from an Austrian aircraft parts manufacturer and a EUR 50 million transfer by a German cable manufacturer (FireEye, 2017; Suess, 2017b). A survey of UK firms in 2016/2017 found that 6% of those surveyed had money stolen as a result of a fraudulent email or website in the previous 12 months (the same percentage as 2015/2016) (Department for Culture, Media & Sport, 2016; Department for Culture, Media & Sport, 2017).
Figure 2.6. Common types of cyber incidents and resulting losses

Source: Adapted from OECD (2017)
2. TYPES OF CYBER INCIDENTS AND LOSSES

Notes

1. According to Risk Management Solutions, Inc. and Cambridge Centre for Risk Studies (2016), the black market value of US credit card numbers, email account credentials, social security numbers, and basic personal information (name, address, email address, phone number) declined between 2012 and 2015. However, the black market value of bank account access credentials, healthcare records, credit history and certain website account access credentials has increased (substantially in the case of healthcare records and bank account access credentials).

2. According to Swiss Re (2017), the types of credit monitoring services that are often provided in the United States are prohibited in continental Europe (although permitted in the United Kingdom).

3. Public sector entities affected by data confidentiality breaches could also face costs related to the release of confidential information. The US Office of Personnel Management, for example, reportedly faces USD 1 billion in costs for credit monitoring services and identity theft protection over 10 years for employees whose data was accessed as a result of a data confidentiality breach (Advisen, 2017a).

4. According to some reports, the developing jurisprudence from data breach litigation in the United States suggests that the breach of some types of data (e.g. social security numbers, usernames, password) is more likely to lead to harm than others (e.g. name or payment card information given the ability to cancel payment cards) (Soloway and Mohler, 2017).

5. The Payment Card Industry Data Security Standard is a set of standards that retailers must adhere to in order to be able to accept and process payment card payments. The standards were established by the payment card networks who, based on contractual arrangements they enter into with retailers, have the authority to impose fines and assessment on non-compliant retailers. As discussed in Chapter 3, these fines and assessments are contractual (different than administrative fines imposed by regulatory agencies) and may be covered under some stand-alone cyber insurance policies (often as a specific add-on/endorsement).

6. The Ponemon Institute (2017) reports the average cost of a breach segmented by the amount of stolen records. For breaches involving less than 10 000 records, the average cost was USD 1.9 million. For breaches involving more than 50 000 records (i.e. at least 5 times more records), the average cost was USD 6.3 million (i.e. just over 3 times more). This would indicate that the average cost per record is lower for larger breaches.

7. For the purposes of this report, only own system malfunctions due to a technical issue are considered (i.e. not malfunctions that result from physical damage, such as a fire in a data centre). This is consistent with how this damage would normally be covered by insurance as tangible damage caused by a physical peril would normally be covered by a property insurance policy rather than a stand-alone cyber insurance policy (subject to the exclusions outlined in Box 3.1).

8. According to an OECD (2009) definition, "malware is a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners. Malware can gain remote access to an information system, record and send data from that system to a third party without the user’s permission or knowledge, conceal that the
information system has been compromised, disable security measures, damage the information system, or otherwise affect the data and system integrity”

9. A Ponemon Institute (2012) survey of medium-to-large US-based companies found much higher estimates of the cost of downtime (USD 22 000 per minute on average and USD 1.2 million per event based on an average duration of 54 minutes). This estimate includes "possible lost traffic, end-user productivity and lost revenues" and potentially other costs.

10. This could also be considered a system malfunction incident as the malware that infected the Saudi Aramco computers deleted all data, including the data needed for the computers to operate.

11. Cyber-extortionists may also use the threat of a DoS attack or a data release (resulting from a data confidentiality breach) as another means of extracting a payment from targeted firms.

12. In the United States, an incident involving the encryption of health data is considered to be a data breach incident and subject to the notification requirements under the Health Insurance Portability and Accountability Act.

References


Advisen (2017b), "$142,000,000 in Response Costs for Anthem", Advisen Cyber Loss Data.


Department of Health and Human Services (2017), "$5.5 million HIPAA settlement shines light on the importance of audit controls", News Release, 16 February, Department of Health and Human Services, Washington.

Department for Culture, Media and Sport (2017), Cyber Security Breaches Survey 2017, Department for Culture, Media and Sport, London.

Department for Culture, Media and Sport (2016), Cyber Security Breaches Survey 2016, Department for Culture, Media and Sport, London.


Detica and Cabinet Officer (2011), The Cost of Cybercrime, Detica Lintted, Surry (United Kingdom).


eBay Inc. (2017), Form 10-K For the Year Ended December 31, 2016, eBay Inc.
Edwards et al. (2014), “Hype and Heavy Tails: A Closer Look at Data Breaches”,
Workshop on the Economics of Information Security.

Council of of 6 July 2016 concerning measures for a high common level of security of
network and information systems across the Union, European Union, http://eur-
lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Council of 25 November 2015 on payment services in the internal market, amending
lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

FBI (2016), FBI Warns of Dramatic Increase in Business E-Mail Scams, 4 April, US
Federal Bureau of Investigation, Phoenix, www.fbi.gov/contact-us/field-
mail-scams, accessed 22 March 2017.

FBI (2017), Business E-Mail Compromise: Cyber-Enabled Financial Fraud on the Rise
Globally, 27 February, US Federal Bureau of Investigation,
9 October 2017.

Finkle, J. (2017), "Cyber firms warn of malware that could cause power outages",
of-malware-that-could-cause-power-outages-idUSKBN1931EG3.

FireEye (2017), Cyber Threats: A perfect storm about to hit Europe?, FireEye Inc.,
Milpitas (California), January.

Gambrell, J. (2016), "Blazes at Iran petrochemical plants raise suspicions of cyberattack",
The Times of Israel, 22 September, www.timesofisrael.com/blazes-at-iran-
petrochemical-plants-raise-suspicions-of-cyberattack/.

Gemalto NV (2016), It’s All About Identity Theft: First half findings from the 2016
Breach Level Index, Gemalto NV, Meudon, France,

Goel, V. (2017), "Yahoo’s Top Lawyer Resigns and C.E.O. Marissa Mayer Loses Bonus
in Wake of Hack", The New York Times, 1 March,
www.nytimes.com/2017/03/01/technology/yahoo-hack-lawyer-resigns-ceo-
bonus.html?_r=0.

Goodman, E. (2016), "Risky business: High financial costs for payment breaches at small
retailers", Property Casualty 360°, 9 September,
www.propertycasualty360.com/2016/09/09/risky-business-high-financial-costs-for-
payment-br.

Hachman, M. (2011), "PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher",
PCMag, 23 May, www.pcmag.com/article2/0,2817,2385790,00.asp.

Halliday, J. (2013), "Data watchdog fines Sony £250,000 over PlayStation ID hack", The
Guardian, 24 January, www.theguardian.com/technology/2013/jan/24/sony-fined-
over-playstation-hack.

Harman, P. (2017), "The newest global cyber attack takes down ports, banks and law
firms", Property Casualty 360°, 30 June,
2. TYPES OF CYBER INCIDENTS AND LOSSES


2. TYPES OF CYBER INCIDENTS AND LOSSES


PwC (2016), Moving forward with cybersecurity and privacy: Key findings from The Global State of Information Security® Survey 2017, PwC.


2. TYPES OF CYBER INCIDENTS AND LOSSES


Swiss Re (2017), Cyber liability: data breach in Europe, Swiss Re, Zurich.


Target Corporation (2017), 2016 Annual Report, Target Corporation, Minneapolis.

Target Corporation (2016), 2015 Annual Report, Target Corporation, Minneapolis.

Target Corporation (2014), 2013 Annual Report, Target Corporation, Minneapolis.


2. TYPES OF CYBER INCIDENTS AND LOSSES


From: Enhancing the Role of Insurance in Cyber Risk Management

Access the complete publication at: https://doi.org/10.1787/9789264282148-en

Please cite this chapter as:


DOI: https://doi.org/10.1787/9789264282148-4-en

This work is published under the responsibility of the Secretariat-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) at contact@cfcopies.com.