**The following is an extract from** [**https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288**](https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288)

**The Sony cases**

In April 2011, amid unstable economic conditions, Sony announced that personal information for 77 million PlayStation Network (PSN) subscribers as well as 24.6 million Sony Online Entertainment accounts had been exposed due to an external breach [64]. The data breach involved information about account logins, passwords, credit card details, purchase histories and billing addresses. Sony’s facilities in Japan were also heavily impacted from the earthquake of March 2011, resulting in the suspension of several critical operations, which rendered the cyber-attack well timed to inflict maximum damage. Sony had to place its PSN services offline the day following the attack [67] to assess the extent of the incident, resulting in loss of revenue; incurred response costs regarding identifying and addressing the vulnerabilities exploited and notifying the customers; a rough estimate of the costs is $171 million. This figure, however, does not include punitive damages from lawsuits, costs from identity theft or any other misuse of stolen credit cards, nor the loss of business and market capitalization [67].

In late April 2011, Sony provided a comprehensive recovery plan and an accurate calculation of the costs inflicted from the earthquake, but they were still not yet able to calculate the full organizational harm from the cyber-attack [64]. The aggregated impact of the earthquake and the data breach resulted in a significant decrease in Sony’s market evaluation as depicted in stock-exchange markets. Sony’s share price dropped 19% after the earthquake, a drop equivalent to the general Japanese stock exchange market, but soon recovered 50% of this loss [64]. After the cyber-attack, however, Sony’s price sustained a 12% loss (this time it was not a reflection of the rest of the Japanese economy), and the revelation of the security weaknesses once Sony had restored service prolonged the recovery phase [64].

Three years after these incidents, in November 2014, confidential data from Sony Pictures were once again leaked. The data included more than 30 000 internal documents, 170 000 emails, social-security numbers of Sony’s employees, personnel reviews and medical histories, and movies which had not yet been released. The same cyber-attack paralysed all of Sony’s systems, rendering the online database of stock footage unsearchable, the telephone system offline, computers and servers unusable; this was described by the FBI as an ‘unprecedented digital assault that would have felled 90 per cent of companies it hit’ [57].

Sony was forced to replace a large number of its systems, set up a hotline for identity fraud, provide psychological counselling for employees and organize seminars on data security. Following the attack, Sony’s employees received emails threatening their families if they did not denounce Sony, their credit cards were available for sale on Dark Net markets, and some witnessed their bank accounts exceeding credit limits. A survey conducted by the Identity Theft Resource Center regarding victims of identity theft, reported that victims’ experienced ‘denial, frustration, rage, fear, betrayal, and powerlessness in the days, weeks, and years after the violation’ [57]. Class-action lawsuits from employees were filed, either because Sony did not notify those whose data was leaked, or over fears of how personal leaked information could be potentially used. This also contributed to the fact that some key staff left the company; and furthermore, the press discovered Sony’s diversity issues, which were discussed extensively in the content of the leaked emails [57, 66].

**The JP Morgan case**

JP Morgan Chase, one of the largest banks in the USA, reported that hackers obtained administrator access to several of their servers. Information regarding names, phone numbers, email and physical addresses of account holders was exfiltrated, affecting 76 million households and seven million small businesses. JP Morgan had announced an increase in their cybersecurity budget of $250 million per year just before the attack occurred [76]. The company was forced to replace the majority of its IT infrastructure, a process that was time-consuming and hindered the daily lives of employees. The remaining budget was spent hiring more than 1000 employees to monitor the company’s systems [74]. Of significant interest are the two long-term effects, which resulted from this hack. The majority of the customers whose information was leaked were obliged to monitor their finances in fear of fraud, while they received fake emails directing them to impostor websites for financial exchanges. As a result, many became victims of financial fraud. The second effect was the replacement of their chief information security officer because of his inadequate collaboration with federal authorities in an attempt to try to control the investigation and obscure the leakage of information [74].

**The Ashley Madison case**

In July 2015, details of 33 million accounts and personal information about people registered on Ashley Madison, a website facilitating extramarital affairs, were leaked [63]. A core principle of Ashley Madison’s business model was privacy and security, through which they would build a trust relationship with their customers. The cyber-attack, therefore, had dramatic consequences for the reputation of the company, not only because it exposed the vulnerabilities of the system, but because it proved that Ashley Madison’s promise to delete data upon customers’ request was not kept [77]. As a result of this practice, Ashley Madison became liable to lawsuits [77], with many organizations soliciting litigants on Twitter [72]. What are of great interest in this case, however, are the repercussions of what was coined as ‘collateral damage’ which are peculiar to the nature of the services the website offered.

Once the data was publicly available and easily searchable, customers became susceptible to blackmail, with professional and personal ramifications [72]. Many of the leaked email addresses contained the ‘.mil’ domain, indicating people who serve in the US military. Adultery, however, is a crime in the US military and members of Ashley Madison were subject to a year of confinement or dishonourable discharge [77]. In a similar vein, owners of 1, 200 ‘.sa’ email addresses were exposed to a potential death sentence, which is the punishment in Saudi Arabia for adultery. New practices of cybercrime emerged, with criminals threatening to expose people whose email addresses were found in the Ashley Madison dataset to their ‘significant other’, unless $225 were paid in bitcoin [65]. Public figures were coerced into ‘painful personal admissions’, others were divorced, while the Toronto police reported two suicides potentially linked to the cyber-attack [65]