Case study: PlayStation Network

In April 2011, Sony revealed that the PlayStation Network, used by millions of consumers worldwide, had been breached by hackers. The breach went unnoticed by Sony for several days and ultimately resulted in the theft of up to 70 million customer records. The records included customer names, addresses, emails, dates of birth and account password details. Information which could have enabled additional attacks or identity theft.

In order to assess the scale of the damage and repair the vulnerabilities that led to the attack Sony took the PlayStation Network offline, a move which cost the company, and merchants who offered services via the network, significant amounts of revenue.

In addition to the cost of fixing the breach, Sony was fined £250,000 by the Information Commissioner's Office as a result of a 'serious breach' of the Data Protection Act, stating that 'The case is one of the most serious ever reported to us. It directly affected a huge number of consumers, and at the very least put them at risk of identity theft.'

The precise financial cost to Sony is unclear but estimates place it at approximately £105 million, excluding the revenue loss by partner companies, damage to its reputation and potential damage to its customers.

Attacking online identities

Adobe Systems is one of the most important companies in the digital economy. Its software is used to produce, publish and present an enormous amount of material – chances are your favourite magazines and books were laid out with Adobe software.

Over the years, Adobe had stored the names, addresses and credit card information of tens of millions of users on its servers. Then, in October 2013, Adobe admitted that data from 2.9 million accounts had been stolen. Later, that number was revised to 38 million accounts, but when the data file was found on the internet it contained no less than 153 million user accounts. Much of this data could be read and soon copies of the stolen accounts were in wide circulation. It also became clear that the people who had stolen user data had also gained access to Adobe's development servers – program code, potentially worth billions of dollars, had also been stolen.

Adobe was forced to change the log in details of every one of its users and to greatly improve its own security. And, of course, users are suing Adobe for not protecting their information.

Is Adobe alone, or are other companies holding valuable data but not protecting it properly?

Attacking specific targets

In December 2013, the American retailer Target announced that hackers had stolen data belonging to 40 million customers. The attack had begun in late November and continued for several weeks before it was detected. By then it had compromised more than 110 million accounts, including unencrypted credit and debit card information as well as encrypted PIN data. By February 2014, American banks had replaced more than 17 million debit and credit cards at a cost of more than $172 million. The amount of fraud linked to the attack is unknown, as is the damage to Target's reputation.

Target was not the first major retailer to be hit by hackers, but this attack was different from most; the weakness that allowed the attackers into the Target computers lay outside of the company. The hackers had gained access through computers belonging to one of Target's heating, ventilation and air conditioning services (HVAC) contractors. Like many large organisations, Target allows other companies to access its internal networks, to submit bills and exchange contracts.

The hack appears to have begun when an employee of the HVAC company received an email from one of their trusted partners. In fact, the email was fake and contained malicious software. Unlike traditional spam email, this message had been targeted at a very specific audience – the HVAC company. It was what is known as 'spear phishing'.

Once the email had been opened, the hidden software went to work and retrieved the HVAC company's Target network authorisations, allowing them to log on to their real objective. In an ideal system, the HVAC company's authorisations should have restricted them to a network responsible solely for billing and contracts, but, like a lot of big organisations, Target used a single network for all of its data, allowing the attackers to eventually locate, and steal, customer data.

The Target attack is an example of an advanced persistent threat. Rather than attempting to attack the retailer directly, the hackers had chosen an external company which was much less likely to have the resources to detect and defend against an attack. Their spear phishing email was directly targeted at the contractor, lulling them into a false sense of security and allowing the malware to retrieve the logon credentials needed to attack Target itself.