WARNING: THE LEGAL CONSEQUENCES OF A CYBER ATTACK RESULTING IN DATA LOSS ARE INCREASING

YOU ARE THE VICTIM OF A CYBER ATTACK. YOU LOSE THE PERSONAL DATA OF CUSTOMERS. YOUR BUSINESS IS INTERRUPTED AND YOUR REPUTATION IS DAMAGED. CAN IT GET WORSE? I'M AFRAID THAT IT CAN.

REGULATORY FINES

Since April 2010 the regulatory body which enforces the Data Protection Act 1998 ("DPA") in the UK, the Information Commissioner's Office ("ICO"), has had the power to impose fines of up to £500,000 on organisations who breach the DPA. The ICO is not shy about using its powers and publicising the fines it imposes and its powers are likely to increase to €1,00,000 when a new EU Regulations comes into force over the next few years.

CLAIMS FOR COMPENSATION

And to add to your woes, until earlier this year, it was only possible to claim compensation under the DPA if the claimant could show that the breach caused pecuniary loss. However in March the Court of Appeal decided that compensation could be claimed for distress as well. The level of damages is yet to be established, and indeed the decision has been appealed, but for the time being this ruling represents a significant extension of the cases where compensation can be claimed.

THE ICO

In the past few years the ICO has issued fines in relation to five organisations who have been the victim of a cyber attack. These fines range from £7,500 (an extremely small fine due to the apparent financial circumstances of the organisation) up to £200,000. On the face of it, it may seem harsh to penalise the victims but in each case the organisation in question was found to be lacking in terms of technological security which is a breach of the DPA.

The DPA contains eight principles which must be complied with by anyone dealing with personal data. The seventh Data Protection Principal ("DPP") obliges organisations to ensure that they have appropriate technical and organisational measures in place to prevent unauthorised processing of data. In the case of these 'victims' they were all guilty to not having systems that were secure enough.

- Sony was fined £200,000 following a DDoS attack on the Network Platform for its Playstation which had not been kept up to date with technical developments and which allowed the hackers to obtain personal information and encrypted financial information
- The British Pregnancy Advisory Service was fined £200,000 when someone fundamentally opposed to what they did hacked into their website and was able to access the names and addresses of people who had contacted BPAS. BPAS was unaware that the website was storing this information.
- Think W3 Limited was fined £150,000 when a coding error in the authentication scripts of a remote login page meant that it was insecure. No penetration testing had been carried out and the hacker gained access to customers' personal information and the system used to process cards. The information was encrypted but the key was not stored securely. None of the cards were used.
- Worldview Limited were fined £7,500 after they were attacked by a blind SQL injection attack and the attacker was able to access the personal information of 4,000 customers and their cards details including their CVV numbers. There was no fraudulent activity.
- Staysure.co.uk were fined £175,000 when their website was hacked because their operating system had not been patched properly despite two patches being released in 2010 and 2013 which would have addressed this vulnerability. In this case fraudulent activity did occur as 5,000 cards were used as financial information was held, including CVV numbers. The information had been encrypted but the hackers gained access to the key as well.

In relation to several of these cases, the ICO was also critical of information being held for longer than is necessary.

THE LESSONS

If you are the data controller the responsibility remains with you. You have to ensure that your IT systems are secure, even if you have external IT providers, you remain responsible for security. If you hold financial data or sensitive personal data (relating to medical, political or criminal matters) then this is likely to lead to significant fines from the ICO and now that the threshold for claiming compensation has been lowered this may also result in financial claims from customers. A warning to ensure that your IT systems and security are up to date and secure.

Laura Irvine
Associate and Criminal Solicitor Advocate,
bto Solicitors