Increased data privacy risk expected in 2022

In the wake of the Russian invasion of Ukraine, the US Cybersecurity and Infrastructure Security Agency has issued a "shields up" notice warning of increased risk of malicious cyber-attacks. At the same time, companies face increasing regulation of data privacy and cybersecurity and claims for losses relating to data breaches and privacy violations. Here, Jon Little of law firm Jones Day explores the risks and how UK private companies can respond.

Cyber risk is increasing. Facing pressure from government investigations and regulation and class actions and other litigation, companies are now being asked on a routine basis to demonstrate that they have taken the necessary cybersecurity compliance steps.

Ransomware

The number of ransomware attacks globally more than doubled in 2021 and there are concerns that the recent events in Ukraine could lead to further increases this year. These attacks require crisis-level management to restore operations, decide whether to pay any ransom, comply with legal notification obligations in a timely manner, and communicate effectively with internal and external stakeholders. Companies should assess their preparedness, update their business continuity and incident response plans and implement appropriate governance and controls.

Cloud Computing Security

Recent security breaches underline the risks of cloud computing. Company directors need to pay keen attention to the management of vendors, insider threats and supply chains. In particular, the allocation of responsibility for attacks between cloud providers and their customers is currently a key area of focus for regulators and litigation.

Legal Privilege

Judicial decisions raise important considerations for companies seeking to protect the results of internal investigations into cyber-attacks. For example, there have been a number of US court decisions holding that a forensic report generated by a consultant retained by outside counsel was not protected by legal privilege from disclosure to opposing parties in litigation. While similar concerns may not exist at present in the UK and all European jurisdictions, cyber-attacks often have global reach, which means documents produced in the UK or Europe may become relevant to US proceedings and therefore questions about whether those documents are protected by legal privilege and should be disclosed in any US proceedings might arise.

Privacy Litigation

Companies face increasing privacy litigation risk due to new laws aimed at protecting personal data. Management teams should be aware that recent cases in some jurisdictions have suggested that individuals will not need to prove damage when asserting a claim arising from a data breach. These cases are expected to fuel litigation, including burgeoning collective actions.

International Data Transfers

Data localisation laws and national security concerns are resulting in increased restrictions on cross-border data flows. These limitations present operational cost and legal risk for companies, and the need for a holistic strategy.

Increased Regulation of Emerging Technologies

Legislators and regulators have begun to focus on the rules and regulations that govern the use of emerging technologies, such as artificial intelligence (AI), biometrics and the internet of things (IoT). The EU is expected to adopt a number of legislative proposals as part of its digital agenda. Companies need to pay careful attention to both existing laws and regulatory trends.

Conclusion

Preparation and speed of response are key to dealing with cyber threats. Given the increased risks generally and the particular threat caused by the situation in Ukraine, companies should assess their preparedness, put appropriate policies and procedures in place and maintain an up to date plan for how to respond to incidents.

Contact us

Inferera@jonesday.com