Exploring businesses' approach to cyber security

21/03/2019

Corporate Crime analysis: Matthew Richardson, barrister at Henderson Chambers, comments on the obligations and opportunities which businesses face in relation to cyber security.

Original News

Report finds many FTSE 350 companies still unaware of the impacts of cyber attacks on their companies, LNB News 05/03/2019 40

According to the government's 2018 'Cyber Governance Health Check' report, which examines the UK's FTSE 350 companies' approach to cyber security, boards at many of the UK's largest companies still haven't grasped the severity of the impact that a cyber attack can have on their business. The report discovered that despite the fact that almost all FTSE 350 companies (96%) who responded have implemented a cyber security strategy, less than a fifth (16%) of the boards are considered to have a full understanding of the impact of loss or disruption relating to cyber threats.

What are some of the key findings of the report and what is the most concerning?

The government report shows a number of encouraging statistics in relation to FTSE 350 companies recognising the growing threat of cyber crime to business. Since 2013, the number of companies rating cyber as the highest possible risk category has tripled. That is a welcome movement in understanding. That, however, is not matched by an equivalent increase in mitigation of those risks. While almost all businesses (96%) have a cyber security strategy, only 46% have a dedicated budget for their cyber security strategy. Likewise, although board engagement at these companies has improved substantially, only around half (53%) receive comprehensive information about cyber threats. The General Data Protection (EU) Regulation 2016/679 (GDPR) appears at least partly responsible for the increased attention boards are giving to cyber threats. 77% of businesses responding to the 2018 health check reported that board discussion and management of cyber security had increased since the GDPR, with more than half of these businesses also introducing increased security measures as a result.

What type of cyber threats should company management fear the most and why?

While many companies have taken the time to invest in the hardware and software that keeps their computer systems safe, very few have taken the time to invest in what cyber security professionals cynically call 'liveware', that is to say the people operating those systems. More and more cyber-attacks involve some element of operator error or abuse. This is because malicious actors have concluded that the human component of these systems is the weak link. In addition to the usual hacking and computer misuse, I am increasingly seeing more and more audacious spear-phishing attacks. These are hacking attempts that are personalised to the recipient and have lately been used to devastating and costly effect on a number of high-profile companies.

What type of preparation should company management undertake to minimise cyber threats?

The statistics say it all, really, company boards need to start taking more and more responsibility for these threats and do everything in their power to ensure that they are getting comprehensive and regular updates on the cyber risk and breach contingency plans. Those plans must be tested and approved by a third party for the sake of validity. Dedicated cyber defence budgets are practically a necessity in 2019.

Given the personalised, well researched nature and many new cyber-attacks, it follows that education and training must therefore be the main focus for companies looking to minimise their risk and, it must be said, liability in the event of a successful cyber-attack upon them. Naturally, these companies all have money to make and every staff day training is a work day lost. However, the calculus weighs heavily in favour of making that investment as the costs of non-compliance and or breach by a successful hacker are massive.

What type of liability, civil or criminal, does company management expose themselves to if they do not prepare for cyber threats?

The liability for a company that fails to take the requisite technical or organisational measures to protect itself are staggering. The GDPR has given the Information Commissioner the power to levy fines based on the annual global turnover of a company. In the case of a breach of the general obligations on data controllers that fine can reach 2% of global turnover. That figure for the average FTSE 350 company would be astronomical. I have little doubt that in the right circumstances of dereliction in regard to cyber security, the Information Commission would have no difficultly flexing her muscle and imposing a fine on this scale.

This also does not account for losses suffered by any companies or individuals affected downstream from the hack, maybe through the loss personal data or trade secrets or actual monetary loss. All of these losses would have to be met by any company that had not complied with the regulatory duties or worse yet, was so ill prepared as to be negligent. A large company could be facing years of litigation and group actions in the event it lost personal data of many customers. Needless to say that any fines would be dwarfed by these costs.

Companies that are providers of 'essential services' that is to say basically infrastructure companies have further duties imposed on them by the Network Information Security (EU) Directive (EU) 2016/1148 and could be subjected to fines that are frighteningly described as 'effective, proportionate, and dissuasive' for breach of those further duties.

What is the current law, statutory or common, on the responsibility of company management for neglecting cyber security? Is any further regulation or oversight necessary?

The primary law that governs the responsibility in regard to data security is Article 32 of the GDPR, which imposes the following duty of all data controllers:

> 'Art 32
>
> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> 1 the pseudonymisation and encryption of personal data
>
> 2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
>
> 3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
>
> 4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing'

The items listed above are considered to be the bare minimum that is required to avoid liability under the GDPR, and I feel certain the law of negligence. However, this is the minimum required and taking into account the factors set out in that the requirements could be substantially higher in certain circumstances.

All companies need to assess the security measures on an on-going basis and regularly review the guidelines issued by the Information Commissioner, government and any relevant trade bodies and associations to keep up with current trends. Given the speed at which the 'state of the art' is moving, it is unlikely that any regulations could have any useful effect in keeping up.

Document information

Published Date
21 March 2019

Jurisdiction
England; Northern Ireland; Scotland; Wales

Interviewed by Kacper Zajac.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.