CoreStream®

In the Press

The strategic risk of cybercrime: Prevention deserves the highest priority

As featured in IT Pro Portal, Information Age, Data IQ Online and Network Security

The threat of cybercrime continues to evolve and grow, as criminals adapt to new security measures and take advantage of changes to our online behaviour.

The only constant appears to be our vulnerability: whatever new steps are taken, by companies or individuals, the criminals always seem to be one step ahead.

The problem is that it isn't an even contest. Hacking and online fraud is hugely profitable for organised crime, encouraging constant innovation and change in attacks. A notable recent development has been the packaging of sophisticated malware tools into kits that require few specialist skills to use. Now, criminals at the top of the chain can simply licence their tools in return for a cut of the proceeds. With hacked personal data now cheap and plentiful in online marketplaces, cybercriminals have proliferated.

The nature of the Internet means that cybercrime knows no borders: criminal activity can be focused on the easiest and richest pickings, and the perpetrators can be spread across the globe. Crime-fighting agencies have been overwhelmed by the volume of activity, and stymied by the fact that so much of it originates from multiple overseas jurisdictions.

In 2015, 25 per cent of large firms and around 15 per cent of smaller ones reported network penetration by unauthorised outsiders in 2015, while 90 per cent of large firms experienced a security breach of some sort (the median number of breaches was 14). These relate only to detected incidents; the real numbers are probably much higher. Many companies are turning to cyber insurance as a means of mitigating the risks of breach, but it is often difficult to define exactly where the blame lies and thus whether a breach is covered. In any case, insurance does little to arrest the growth of cybercrime, it simply shifts the costs elsewhere.

In the Press

The EU's forthcoming General Data Protection Regulation (GPDR) is unlikely to do much to reduce cybercrime, either. The GDPR extends responsibility for protecting personal data to almost any business that holds it, no matter their size, including hosted service providers. It may lead to breaches and hacks becoming bigger news, due to increased notification to the Information Commissioners Office (ICO) and larger fines to the guilty parties. Organisations will probably put more resources into security and breach prevention as a result. However, the increased expenditure will probably only divert criminal activities towards softer targets.

New technologies and services, like advanced encryption, two-factor authentication and password managers, will improve the defence against current threats. However, once their use becomes widespread, cybercriminals are likely to repeat the patterns of the past and shift their focus to other, as yet unidentified vulnerabilities. To get ahead of the criminals, we need to change the way we do things.

Everyone should understand that cybercrime is a threat to all organisations, whatever their size or type. It will continue to grow and nothing that the government or the regulators are doing at the moment is likely to curtail it.

Therefore, it is up to business leaders to recognise the threat and to ensure that their organisation is adequately prepared and protected. Unfortunately, according to PwC's Global Economic Crime Survey, only 37 per cent of companies have any kind of cyber incident response plan, and fewer than 50 per cent of company board members have ever requested information about their organisation's cyber-readiness. Astonishingly, as of 2015, 32 per cent of organisations had not conducted any form of security risk assessment at all. This suggests a serious lack of risk awareness and good governance in far too many firms.

Technology has become integral to most business operations, and almost all of that technology is networked. This means that cybercriminals can gain access to sensitive data or intellectual property via almost any part of the business. Lost data can be replicated and distributed at will, so a breach can never be truly resolved, and serious data losses may even threaten business viability. This makes cybercrime a serious strategic risk, and plans for prevention and mitigation deserve the highest priority. However, many business leaders are content to leave cyber security to the IT department, in the belief that technology can fix the problem. This is a dereliction of their duty to shareholders, and reflects a fundamental misunderstanding of the threat, which is primarily linked to user behavior.

In the Press

The process of risk management should be the same as for any other threat. The first step is to understand what makes the organisation an attractive target to cybercriminals, and where the main vulnerabilities lie. Tackle these by breaking them down into appropriate tasks and responsibilities, assign those to the right people, and ensure that each has visibility at a senior level. Monitor all actions taken, and once the appropriate measures are in place, ensure they are tested continuously and audited regularly.

Ultimately, the aim should be to embed cyber security into all business processes. This won't stop your company from becoming a target, but it will allow you to withstand the attack with minimal loss.

Matt Eddolls, Head of Risk Change, CoreStream

ENDS