Cybersecurity Part I: Lessons from James Bond's 'Spectre' | back to top

Fans of the recent James Bond, Spectre, will be aware of the dangers around handing the Intelligence Service to a megalomaniac know-it-all and entrusting global surveillance to a jilted psychopath with an unhealthy obsession with control and revenge. Underlying Spectre's almost fantasy storylines, gadgets and villains is a real threat to individuals, institutions and national security alike: cyberattacks. As the top concern for organisations in 2016 and in light of the successful attacks since Christmas on organisations we might have expected to be impenetrable, including the BBC and the Ukrainian Power Grid, cybersecurity clearly must be taken seriously, but what does this mean in practice?

Cybersecurity refers to the necessary provision of protection, from unlawful use, access or interference, for:

- electronically-stored information; and
- communication networks integral to contemporary society, business and government.

As Spectre demonstrates, information is power and not everyone shares the same vision of using it "for the good of mankind". Most organisations hold information that could be potential targets for cybercrime, including:

- Information held on employees or workers (addresses, bank details, communications etc.);
- Information held on consumers/students (names, payment and account details, disciplinary record etc.); and
- Confidential information in contracts with third parties.

The risks for universities can be just as precarious as for other businesses and networks. A successful cyberattack can result in claims for compensation by individuals for damage and distress caused by the unlawful obtaining, release or use of their personal data. If a university has failed to comply with obligations to keep information (and networks) secure, then it could also face prosecution or sanctions, and authorities can publicise their investigations. The inevitable reputational fallout from the publication, media coverage and obligation of the university to inform its stakeholders can be devastating, as has been the case for TalkTalk and Ashley Madison.

Protection is therefore crucial. Current legislation attempts to prevent cyberattacks by imposing obligations on institutions and there are more on the way. The EU is currently in the process of agreeing EU-wide rules on cybersecurity. These will look to improve national cybersecurity capabilities and encourage cooperation between member states. The proposed directive will also create security and notification requirements for operators of essential services and for digital service providers, including services such as cloud computing, search engines and online marketplaces.

A challenge for universities is that cybercriminals are constantly developing new technologies which require reciprocal updates in defences. Although some organisations will need complex security systems, the majority of security breaches occur where organisations have failed to implement even basic protection. Minimal protection includes encrypting stored information and using policies for handling data, updating software protection and training employees with access to certain information. Other practical means of protection include:

- Carrying out checks and vetting employees with access to personal data;
- Ensuring security training for employees and users. Humans are usually the weakest link in safeguarding security
- Ensuring agreements and policies are in place for third party access to personal data or confidential information; and
- Preventing insecure use of removable devices and media (memory sticks/portable computers), by scanning for viruses before introducing new hardware or software, limiting media introduced and implementing safe use policies etc.

It doesn't take a genius to work out that prevention is probably the best cure. Universities will individually need to assess where their vulnerabilities lie, analyse the risk and implement policies and practical solutions to ensure compliance. Understanding the risks and introducing at least some protection is half the battle. Regardless of the extent of implementation, cybersecurity will never be able to prevent all attacks, but organisations have an obligation to at least demonstrate compliance with legislation and a willingness to invest in this area. Few universities will have their own "007" to save the day from cyberattacks, making cybersecurity all the more important.

GCHQ together with the Centre for Protection of National Infrastructure (CPNI) has re-issued guidelines and advice on cybersecurity. You can find out more on the following websites:

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

http://www.cpni.gov.uk/

http://europa.eu/rapid/press-release_IP-15-6270_en.htm

Lydia Stone-Fewings
Trainee Solicitor, Commercial
T: 0121 214 0315
E: lydia.stone-fewings@shma.co.uk