CYBER SECURITY & REAL ESTATE

CUSHMAN & WAKEFIELD

October 2015

Is it **their** problem, **your** problem or **our** problem?

Hacktivism has now reached unprecedented levels. Major organisations and corporates are rarely out of the news from compromises by nation states, organised crime, competitors and individuals. With relative ease, an invisible enemy can find its way into a rich trove of trade strategy documents, IP related to product design, and large volumes of consumer data that can be exploited, sold or used for economic or military gain. It is, however, our employees who remain the most cited culprits of incidents from loss of devices, poor device protection or falling victim to phishing and become unintended accomplices.

The theme of insider threat emerged very strongly at CoreNet Global Summit's panel debate in London this September. Daniel Cuthbert, the COO of Sensepost, a global security firm that specialises in ethical security testing, used his software to demonstrate device vulnerability amongst CoreNet's audience. The level and extent of vulnerability was astonishing.

77Million

Number of gamers whose details were **stolen** from Sony's Playstation network in 2011

Cuthbert explained that whilst firms can protect their architecture and data with malware detection, vulnerability scanning tools and other types of controls and encryption, we leave ourselves exposed from two major threat sources; Bring Your Own Device policies and free wifi. Both provide easy gateways. For him, the answer to the question lies with you and me and a basic duty of care.

But it became clear in the debate that real estate also needs to transform its awareness on the topic, and understand where it fits as well. Erwin Franz-Schultz, IT architect and Technical Head of IBM's Energy & Utilities sector, outlined the vulnerabilities of enterprise networks, IP and software which are now commonly used in the built environment to control services, safety systems and plant.

550

Data breaches in US universities between 2006 and 2013

As a leading expert in smart grids and cyber security, he expressed the view that cyber attacks are no different to any other risk faced in scenario testing and disaster recovery planning. It simply happens to be a different type of threat which needs its own assessment and mitigation plan. Brian Lord, an expert in national intelligence and cyber operations, now with PGI Cyber following a career with GCHQ as Deputy Director reinforced this by urging the audience to normalise the threat. By this he meant, understand the incident, and in simple risk management terms understand the risk severity and probability of occurrence. He also meant remove the emotion of the media. Most Cyber attacks would be described as theft, blackmail, vandalism or anti-social behaviour if reported in the non-Cyber world.

Despite the pragmatism, he did underline Cuthbert's view about personal responsibility and outlined how responsible organisations implement and maintain systems for storage and transfer of sensitive information and why disciplines around encryption remain highly effective.

Lord flagged up the role of property and its advisors in supply chains. In an outsourced world with complex supply chains, we are reliant on information security arrangements from multiple providers, and in turn hold data on behalf of other parties reliant on the rigour of our own information security. Yes, Codes of Practice for Cyber Security in the Built Environment and International Standards for Information Security Management Systems, but the question remains whether we know yet what good looks like, or indeed how to answer any procurement teams questions properly ourselves. With new EU General Data Protection Regulations proposing fines of up to 5% of global turnover for data protection penalties, answers to these questions need to be found quickly.

$110Million

Number of payment card records **stolen** from Target Corporation through the company's HVAC contractor in 2013

$252Million

Target's gross financial **loss** in 2014 as a consequence

$80Billion

Global IT **security spend** in 2015

4% or less

of a typical IT budget is spent on **Cyber Security** (last 5 years)

Those who are spending **more**?

Healthcare Providers

Oil & Gas

Utilities

71%

of compromises go **undetected**

(PwC – Global State of Information Security Survey 2015)

CONTACTS

Michael Creamer

Head of Enterprise Client Solutions: EMEA
Global Occupier Services
michael.creamer@cushwake.com
T: +44 207 152 5080

Keith Inglis

Partner, EMEA
Global Occupier Services
keith.inglis@cushwake.com
T: +44 207 152 5874

10 CYBER SECURITY TIPS FOR REAL ESTATE & FACILITIES MANAGEMENT PRACTITIONERS

1 Training and awareness.

2 Use classification systems for distribution of sensitive information – highly classified material will carry encryption and other protection.

3 Implement business guidelines on handling of data, device use, and requirements from the supply chain. Remember that they need to be embedded into your supply chain of service providers, consultants and contractors, and that starts with vendor risk assessments.

4 Protect your network – there is a vast array of products to protect networks, software and devices – companies currently spend less than 4% of their total IT budgets on cyber protection.

5 Spend time understanding the system architectures, protections and controls in buildings that you occupy, but which may be outside of your operational control. Make sure that the landlord has undertaken a vulnerability assessment from a reputable security systems specialist and shared its findings with you.

6 As with any disaster recovery planning, develop well worked out responses to different threats.

7 Stop being so trusting – ask why something is free.

8 There's no excuse for poor passwords.

9 Get the debate at board level, and help them to understand the reputational, financial and competitive risks they face without a robust management strategy.

10 Risks and responses evolve at lightning speeds. Active collaboration with industry groups keeps you connected to the conversations.