Managing real estate cybersecurity
Managing real estate cybersecurity

Cybersecurity, which is viewed as one of today’s most prominent threats, has not yet been highlighted as a key issue for the real estate sector. However, with the transition to intelligent buildings, SMART everything, enabled by the Internet of Things and the matter of corporate liability, concerns within the sector are now rapidly changing.

So, how real are the threats and what actions should the sector take to mitigate the risks? This goes way beyond IT, and has an immediate impact not only on their corporate real estate, but also on their ability to manage their investment portfolios.

Setting the scene: today’s cyberthreats

It is a cold, rainy day in London in the run up to Christmas, and shoppers have moved to retail centres to keep dry and warm as well as continue their Christmas shopping.

Suddenly, without warning, temperatures start to rise. People are beginning to sweat in their winter clothes and wilt in the heat. The fire extinguishers and sprinkler systems go off, chaos ensues and the whole shopping centre has to be cleared, fast.

The security guards are scratching their heads, completely clueless as to what is happening, particularly as their systems are telling them there is no fire and nothing wrong with the building temperature control – nothing mechanical at least.

The problem, which has not yet been identified, is that the shopping centre’s brand new, all-electronic building management system has been hacked, and the hacker is now manipulating all the controls.

It is not where one would expect hackers to attack, but the potential for disruption to businesses is just as great as for any virus or theft of information.

This is a hypothetical situation of course, but one that could potentially happen in just about any large new building, demonstrating the need for a coordinated approach to security from the real estate sector.
Managing real estate cybersecurity

Owner liability

Gone are the days when a company could focus solely on the physical aspects of security; instead, attention today is turning to a new digital challenge.

Building management systems, which handle everything from air conditioning to closed circuit television, access control, lighting and door locks, traditionally worked on serial networks and were segregated from conventional IT networks.

As these systems have become internet enabled, they are now open to all possible threats that afflict conventional IT systems.

The potential for harm is significant. In real estate, the most immediate impact is likely to be felt by the tenant of the building rather than the owner, with loss of sales from collateral impact and loss of clientele.

The longer-term impact is then felt by the real estate company as it is forced to compensate its tenants for loss of trading revenues and brand reparation when the true cause of the incident is discovered.

Security vulnerabilities

Building management systems are open to abuse because their networks tend to be managed by facilities managers or security guards, often little or no background in IT or networking.

As a result, building management systems can fail basic security requirements, despite the increasing trend towards intelligent buildings to help reduce energy wastage and inadequate security.

This has prompted manufacturers of lighting, access control, heating and air-conditioning systems to try and build standards that leverage the Internet of Things and support better integration of previously disparate systems.

Much of this effort falls under the umbrella of the Open Building Information Exchange, whose aim is to establish and maintain a standard XML and Web Services guideline to facilitate the exchange of information between intelligent buildings, enable enterprise application integration and deliver real systems integration.

Yet many of these systems are being designed without keeping cybersecurity protection measures and controls in mind.

For example, a quick online search will reveal each building management system controller is used at which Heathrow Terminal, which would enable a would-be attacker to start planning an attack by simply by purchasing one of the products and testing it.

While it would be difficult to know exactly how these systems are configured, an attacker would be able to determine the base product through open-source information.

The fundamental issue is that the controller, embedded operating system and web server have not been protected to any significant degree.

This is a common concern with embedded operating systems, as they are hard to patch and update, and are often overlooked since they are not maintained by traditional IT teams. They instead operate on legacy technology, installed or upgraded only once every 10–15 years.

Protecting your assets

Cybersecurity and physical security staff have a shared purpose: asset protection.

The key, however, is to identify the full extent of assets being protected, as the sector’s physical assets provide a vector to a more damaging and broader population of organisations.

Real estate firms should focus on the business impact of risk and, in doing so, ensure that traditionally divergent management controls and disciplines share a common language and develop a mutual respect and collaborative approach between cybersecurity and physical security staff to address each other’s concerns.

This will include understanding the various regulations and guidelines that each have to follow, which may at times be conflicting.

The consequences of a security system failure could be catastrophic. In recent years, such failures have led to many well-publicised data breaches.

Indeed, such is the prevalence of cybersecurity incidents that many would say there are now only two types of organisations: those that have been hacked and are aware, and those that have been hacked but remain blissfully unaware of their exposure.

The case of the data breach

The past 10 years have seen an unforeseen level of data breach incidents.

The Identity Theft Resource Centre is forecasting that the financial impact of cybercrime will continue to grow by 10% annually until the end of 2016.

The Ponemon Institute has conducted a research project to identify trends in reported cyberattacks.

These reported events have resulted in technical invasions, including reported instances of viruses, worms or trojans infiltrating the company’s computer system, malware, web-based attacks, stolen or lost devices, employee error (negligent or intentional), phishing and social engineering.

With criminals stealing everything from customers’ identities to bank account details, public anxiety is growing almost as quickly as criminals and hackers are devising new methods to infiltrate ‘secure’ systems.

Within the sector, property managers, brokers/agents, developers, appraisers, multiservice real estate firms and others hold significant amounts of confidential third-party information, either in the form of personally identifiable information or confidential corporate information stored in rental applications, credit reports, leases and rental agreements – all the type of information cybercriminals target.

Having measures in place for the maintenance and destruction of confidential records will ensure that such data is only held for as long as justifiably required, to safeguard against possible identify theft and ensure compliance with data protection and privacy laws.

The confidential data stored across multiple online and mobile devices must all be protected and/or adequately disposed of.

This can be achieved with software that automatically wipes information from hard drives and prevents restoration of material that has been deleted.

Real estate investment trusts (REITs), which are a multi-trillion-pound industry, own and operate income-producing real estate or engage in financing real estate. Depending on the REIT structure (public versus private) and type of investor (individual or corporation) information and intelligence held by REITs need measures to prevent, or at least minimise, the risk of data and financial loss.

---

**Managing real estate cybersecurity**

Misappropriated customer or tenant information from lost laptops, for example, can result in significant liability for an owner and/or landlord.

In a report, *Unprepared for security breaches*, Symantec found that 80% of the data breaches reported happened to organisations that did not rely on the internet as a core piece of their business. These losses resulted from stolen or lost equipment.

Symantec’s report also found that of the 46% of reported lost laptops containing confidential data, only 30% were encrypted and just 10% had other anti-theft technologies.

While real estate firms increasingly look to outsource the storage of information to gain effective, cost-friendly IT services, the use of third-party IT systems needs to be appropriately managed by placing contractual responsibility, such as reporting breaches, on their service providers.

---

**The loss of data**

---

**The cost of cybercrime**

The key area where companies lack awareness of the financial impact is the cost of remediation.

Awareness of cybercrime may be increasing, but the cost associated with remediating these attacks has been slow to unfold.

According to the Ponemon Institute, the most expensive cyberattack experienced in their 2014 study incurred more than US$51m in damages and remediation costs; the smallest was still over US$1m, and the average expenditure to remediate these attacks was US$7m.

The average cost of a forensic investigation into a lost laptop today is about US$50,000, 80% of which is related to data breach fines and remediation packages for impacted customers and personal data owners, compared with just 2%-3% for the cost of replacing the computer.

To investigate and remediate a breach, forensic companies are often hired to identify its source, which adds further costs.

Expenses associated with notifying those whose confidential information may have been compromised can also be significant.

Responding to breaches may also negatively impact productivity, drawing on crucial company resources in an attempt to respond quickly and effectively.

Finally, network interruptions can also lead to loss of income and generate unnecessary additional expenses for real estate firms and their tenants who rely on their network to run their daily business, thereby creating the potential for further liability.

Combined, these liabilities and costs can escalate into millions, damaging the balance sheets of larger real estate firms and crippling smaller businesses.

---


Managing real estate cybersecurity

The regulatory environment

The impact that the ever-changing regulatory environment will have on real estate businesses presents added challenges.

Many countries are adopting statutory requirements for remediation if data protection is deemed inadequate.

The jurisdictional requirements vary across countries with multinational businesses likely to have to comply with multiple cybercrime or data breach measures.

In the US for example, class action lawsuits are typically launched in the aftermath of a data breach. Meanwhile in the European Union (EU), a harmonisation of the current 28 national directives into one new EU General Data Privacy Regulation will result in significant fines of up to 5% of global annual turnover capped at €100m against companies that are culpable for the loss of personal data.

Mandatory breach reporting will be established in the EU, in addition to fines levied by national and international regulators.

As these regulations are being finalised, many real estate firms have yet to scope out and bring their IT and data processing systems up to speed for 2017-2018 when the legislation comes into effect.

EU and UK regulators have publicly stated that there will be no extension to implementation timelines, and ignorance around the new legislations will merely demonstrate a breakdown in good corporate governance.

How real estate firms, therefore, decide to respond will have a substantial impact not only to their tenants’ and their own operational performance, but also increasingly on their overall corporate brand reputation.

In summary, it is therefore clear that the issue of cybersecurity in the Real Estate sector is both a very clear and present risk, but also one that now needs to be tackled proactively by Real Estate firms. Impending legislation will further focus the minds of organisations to address these risks, often overlooked in previous years. The convergence of physical and technical security brings greater challenges to organisations and the consequences are now such that the impact of a cybersecurity incident can have far reaching implications for both real estate organisations and tenants. Good cybersecurity can be an enabler to businesses in today’s interconnected and ever increasingly connected world and therefore, adapting a business focussed and proactive approach to cybersecurity risk management will reap wider benefits rather than simply offer protection to previously unaddressed risks.
EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Global Real Estate, Hospitality and Construction Sector
Today's real estate, hospitality and construction sector must adopt new approaches to address regulatory requirements and financial risks, while meeting the challenges of expanding globally and achieving sustainable growth. EY's Global Real Estate, Hospitality and Construction Sector brings together a worldwide team of professionals to help you succeed – a team with deep technical experience in providing assurance, tax, transaction and advisory services. The Centre works to anticipate market trends, identify the implications and develop points of view on relevant sector issues. Ultimately it enables us to help you meet your goals and compete more effectively.

© 2015 EYGM Limited.
All Rights Reserved.

EY No. DF0223
14261.indd (UK) 09/15. Artwork by Creative Services Group Design.
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com