Six Cybersecurity Challenges Facing the Real Estate Industry

The real estate industry has become a hotbed for cyberattacks in recent years, and many companies feel they are not sufficiently protected. According to recent research, 74% say they could be doing more to protect against these cyber vulnerabilities. To put this into perspective, let's examine the most pressing threats that are increasing the sector's risk exposure to damaging cyberattacks.

Six Cybersecurity Challenges and Solutions in the Real Estate Industry:

1. Lack of Security Oversight and Regulation

THE CHALLENGE: Given the lack of stringent Cybersecurity regulations in the real estate industry, your business may be inadvertently holding itself less accountable for maintaining high standards of data protection. This creates vulnerabilities that not only put your clients' sensitive information and financial data at risk, but also expose your business to substantial financial losses.

THE SOLUTION: Implement a regulatory compliance management framework, such as NIST CSF or NIST 800-53, do regular assessments against the associated controls, and put a plan in place to address any gaps.

> ***74%*** *say they could be doing more to protect against cyber vulnerabilities*

2. Rapid Proliferation of IoT Devices

THE CHALLENGE: The recent adoption of Internet of Things (IoT) and Operating Technology (OT) devices has significantly expanded the sector's attack surface. While these devices provide sophisticated capabilities, like those used to monitor and control buildings, they often lack adequate security controls, which gives hackers easy access to sensitive information, critical systems, and networks.

THE SOLUTION: Ensure your IoT and OT devices have robust security protocols in place or are configured to operate without internet exposure. For example, many IoT devices come with a default password which should be changed. Additionally, you should ensure these e-devices are inventoried and regularly patched.

3. Rise in Contract Workers and Temporary Employees

THE CHALLENGE: You may be exposing your business to heightened security risks if you rely on contract workers and temporary employees to manage your IT infrastructure. Although many of these workers may be trained in Cybersecurity practices, they may not be aware of, or as committed to, your company's security protocols as your full-time employees.

THE SOLUTION: Before onboarding your contract or temporary worker, ensure they are adequately trained in Cybersecurity practices, educate them on your company's policies and procedures, and set expectations regarding their adherence to those practices. We also suggest that you use the principle of least privilege (PoLP) when assigning access to these workers. Only give them access to the systems and data they absolutely need to perform their job. As soon as the contract is over, revoke their access.

4. Limited Attack Surface Visibility

THE CHALLENGE: Organizations that oversee several properties with each operating their own unique IT infrastructures will struggle to gain comprehensive insights and control over the entire technological landscape. Without a unified view across properties, you may not be able to spot and address vulnerabilities, which can increase the risk of undetected security breaches.

THE SOLUTION: Adopt a unified IT platform that consolidates technology across all sites, providing a holistic view and highlighting key performance indicators (KPIs) on a user-friendly dashboard. This cohesive approach ensures threats are swiftly identified and addressed using the right technologies. A unified platform ensures that all properties adhere to the same strict security guidelines, reducing points of vulnerability.

5. Substantial Cash Flow

THE CHALLENGE: The sector's extensive cash flow and access to sensitive data like bank accounts and personal identifiable information (PII) make it a desirable target for cybercriminals. Plus, the massive volume of daily fund transfers gives hackers ample opportunities to intercept and redirect those funds.

THE SOLUTION: Implement a robust Cybersecurity program that includes advanced software, continuous training, and multi-layered defense mechanisms to safeguard financial transactions and sensitive data.

6. Physical Security Overlaps

THE CHALLENGE: Modern real estate properties often blend digital and physical systems. Buildings utilize digital controls and physical access points like doors or elevators, which, when compromised, can grant unauthorized access. The rise of internet-connected devices enhances functionalities but also expands vulnerability avenues. Real estate offices store sensitive digital data, making them targets for breaches. Moreover, many security measures, such as electronic locks, rely heavily on uninterrupted power and connectivity, and any disruptions can render them ineffective, exposing properties to threats.

THE SOLUTION: Ensure that networks for critical physical security infrastructure are separated from regular business networks. This minimizes the risk of a compromise in one area affecting the other. Physical access control systems, like any software, need regular updates to protect against known vulnerabilities. Ensure this software is part of the regular update schedule. For smart buildings, ensure the use of devices from reputable manufacturers that adhere to recognized security standards.

A Cybersecurity breach can have devastating consequences for your business, putting your financial assets, your clients' trust, and your reputation in jeopardy. By embracing proactive and comprehensive security strategies, enforcing stringent security protocols, and fostering a culture of Cybersecurity awareness and responsibility, you can safeguard your organization against the multifaceted cyber threats that loom in the digital landscape.

For more information about how we can help you navigate the complex cybersecurity risks facing the real estate industry, contact us here.