CUSTOM HOUSE
RISK ADVISORS

Cyber Insurance for Residential and Hospitality Real Estate Owners

BY GEOFFREY MILLER, ESQ. AND THOMAS HUNT, ESQ.

CUSTOM HOUSE
RISK ADVISORS

CONTENTS

INTRODUCTION

The real estate sector, and in particular the habitational and hospitality asset classes, thrive on trust. Guests in hotels and tenants in apartment buildings entrust their landlord or property manager with their personal information, financial details, their personal property, and a sense of security. In today's interconnected digital age, this trust extends to the cybersecurity measures you have in place as well. A data breach or cyberattack can shatter that trust, leading to financial losses, reputational damage, and even legal trouble.

In this white paper, we will explore the growing cyber threats facing the hospitality industry, and examine why cyber insurance is no longer an optional component of your company's data-protection plan, but a key necessity to ensure successful continued operation. Herein, we'll delve into the specific risks you might face, the benefits of cyber insurance, review the best practices for minimizing your risk profile, and advise on how to secure better insurance coverage.

PART 1: WHY DO APARTMENT AND HOSPITALITY OWNERS AND OPERATORS NEED CYBER INSURANCE?

These asset classes are prime targets for cybercriminals due to the vast amount of sensitive data they collect and store, including: Guest/tenant names and contact information, social security numbers, payment card/bank account details, passport information, and travel documents.

A successful cyberattack can compromise this data, leading to a cascade of problems:

Financial Loss from Claims: Victims of identity theft can incur significant financial losses due to fraudulent charges and attempts to open new accounts in their name. You, as the property owner/operator, may be held liable for these losses if the breach stemmed from inadequate security measures.

Response and other First-Party Expenses: There's also the cost of responding to the incident, the loss of data or "bricking" of equipment, and other first-party expenses.

Reputational Damage: News of a data breach can severely damage your reputation and brand image, leading to lost business and difficulty attracting new tenants/guests.

Regulatory Fines: Data breach notification laws mandate that affected individuals be notified within a specific timeframe. Failure to comply can result in hefty fines from regulatory bodies. For owners and operators with operations in Europe, noncompliance with the EU's General Data Protection Regulation (GDPR) can result in fines of up to 4% of a company's global revenue or €20 million, whichever is greater. Some regulatory bodies may even seek an enforcement action or payment of damages just for the data breach itself, depending on the facts and circumstances.

Business Interruption: Bookings, reservations, and showings may no longer be possible, leading to lost income.

Cyber insurance provides a critical financial safety net, helping you navigate the complexities and costs associated with a cyberattack. They can mean the difference between recovering quickly and facing financial ruin.

PART 2: **The Biggest Cyber Threats to the Hospitality Industry**

Here's a closer look at some of the most common cyber threats faced by apartment buildings and hotels:

Ransomware: This type of malware encrypts your data, rendering it inaccessible until a ransom is paid. The ransom is often required to be made in cryptocurrency to mysterious bad actors in foreign countries, which can create legal issues. Ransomware attacks can cripple your operations, preventing guests from accessing their rooms or tenants from paying rent online.

Social Engineering: Cybercriminals use deception to trick employees into revealing sensitive information or clicking on malicious links that can infect your network with malware. Common tactics include phishing emails, smishing attacks (text message scams), and vishing attacks (phone scams). Once inside your network, attackers can steal data, launch further attacks, or commit funds transfer fraud.

Data breaches: Hackers can exploit vulnerabilities in your systems to gain unauthorized access and steal sensitive data. This can occur through brute-force attacks, malware infections, or unpatched software vulnerabilities.

Fund Transfer Fraud: Social engineering tactics are often used to perpetrate this type of fraud. Hackers may impersonate a vendor or executive and trick employees into authorizing fraudulent wire transfers.

PART 3: **What is Cyber Insurance and How Does it Help?**

Many apartment and hospitality owners and operators say that they already have plenty of insurance. They maintain commercial property, general liability, and other traditional insurances to protect their business. Why wouldn't those cover a cyber-attack or data breach? The problem with this is it has become increasingly standard for carriers on these traditional insurance lines to broadly exclude cyber risk because they do not want to cover the size and scope of these losses, necessitating a separate product.

Cyber insurance is a specialized insurance policy designed to protect businesses from the financial repercussions of cyberattacks. Unlike traditional insurance, cyber insurance goes beyond just data recovery. It offers immediate assistance in the aftermath of a cyberattack, providing access to a network of pre-vetted vendors critical for incident response:

Breach Counsel: Legal experts who guide you through regulatory compliance, notification requirements, and potential litigation. These experts can assist with certain acts, like ransom payments, that require legal advice to ensure there is no OFAC or other legal violation.

Cyber Forensics: Specialists who investigate the attack, identify the scope of the breach, and collect evidence.

Public Relations (PR): Professionals who help manage the reputational fallout from a data breach and communicate effectively with tenants/guests.

Threat Actor Negotiation: In ransomware situations, someone to communicate and negotiate with the threat actor.

Call Centers, Notification, and Credit Monitoring Services: Data breach notification laws may require you to notify and protect thousands or even hundreds of thousands of people. Cyber policies generally come with services to handle this for you. This is in addition to the financial coverage as many cyber insurance policies offer coverage for:

Network Security Liability: Covers costs associated with data breaches caused by your network security failures including lawsuits and regulatory claims.

Privacy Liability: Covers costs associated with privacy violations, including wrongful data collection claims.

Business Interruption: Covers lost revenue due to a cyberattack that disrupts your operations. Rebuilding or Recovering Data: Covers costs to get your network and data back to the pre-loss state.

Social Engineering & Wire Fraud: Covers the response and funds lost when someone at the company is tricked into sending money to a fraudster's account.

Media Liability: Covers costs associated with copyright claims, unauthorized use, rights or privacy violations, libel and slander, and other misuse or unfair competition-related claims.

Ransomware: Covers costs incurred resulting from a ransomware threat, including money and cryptocurrency, and costs incurred to mitigate or reduce such expenses, including negotiation.

In some cases, depending on the specific policy, cyber insurance may even provide funds to assist with paying a ransomware demand, as a last resort to restore access to critical systems and minimize downtime.

PART 4: Cyber Insurance is Not as Expensive as You Think

As we've discussed, the risk of cyber-attacks isWhile cyber insurance is an additional expense, the cost pales in comparison to the potential financial losses incurred during a cyberattack, as well as the cost of your other traditional insurance lines. Premiums are determined by several factors, including the size of your organization, its income, the type of data you store, and your existing security posture.

By implementing strong cybersecurity measures, you can significantly lower your risk profile and secure more affordable cyber insurance coverage. Here are some safeguards to consider:

Multi-Factor Authentication (MFA): MFA is now practically a requirement for obtaining cyber insurance. It adds an extra layer of security by requiring a second verification step beyond a username and password. This could involve entering a code sent to a registered phone number, using a fingerprint scanner, or authenticating through a dedicated security app.

Employee Training: Regularly train your staff on cybersecurity best practices. This should cover common social engineering tactics, phishing email identification, password hygiene, and the importance of reporting suspicious activity. Implement the rule of least privilege, i.e., a given employee/user should only be given minimum access to sensitive data accomplish a legitimate business task. This limits the damage that can be caused by rogue employees.

Phishing Simulations: Conduct regular phishing simulations to test employee awareness and preparedness. These simulations send simulated phishing emails to employees and track who clicks on malicious links or enters their credentials. This helps identify knowledge gaps and allows you to tailor training programs accordingly.

Cybersecurity Policies: Develop and implement clear cybersecurity policies that outline acceptable use of technology for employees and guests. These policies should address topics like password complexity requirements, data security protocols, and proper handling of guest information. These policies should outline administrative, technical, and physical safeguards that must be taken for sensitive data that the company stores.

Endpoint Security Solutions: Implement endpoint security solutions like firewalls and antivirus software on all devices connected to your network. These tools can help detect and prevent malware infections, including ransomware.

GUESTS IN HOTELS AND TENANTS IN APARTMENT BUILDINGS ENTRUST THEIR LANDLORD OR PROPERTY MANAGER WITH THEIR PERSONAL INFORMATION, FINANCIAL DETAILS, THEIR PERSONAL PROPERTY, AND A SENSE OF SECURITY. THIS TRUST EXTENDS TO THE CYBERSECURITY MEASURES YOU HAVE IN PLACE.

Regular Security Assessments: Conduct regular vulnerability assessments and penetration testing to identify weaknesses in your network security. This proactive approach allows you to address potential security gaps before they can be exploited by attackers.

PART 5: Claim Examples: Social Engineering Funds Transfer Fraud

This happens every day. A bad actor impersonates a legitimate vendor via email, phone, or invoicing and convinces an accounts payable employee to authorize a wire transfer to their account. This can be a totally fake payment or redirecting a legitimate payment to the fraudster's account. The employee, unaware of the scam, authorizes the transfer, resulting in a significant financial loss for your property.

HOW CYBER INSURANCE HELPS:

Most basic cyber policies include a sublimit for social engineering fraud which can cover the following:

Forensic Investigation: Cyber forensics experts to be deployed to investigate the attack, determine the scope of the fraud, and identify the perpetrators (if possible).

Legal Expenses: Legal counsel to help you recover the stolen funds and potentially pursue legal action against the attackers. However, it's important to note that recovering stolen funds is not always guaranteed.

Reimbursement for Lost Funds (Up to Sublimit): Your cyber insurance policy may reimburse you for the stolen funds up to the remaining sublimit amount, mitigating the financial impact of the fraud.

IMPORTANT CONSIDERATIONS:

Sublimits and Coverage Stacking: While your cyber insurance policy offers valuable protection against social engineering fraud, it's crucial to understand sublimits. For example, your policy may cover up to $250,000 in losses stemming from social engineering. If the fraudulent transfer had been for a higher amount, you would be responsible for the remaining balance.

Commercial Crime Policies and Fidelity Bonds: For additional coverage against employee theft and fraudulent activity, consider exploring what is available from commercial crime policies or fidelity bonds. These can often be "stacked" with your cyber insurance policy to provide additional total limits. When doing this, it's important to structure priority of coverage and deductibles to have as much insurance as possible without any donut holes or a second deductible for going between layers.

Traditional Funds Transfer Fraud and Wire Fraud Coverage Isn't the Same: Usually policies provide larger limits for traditional wire fraud, which is tricking the bank, not tricking your employee. The latter is typically excluded, and it instead falls under the narrower (and often optional) "Social Engineering" or "Fraudulent Instruction" coverage.

PART 6: Claim Examples: Ransomware and Data Breach

Imagine a worst-case scenario: a sophisticated ransomware attack cripples your property management system. Hackers encrypt your data, preventing tenants from accessing online portals and disrupting core business operations. The attackers begin to slowly exfiltrate the sensitive information of 100,000 tenants across the country and leak it on the dark web in an effort to pressure a ransomware payment.

How Cyber Insurance Helps: In this harrowing situation, your comprehensive cyber insurance policy can offer a lifeline:

Incident Response: Cybersecurity experts would be deployed to contain the attack, isolate infected systems, and assess the scope of the damage.

Threat Actor Negotiation: You wouldn't have to face this crisis alone. Your policy would likely provide access to a dedicated negotiator with extensive experience in dealing with cybercriminals. This expert would work tirelessly to negotiate a lower ransom demand, potentially mitigating your loss.

Ransom Payment (Policy and Legality Dependent): While cyber insurance generally discourages paying ransoms, some policies may consider it a last resort to restore critical operations and minimize downtime. The decision to pay would involve careful consultation with your cyber insurance provider, legal counsel, and the negotiator.

Data Recovery and Rebuilding: Recovering from a ransomware attack goes beyond simply paying a ransom. Your cyber insurance policy would likely cover the costs associated with:

Data decryption: Utilizing specialized tools and expertise to unlock your encrypted data.

Data restoration: Rebuilding lost data can even include going back to the first-party sources to rebuild data sets like tenant, HR, and sales files when no other means are available.

Hardware replacement: In some cases, if the attack damaged critical hardware, your policy might cover the cost of replacement. This is generally referred to as a "bricking" sublimit.

Legal Expenses and Breach Coaching: Your policy would likely provide legal counsel to guide you through the complex legal and regulatory landscape following a data breach. An attorney-breach coach would be assigned to help you navigate the notification process, ensure compliance with data breach laws, and potentially pursue legal action against the attackers.

Credit Monitoring and Public Relations: Protecting your tenants' personal information is paramount. Cyber insurance can cover the cost of providing credit monitoring services to affected individuals for a set period, mitigating

the risk of identity theft. Additionally, your policy might provide access to PR professionals experienced in managing reputational damage and communicating transparently with tenants, the public, and regulatory bodies.

CONCLUSION AND NEXT STEPS

Cybersecurity threats are an unfortunate reality in today's digital world. By implementing robust cybersecurity measures and securing comprehensive cyber insurance coverage, apartment building and hotel owners and operators can significantly mitigate risks and protect their businesses from financial devastation. Remember, cyber insurance is not just about recovering from an attack—it's about comprehensive protection throughout the entire incident response lifecycle. Don't wait for a cyberattack to happen before taking action. Invest in your cybersecurity posture and secure cyber insurance to safeguard your property, your reputation, and the trust of your tenants and guests.

HOW CUSTOM HOUSE RISK ADVISORS CAN HELP

Partnering with a risk management consultancy like Custom House Risk Advisors can significantly enhance your cybersecurity posture and help you navigate the complexities of cyber insurance. Here's how our expertise can benefit you:

Securing the Best Cyber Insurance Coverage: Our team of experienced professionals understands the ever-evolving cyber risk landscape and the nuances of cyber insurance policies. We can work with you to identify your specific needs and negotiate with insurance providers to secure the most comprehensive and cost-effective coverage possible.

Contractual Risk Transfer: Our contract review team which includes several attorneys can review your management agreements, network security vendor agreements, and other applicable contracts to ensure that cyber risk is transferred to third parties to the extent possible and that your cyber insurance carriers understand this aspect of your profile, to provide best pricing accordingly.

Cybersecurity Audits and Improvements: We can conduct a thorough audit of your existing cybersecurity measures, identifying vulnerabilities and recommending additional safeguards for improvement. This proactive approach can significantly reduce your risk of a cyberattack and potentially lower your cyber insurance premiums.

Collaboration Across Departments: A successful cybersecurity strategy requires collaboration between accounting, IT, management, and the insurance broker team. Custom House can function as a bridge, facilitating communication and ensuring all departments are aligned in their approach to cyber risk mitigation.

Navigating Cyber Insurance Applications: These applications are increasingly complex and small errors can be costly. Custom House will work together with accounting, IT, and Management to gather and present your company's information in the best possible light and if there are major hinderances to the application, we can recommend new procedures and solutions to increase security and improve your insurance marketing.

Expert Claims Handling: In the unfortunate event of a cyberattack, our team can guide you through the complex claims process. We'll work with your cyber insurance provider to ensure a smooth and efficient resolution, minimizing downtime and financial losses.

Ongoing Support During Breaches and Ransomware Events: A cyberattack is a crisis situation. Custom House will be by your side throughout the entire incident response process, providing ongoing advice and support. We can help vet and supervise the various vendors provided by the carrier and advise you when it may be time to replace vendors or go a different direction. Sometimes vendors may unconsciously seek to benefit the carrier, as a repeat player, over the insured, so it's important to have someone on your team who only represents your interests.

By partnering with Custom House, you gain a dedicated team of experts who can help you achieve a more secure future. Whether you have cyber insurance, you don't yet, or you just have questions about insurance and best practices, we're here to help.

If you'd like to learn more about how cyber insurance can help your company, please contact a Custom House team member today. ■

For more information on cyber insurance and the essential role it plays in protecting your company's data, reputation, and ongoing success, contact the authors:

Geoffrey Miller, Esq.
gmiller@customhouserisk.com

Thomas Hunt, Esq.
thunt@customhouserisk.com