The Evolution of Cyber Risk in Senior Living Environments

Gallagher

Insurance | Risk Management | Consulting

Cyber

Senior Living

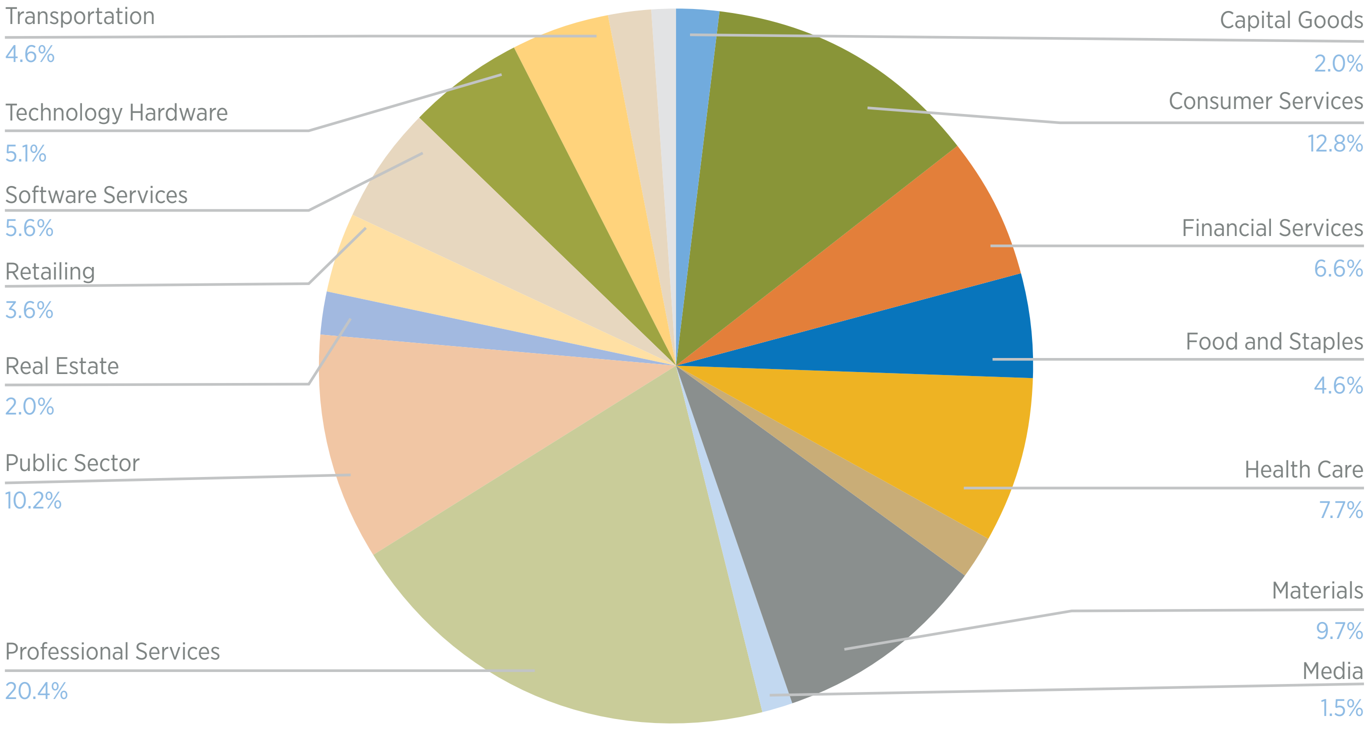
By: John Farley
Managing Director
U.S. Cyber Practice

Those that manage risk in senior living environments have traditionally been focused on perils associated with the physical safety of residents, professional errors and omissions, contractual liability and other forms of risk. However, a comprehensive enterprise risk management approach that reflects today's changing risk landscape calls for a reassessment of what is now impacting bottom lines, brand reputations and most importantly patient safety. Cyber risk has emerged as one such threat that cuts across all sectors and poses a very real threat to senior living organizations.

Today's cyber threat actors favor multiple attack strategies. Ransomware has emerged as the attack method of choice, where malicious software is launched via phishing emails. Once inside a network it often spreads quickly to lock down all data throughout the victim's entire ecosystem, impacting devices, servers, phones and many other integral parts of the organization, effectively ceasing operations. Demands in the six and seven figures are often made in exchange for the release of data. Refusal to pay often results in threats to destroy data or release sensitive data to the public. Legal costs, business interruption, IT forensics investigation costs, regulatory fines and other costs may also follow. To illustrate the bottom line impact of ransomware attacks, Coveware issued a recent report[1] that found that the average ransom payment was $322,168. Even more concerning, business interruption costs could be even greater than the amount of the ransom paid, as the average downtime being 20 days.

In a senior living environment, critical life-supporting medical devices and electronic medical record systems could become inaccessible. What might be an initial financial threat could quickly escalate to an inability to properly care for residents effectively, raising risks exponentially.

Common Industries Targeted by Ransomware Q4 2021



[1] Coveware: Industry Segments that succumb to a Ransomware Attack in Q4 2021

PREVENTING AND MITIGATING RANSOMWARE ATTACKS

Implementing an effective cyber risk management program always starts with obtaining a comprehensive understanding of your environment with insight into security gaps specific to the organization.

Implementing an effective cyber risk management program always starts with obtaining a comprehensive understanding of your environment with insight into security gaps specific to the organization.

The FBI has offered advice on preventing and mitigating ransomware attacks, including:

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication with strong pass phrases where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configures access controls with the least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organization.
- Disable hyperlinks in received emails.
- Focus on cybersecurity awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

TRANSFERRING CYBER RISK

The cyber insurance marketplace offers solutions to transfer risks associated with ransomware and other cyber threats. Policy terms and conditions vary and can be negotiated. Most policies cover both first and third-party costs, and a select few may negotiate coverage to extend to bodily injury and property damage resulting from cyber attacks.

Those that seek comprehensive cyber insurance coverage need to be prepared for a market that is laser-focused on data security controls, with a particular focus on those designed to prevent ransomware attacks. Without these in place, applicants may be subject to higher insurance rates, reduced policy limits, greater retentions and policies that restrict coverage. There is also a distinct possibility that a cyber insurance underwriter will decline to offer terms at all if they are not satisfied that specific protections are in place. Questions around multifactor authentication, remote desktop protocol, privileged access management, data backup practices, email hygiene, incident response planning and employee training will need to be answered.

To that end, it is advisable to work closely with your cyber insurance broker prior to entering the cyber insurance market. Doing so may help you understand where your security controls may be lacking and can provide a roadmap to remediation. Ultimately, the goal will be to be viewed as a best-in-class risk by the underwriting community.

Additional Resources:

Gallagher Cyber Webinar Library
Gallagher Cyber Insights Library

John Farley
Managing Director
Cyber Practice
John_Farley@ajg.com

About the Author

John leads Gallagher's Cyber practice in the U.S. and works closely with our teams across the world in our Global Cyber Practice. He provides thought leadership on a variety of cyber risk management best practices. He assists clients across all industries in navigating the dynamic cyber insurance markets as a means to cyber risk transfer while providing guidance on emerging regulatory risk, cyber attack techniques, cyber risk prevention and data breach cost mitigation strategies.

During his 30 years in the insurance industry, John forged strategic relationships with cyber insurance underwriters, privacy attorneys, IT forensics investigators, and law enforcement. His extensive experience earned him a seat on an advisory board for the U.S. Treasury.

Connect With Us

FirstName LastName

Job Title
Team/practice area/division

Address
Address Line 2 (optional)
T: 123.456.7890
E: firstname_lastname@ajg.com

ajg.com **The Gallagher Way.** Since 1927.

Gallagher

The information contained herein is offered as insurance Industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete Insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis. Gallagher publications may contain links to non-Gallagher websites that are created and controlled by other organizations. We claim no responsibility for the content of any linked website, or any link contained therein. The inclusion of any link does not imply endorsement by Gallagher, as we have no responsibility for information referenced in material owned and controlled by other parties. Gallagher strongly encourages you to review any separate terms of use and privacy policies governing use of these third party websites and resources. Insurance brokerage and related services to be provided by Arthur J. Gallagher Risk Management Services, Inc. (License No. 0D69293) and/or its affiliate Arthur J. Gallagher & Co. Insurance Brokers of California, Inc. (License No. 0726293).