Cyber incidents are increasing at a rapid rate across all industries and geographies; in the first half of 2018, 72 percent more data was compromised compared to the same period the previous year[1]. Most of the data compromises can be attributed to human error, such as an employee accidentally emailing protected data to the wrong party, or the unauthorized access to an organization's network by an employee or a third party.

While cyber risk has not historically been top-of-mind for senior living providers, the growing sophistication of attacks and prevalence of cybercrime requires the development of rigorous data and network security protocols throughout the field. Even as organizations with the strongest cybersecurity practices remain vulnerable to cyber incidents, to best protect senior living organizations and their residents' data, it is also imperative to proactively develop a breach response plan.

Senior living providers face a uniquely challenging risk landscape as they experience risks inherent to both the health care and real estate industries. Approximately *one-third* of all cyber claims Willis Towers Watson reported to insurers between September 2017 and September 2018 were made on behalf of clients within the health care and real estate sectors[2]. Additionally, organizations of all sizes are experiencing an increase in cyber incidents. According to a recent Verizon Data Breach Report,[3] approximately 61 percent of data breach victims are organizations with fewer than 1000 employees. Cyber extortion, denial of service attacks, network disruption, and violations of privacy have all been on the rise.

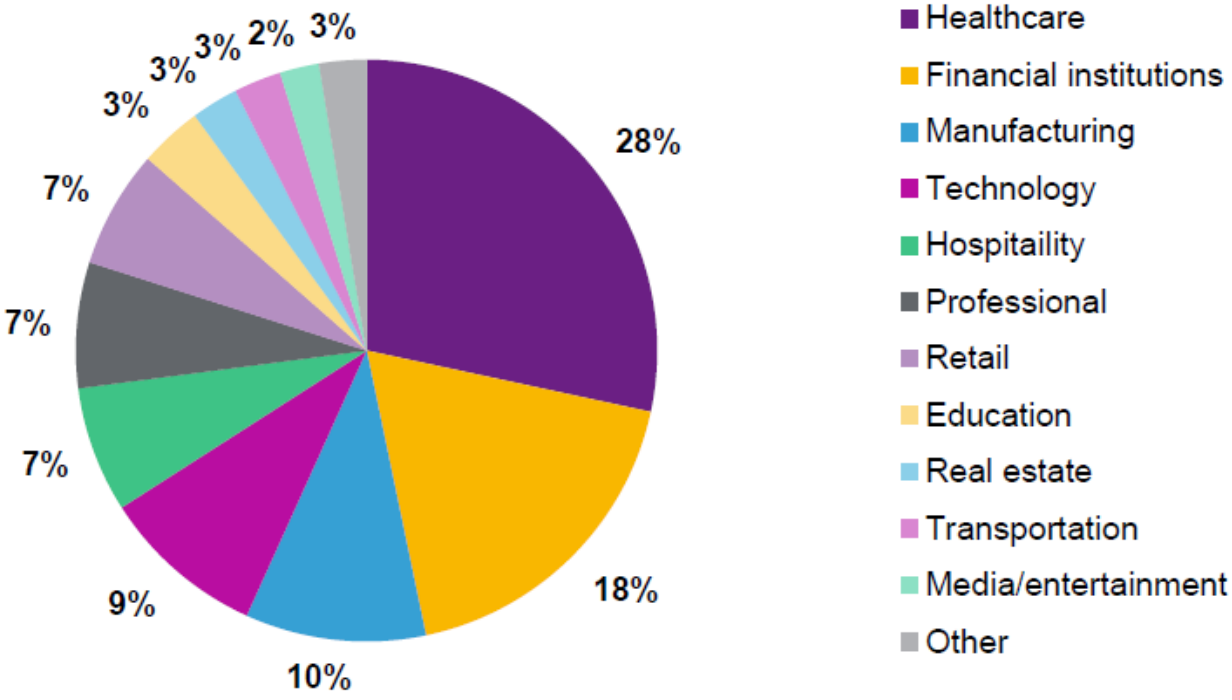
[1] Data Breach Discoveries from the Breach Level Index: Data Privacy and New Regulations Take Center Stage: 2018 First Half Review; powered by gemalto
[2] Willis Towers Watson 2017-2018 Reported Cyber Claims Index
[3] Verizon 2017 Data Breach Investigations Report 10th Edition

CYBER and Senior Living

Not a Matter of *If* or ***When***, but ***How Much***

By Rodger Lederer, Lindsay Combs, and Teresa Leahey, Willis Towers Watson

Cyber Claims by Industry



*Willis Towers Watson 2017-18 Reported Cyber Claims Index

INCIDENTS

Providers...

WHAT IS UNIQUE ABOUT THE CYBER RISKS OF SENIOR LIVING PROVIDERS?

The frequency and severity of cyber claims reported by senior living providers is largely due to increased regulation, the value of records held and the ease of access to those records.

Regulatory Landscape

Organizations holding data that are highly regulated are more likely to incur significant fines and penalties following a data breach, making even accidental disclosures costly. In 2018, the health care sector experienced the highest per capita data breach cost of any industry, nearly *twice* that of the next highest sector[4]. While not all organizations within the senior living sector are subject to HIPAA, some are; information held by senior living providers may also be federally regulated by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Additionally we may see more localized efforts to enact privacy legislation, such as California's Consumer Privacy Act (CCPA).

These regulations are intended to protect the privacy of the staff, residents and applicants of senior living communities. It is likely that a provider has the date of birth, Social Security number, and bank account information of staff and residents alike, as well as the insurance account information for all residents. This type of information is categorized as Personally Identifiable Information (PII) or Protected Health Information (PHI). While we will further explore the value of these records below, it is important to note that it is the responsibility of organizations throughout the senior living sector to maintain the integrity and privacy of this data.

Many organizations hold the belief that because they outsource the storage or processing of data, they have transferred their risk and potential liability to that outsourced provider. Yet this is a misconception; the organization that owns the data is ultimately liable for maintaining it. Furthermore, it is likely that in the event of a breach to a senior living community, everyone from the owner to the operator may be held, or at least initially viewed as, liable. It is therefore imperative, especially in such a highly regulated sector, for each party to proactively review their cyber risk management protocols and breach response strategy.

Value of Records Held

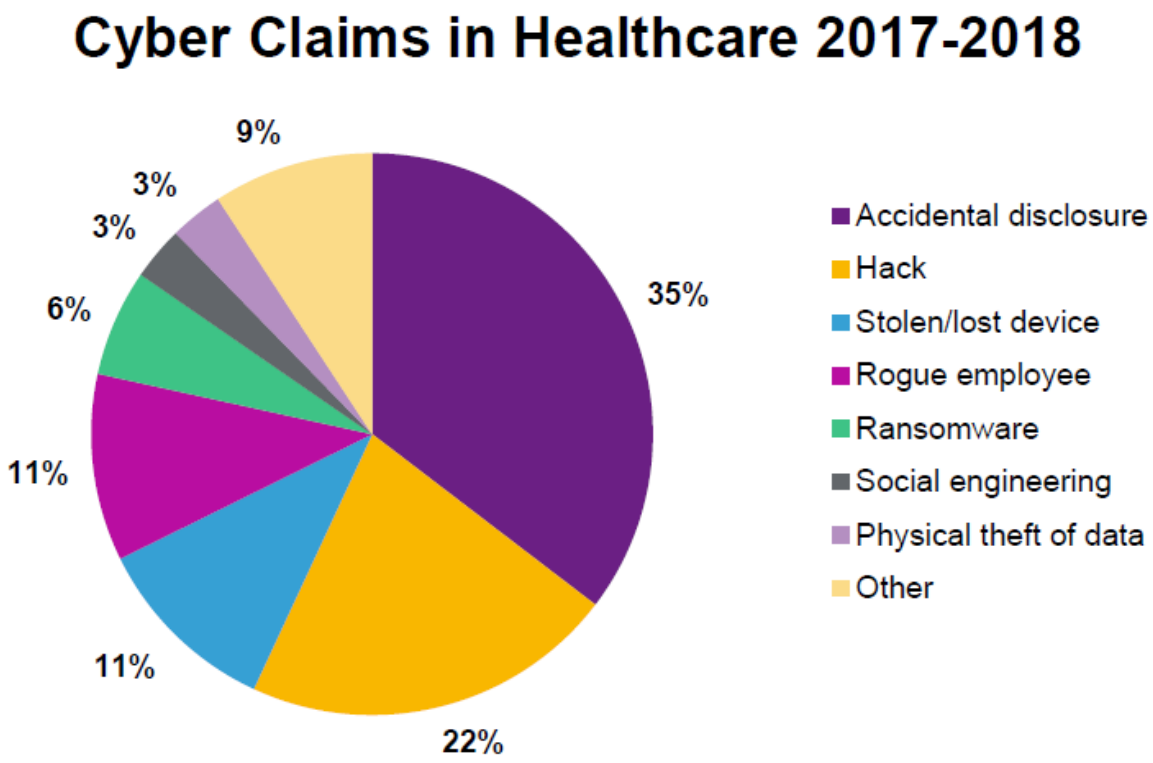
While senior living communities do hold credit card information for residents, the PII and PHI records held are significantly more valuable to bad actors. When credit card information is compromised, an affected individual may quickly and easily cancel the card and dispute fraudulent charges, rendering the stolen information worthless. It is much more challenging for impacted parties to resolve a situation where their Social Security number is stolen or their health care information is fraudulently accessed. Criminals can make millions of dollars defrauding Medicare by utilizing stolen information to bill for services not actually provided.

Theft of PII and PHI may result in substantial profit for criminals, but only for those who know what to do with the information once it has been stolen. An easier criminal enterprise is to simply hold the data or the network of an organization with such sensitive data hostage, also known as ransomware or cyber extortion. These bad actors operate on the assumption that organizations will pay handsomely to regain access to their data and/or systems, as well as avoid the public relations fallout of having a more severe breach.

Ease of Access

In addition to being known for holding valuable data, senior living providers are also seen by bad actors as not dedicating significant resources to cybersecurity, creating an attractive target for cyberattacks. According to a leading cyber insurer, the health care industry has accounted for 33 percent of all ransomware attacks since 2016, the most of any industry[5]. And yet the primary cause of a cyber breach for senior living providers is an organization's employees; according to the Willis Towers Watson 2017-18 Reported Cyber Claims Index, 69 percent of claims in the health care industry can be attributed to the human element (comprised of accidental disclosure, stolen/lost device, rogue employee, ransomware, social engineering, and physical theft of data).[6] Something as simple as a lost laptop or even a paper file can result in substantial financial and public relations cost.

[4] Ponemon Institute LLC 2018 Cost of a Data breach Study: Global Overview
[5] Chubb Healthcare by the Numbers: Cybersecurity
[6] Willis Towers Watson 2017-2018 Reported Cyber Claims Index



*Willis Towers Watson 2017-18 Reported Cyber Claims Index

WHAT ARE THE BIGGEST CYBER RISKS FOR SENIOR LIVING PROVIDERS?

Perhaps the biggest cyber risk to senior living providers is not having a plan in place to manage and respond to cyber risks.

The most likely cyber incident to be experienced by a senior living provider is a privacy breach, and the costs associated with this type of breach can be significant. In the first half of 2018, the total average cost of a data breach in the U.S. was $7.91 million, nearly twice the global average due in large part to the country's regulatory requirements.[7] In addition to regulatory fines and penalties, a senior living provider might also incur costs to notify and offer identity protection to impacted parties, employ a public relations firm, and defend against claims. In instances where an attack occurs, rather than an accidental disclosure, an organization could incur even more expenses, such as those to make a ransom payment and employ a computer forensics team to identify and resolve the source of the breach.

The faster an organization can identify, contain, and resolve a breach, the lower the overall cost of the incident. Organizations that contain a breach in under 100 days spend, on average, $1 million less than organizations that take longer to do so; organizations that contain a breach in under 30 days save, on average, another $1 million.[8] For an organization to adequately respond to a cyber incident, it must have already developed an incident response plan. This plan should include, at a minimum, the responsibilities of leaders within an organization and the identification of partner vendors to assist in the resolution of the incident. Many cyberinsurance policies provide access to vendors, such as computer forensic firms and breach response coaches, who can be employed within the limits of the policy at no additional cost.

It is also important to note that of all risks experienced by senior living providers, property damage and corresponding business interruption losses are some of the most costly. It is becoming increasingly standard in the cyberinsurance market to include coverage for business interruption, and even contingent business interruption, due to malicious cyber events, such as ransomware attacks. Many insurers are also offering coverage for interruption due to system failures, such as those caused by a faulty system update.

> "The most likely cyber incident to be experienced by a senior living provider is a privacy breach..."

[7] Ponemon Institute LLC 2018 Cost of a Data breach Study: Global Overview
[8] Ponemon Institute LLC 2018 Cost of a Data breach Study: Global Overview

WHAT STEPS CAN SENIOR LIVING PROVIDERS TAKE TO BETTER PROTECT RESIDENTS AND THEIR INFORMATION?

Proactive actions senior living providers can take to best protect residents and their information include:

- Performing a network security audit, including a review of:
  - How all systems interact and are protected, including their Internet of Things (IOT) environment
  - Data encryption practice
  - Backup procedures to ensure recoverability of data
  - Compliance requirements and current privacy practices, including the limitation of access to PHI and PII to only necessary parties
  - Potential vulnerabilities of third party vendors that could create liability for the provider
- The development and offering of ongoing cybersecurity training for all employees and residents, including topics such as:
  - Proper password protocol
  - Safe social media use
  - How to recognize and report a phishing or social engineering attempt
  - Responsible software installation
- The creation and maintenance of an incident response plan, including:
  - C Suite
    - ✓ Outlining of roles and responsibilities in the event of an incident
    - ✓ Annual test of breach response plan
    - ✓ Determination of how costs associated with an incident would be managed
  - Breach response vendor management
    - ✓ Identification of vendors to be employed in the event of an incident
    - ✓ Determination of how they would be compensated: Is a retainer required? Are they covered by the cyber insurance policy and if not, are they able to be endorsed for coverage?
    - ✓ Confirmed understanding of how rapidly these vendors could respond

Rodger Lederer is Vice President of Willis of Illinois, Inc. Senior Living & Long-Term-Care Centers of Excellence; and Lindsay Combs and Teresa Leahey are Cyber Specialists, FINEX Cyber/ E&O North America. The Willis Towers Watson Senior Living Center of Excellence currently represents more than 450,000 senior living communities nationally, working with owners, operators, equity partners, managers and developers of all senior living venues. For more information, visit www.willistowerswatson.com or email rodger.lederer@willistowerswatson.com.