White Paper

Senior Living Data Security

How to safeguard sensitive data from online attacks and third-party hacks

Yardi is committed to updating and monitoring database security continuously, so you can protect sensitive information and feel safe putting your data in our hands.

A Global Cause for Concern

In 2016, hacking hit the mainstream. Millions of Google accounts were compromised, and Yahoo made headlines with two major intrusions. In 2017, the Equifax breach exposed the personal information of 147 million people. A years-long Marriott breach in 2018 exposed 383 million guests.

By October of 2019, the number of data breaches reported that year had already surpassed the annual figure for 2018. We also saw the rise of a significant new threat: data exposure from unsecured databases and credential stuffing. In early 2020, Marriott announced an incident affecting 5.2 million guests. As a result, awareness of network vulnerability remains high, and smart companies are moving quickly to fortify their defenses.

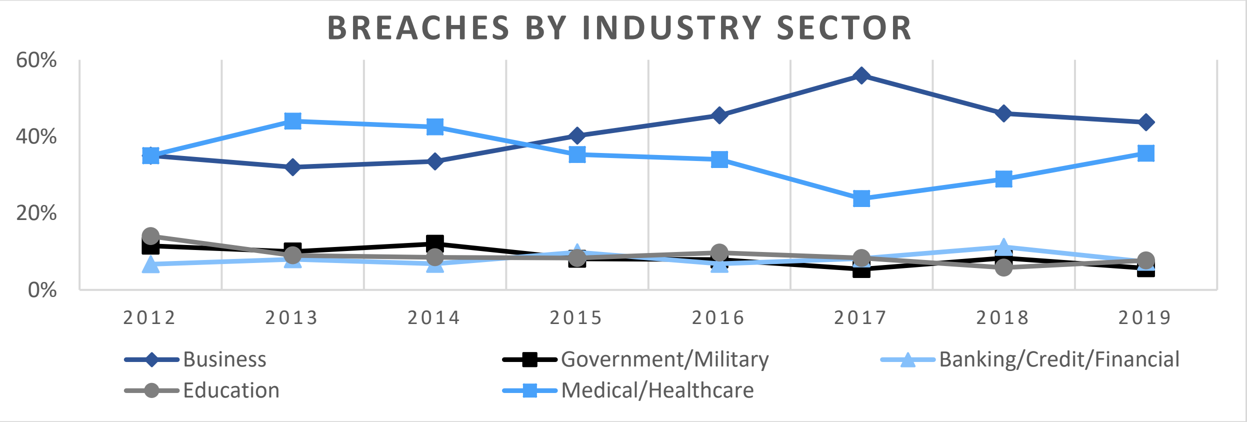
Why Do Hackers Want Healthcare Data?

According to the Identity Theft Resource Center (ITRC), hacking attacks were the leading cause of data breach incidents for the tenth consecutive year in 2018. Personally identifiable information (PII) presents an alluring target for hackers. Whereas stolen credit card information diminishes in value due to market saturation, the information stored by medical facilities, including patient data and healthcare records, has become increasingly valuable.

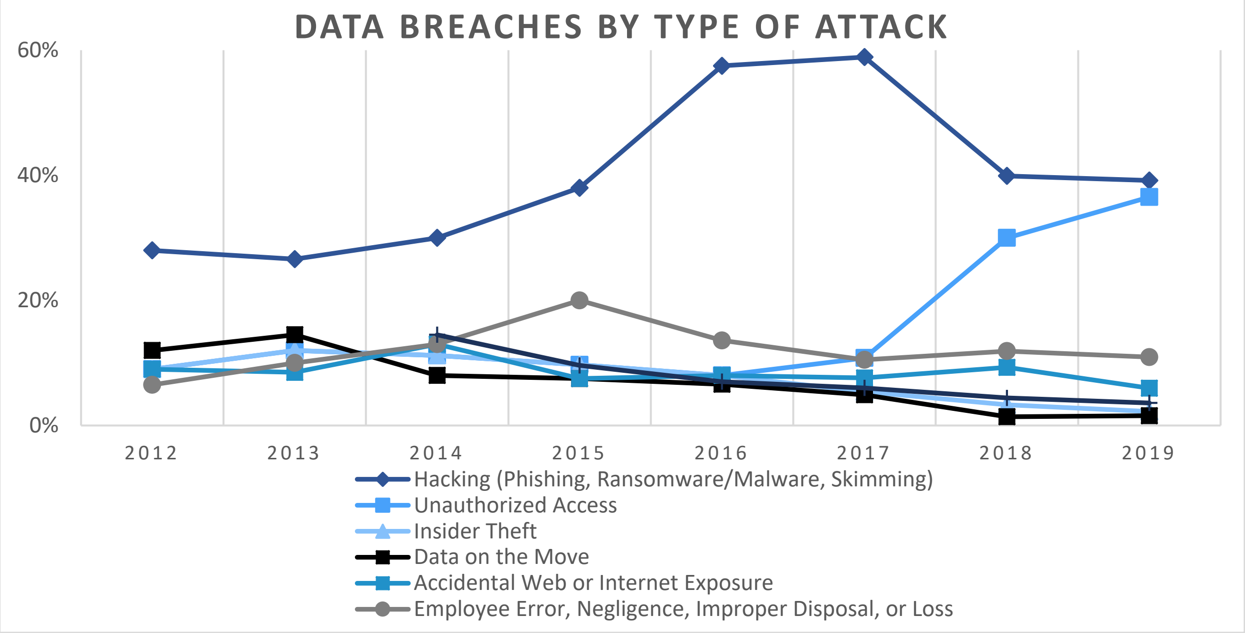
Social Security numbers and birth dates can be used to fake entire individual profiles, making medical information a valued and vulnerable target. Hackers also use health data to forge prescriptions for opioids and other narcotics.

Data Breach Evolution & Forecast: More Consumers than ever Affected

According to the ITRC, the total number of reported breaches increased by 17% between 2018 and 2019. At the same time, the reported number of sensitive consumer records exposed dropped by 65%, from 471 million in 2018 to 164 million in 2019.



The business sector experienced the highest number of breaches for both years, followed by the medical and healthcare sectors. Hacking remains the most common method, totaling 577 data breaches (39%) and exposing 15 million sensitive records in 2019. Unauthorized access exposed the most data at 142 million records. Breaches in the banking, credit, and financial sector exposed 61% of sensitive records in 2019. In the face of this ever-increasing risk, the ITRC emphasizes the need for stringent data security from consumers and businesses.



Ransomware: Funding for Hacking R&D

In its 2019 Data Breach Investigations Report, Verizon once again ranked ransomware as a key threat, particularly in the healthcare sector, where it accounts for over 70% of all malware attacks. Recent large-scale data breaches have made it more important than ever for companies to be proactive. The Experian Data Breach Resolution team asserts that all public and private organizations must ensure they use the most robust technology available to thwart attacks, going beyond traditional cybersecurity and adding fail-safes to ensure continued operation.

Ransomware invades a network through spam email, a camouflaged link, or a Trojan Horse attachment, encrypting data and locking out users. Paying the ransom releases the data and the device. Payment demands range from a few thousand to millions of dollars. While ransomware primarily struck individuals in the past, the latest victims are institutions like hospitals and government agencies.

For perpetrators, ransomware is a pure moneymaking enterprise, but for public entities, attacks could have catastrophic ramifications. With life-threatening risks involved, victims usually pay up quickly, and attackers become emboldened each time. Experian notes that “[paying the ransom] has unintended consequences of funding more research… by attackers, who in turn develop more sophisticated and targeted attacks.”

In recent years, several high-profile ransomware attacks on health facilities made the news, including incidents at East Ohio Regional Hospital, Hollywood Presbyterian Medical Center, and Kentucky’s Methodist Hospital. In mid-2019, ransomware attacks hit multiple New York-based medical groups, blocking access to EHR systems and forcing care providers to make do with pen-and-paper charts. While facilities scrambled to restore services, patients were asked to provide their own medication records and medical histories.

Vulnerabilities in Senior Living

Network penetration can put senior living providers' sensitive data at risk. Below we discuss common issues and how to address them to keep your data safe.

Things to look for when choosing a cloud provider:

1. A completed Standard Information Gathering (SIG) questionnaire. This industry-standard questionnaire covers all areas of cyber security.
2. Relevant audit docs, including SSAE18, ISO, PCI, HIPAA.
3. Latest security tests results, including network penetration tests and application penetration tests.
4. Business continuity plans, including verification of maximum data and time loss before site is back online.
5. Guaranteed uptime for the application. Usually expressed in "nines". Three "nines" equals a 99.9% uptime guarantee, or about 45 minutes of unscheduled downtime per month.
6. Scheduled maintenance hours. Is there a cap on maintenance that affects system availability?
7. Data center redundancy. Is your data being saved in multiple locations to provide a backup in the event the main database is compromised?

Problem: Poor Network Protection & Preparation

Whether through a phishing scheme or a compromised password, once a network's security has been penetrated, all the data stored in it is at risk. Historically, many organizations felt safe using perimeter protection like firewalls and tightening access at network entry points. Unfortunately, hackers constantly develop new techniques and can now pass unnoticed through even the strongest perimeter protection. Malware can infect a network and stay dormant for months. The malicious code works slowly and invisibly, seeking out weak points and probing for vulnerabilities as it travels through the network in search of databases and file servers. Once it finds something valuable, it can transfer data outside the network or encrypt files as part of a ransomware attack.

"Hackers are constantly deploying attacks, and you never know where it's going to hit," says Jay Shobe, vice president of technology at Yardi. "It's akin to trying to open every car in a parking lot. You're not actually targeting anything in particular; you're just looking for vulnerabilities."

Solution: A Trusted Cloud Provider

In the Yardi Cloud, client data resides behind multiple layers of firewalls and intrusion prevention systems. Strong password policies and SSO integration authenticate users in real time, and role-based security ensures that users can only access appropriate data. Multiple encryption layers protect data at rest and in motion.

Yardi constantly backs up and replicates data to an off-site business continuity center. We exclusively host in Tier 3 co-location spaces from leading providers, with end-to-end redundancy for power, connectivity, and more.

Problem: Low Security Awareness among End Users

Another issue with the perimeter-only approach is that access through a single point of entry makes the employee the first line of defense. As a result, one poorly trained staff member can compromise an entire organization's database with just one click on a phishing email or an inadequate password. Lack of staff training and failure to prioritize security awareness means employees are often the weakest link when it comes to network security.

Solution: Security Awareness Training & Tests

Identifying a threat and creating a set of security strategies is not enough. Employees need to be trained on phishing schemes and the importance of strong password protection. For example, security awareness training programs can deploy anti-phishing campaigns that send suspicious emails with links. If clicked, those links trigger a pop-up screen alerting the employee to their error and directing them to online security awareness training.

While moving from paper to electronic health records opens up the risk of a data breach, the demand for improved data accuracy, productivity, and convenience will not diminish in the near future. It is important to create flexible applications backed by powerful security protocols that can evolve as new threats emerge. Companies need to make data secure while ensuring that staff can access the information they need.

Problem: Vulnerable Mobile Devices

Due to the changing nature of the healthcare industry, mobile apps and laptops have greatly increased the number of hackable entry points. Not only can physical devices be stolen and used to access the network; insecure devices mean data can be accessed over insecure Wi-Fi networks.

“Mobility is not going away,” says Shobe, “even though the ability for people to access systems from their devices adds an entirely new level of security concerns. Being able to monitor endpoints like desktops, laptops and mobile devices is becoming increasingly important.”

Solution: Mobile Device Management

Mobile device management (MDM) enables system administrators to control which devices can access company assets. They can enforce the company's security protocols regarding app downloads as well as Wi-Fi and PIN policies. With MDM, company devices can be remotely wiped of all content in the event of a breach or after an employee is terminated. Even personal devices can be blacklisted or whitelisted using MDM. For employee-owned devices, MDM can be limited to company data only, leaving any personal records untouched.

Problem: Inadequate Front-End Security

Using software products from multiple vendors can heighten risk exposure, especially when sensitive data is shared across platforms with disparate security levels. A weak password or inadequate authorization policy could allow users or malicious parties to access unauthorized information. Switching between systems creates additional layers of vulnerability, making comprehensive network security difficult to maintain.

Solution: Front-End Security Administration

The Yardi Senior Living Suite includes detailed security permissions with multiple levels of access (e.g., read-only, read/write) for users or groups of users. System administrators use a convenient tool to assign resources and privileges, so users can access only relevant, authorized information and tasks.

Security Layers in the Yardi Cloud

- Data sent over the internet is always encrypted.
- Defense-in-depth security offers multiple layers of protection, from the exterior network to the servers.
- Anti-virus and anti-malware applications safeguard all servers in real time.
- Microsoft Active Directory ensures that users can only access their own organization's applications.
- Multiple layers of database encryption secure data at rest. All login attempts are authenticated.
- System administrators can assign role-based access to data and functions. They can define idle periods for session timeouts as well as requirements for password length, complexity, and change frequency.

Conclusion

Data security presents a moving target, so complacency is one of its biggest threats. Whenever an attack is thwarted or a breach is mended, the invaders evolve. It is not enough to put security protocols in place; you have to be proactive and stay informed on data breach trends. Additionally, you need to implement continuing security awareness education for staff. As Experian explains, "Organizations can't wait until an attack happens to ensure they are protected. They need to look at the signs early on to start preparing for new types of security threats."

Working with a successful cloud service provider is a great way to gain peace of mind without a large investment in time and staff. With 20 years of experience, Yardi's award-winning Cloud Services division supports over 10,000 clients in 12 global data centers. Regular, rigorous audits ensure the most secure environment possible. Staying on top of the latest developments in data security is one of our many vital services for our cloud customers. Yardi can help you prepare for security challenges by helping you navigate the solutions available for companies that use and store sensitive data.

Leading Business-Wide Real Estate Management Software & Services

Yardi offers superior products and outstanding customer service. We take care of our employees and the communities where we work and live. With that commitment, Yardi leads the industry in business platforms for real estate accounting and investment, property management, and asset management. Organizations like yours have been using our proven software with confidence for decades.

The Yardi Senior Living Suite meets or exceeds industry best practices with multiple levels of security and employs the latest security protocols and techniques. You can operate all aspects of your senior living business knowing that data from patient records to accounting information is protected effectively. Guaranteed data recovery and around-the-clock monitoring safeguards server operations even in the event of an unexpected natural disaster.