Senior Living Data Security

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

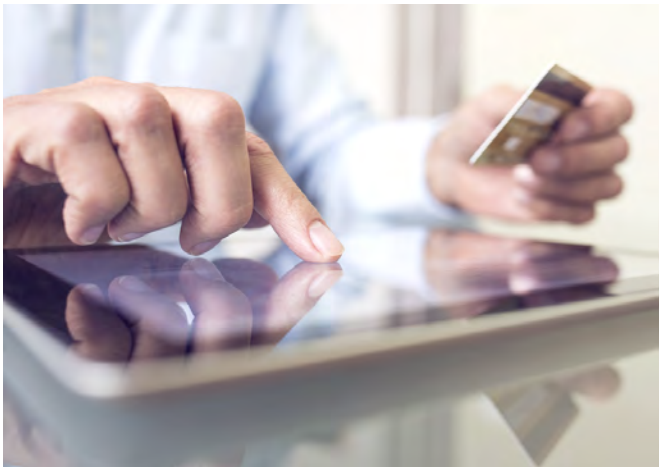
YARDI

Yardi is committed to providing you with continually updated and monitored database security, allowing you to protect sensitive information and feel safe putting your data in our hands.

Table of contents

Introduction

Global cause for concern



It's no secret personal and business data security continues to be a global concern

In 2016, hacking hit mainstream. Millions of Google accounts were compromised during an ongoing malware attack, and Yahoo made headlines while disclosing not just one, but two major intrusions. That year, broad DDoS attacks took out most of the U.S. Eastern Seaboard, the San Francisco transit shut down completely over Thanksgiving and there was controversy over the 2016 presidential election.

Since, dozens of significant cyber incidents, including the Equifax breach in July 2017, the Uber breach disclosed in November 2017, as well as numerous cyber attacks on government agencies worldwide have been reported. As a result, awareness of network vulnerability remains high, and smart companies are moving quickly to fortify defenses.

Why do hackers want healthcare data?

Personally Identifiable Information (PII), including patient data and healthcare records, present an alluring target to hackers. As stolen credit card information diminishes in value due to market saturation, the type of information stored by medical facilities has become increasingly valuable.

Social Security numbers and dates of birth can be used to create an entire profile of an individual, making medical information a highly valued, and relatively vulnerable, target. Hackers also use health data to forge prescriptions for opioids and other narcotics. According to the Identity Theft Resource Center (ITRC), hacking/skimming/phishing attacks were the leading cause of data breach incidents for the ninth consecutive year in 2017.[1]

Ransomware – funding for hacking R&D

In the Data Breach Industry Forecast for 2017, Experian predicted an increase in ransomware attacks, particularly on healthcare organizations with distributed networks.[2] As the report explains, "It only takes one compromised or outdated system to lead to exposure." With 2017's large-scale data breaches, it's now more important than ever for companies to be proactive. And in 2018, ransomware attacks are indeed on the rise. Experian asserts that all organizations, both public and private, must ensure they are using the most robust technology available to thwart attacks, including going beyond traditional cybersecurity and adding fail-safes to ensure continued operation.[3]

Ransomware typically 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 small sums to thousands of dollars. While in the past ransomware primarily struck individuals, the latest victims involve data-rich institutions like hospitals and government agencies.

For perpetrators, ransomware is purely a moneymaking enterprise. For healthcare providers, ransomware attacks can have catastrophic ramifications. With life-threatening risks involved, ransomware attackers expect their victims to pay up quickly. Unfortunately, every time a ransomware victim capitulates, attackers become emboldened.

In 2016, several high-profile ransomware attacks on health facilities made the news, including incidents at Ottawa Hospital, Hollywood Presbyterian Medical Center and Kentucky's Methodist Hospital. In 2017 a strain of ransomware spread worldwide, affecting hundreds of thousands of targets including temporarily crippling National Health Service facilities in the United Kingdom, hobbling their emergency rooms and delaying vital medical procedures.[4]

"[Paying the ransom] has unintended consequences of funding more research and development by attackers who in turn develop more sophisticated and targeted attacks."

- Experian

[1] Identity Theft Resource Center® and CyberScout®, *2017 Annual Data Breach Year-End Review*. (**https://www.idtheftcenter.org/2017-data-breaches**)

[2] Experian® Data Breach Resolution, Experian, *2017 Fourth Annual Data Breach Industry Forecast, 2017* (**http://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf**)

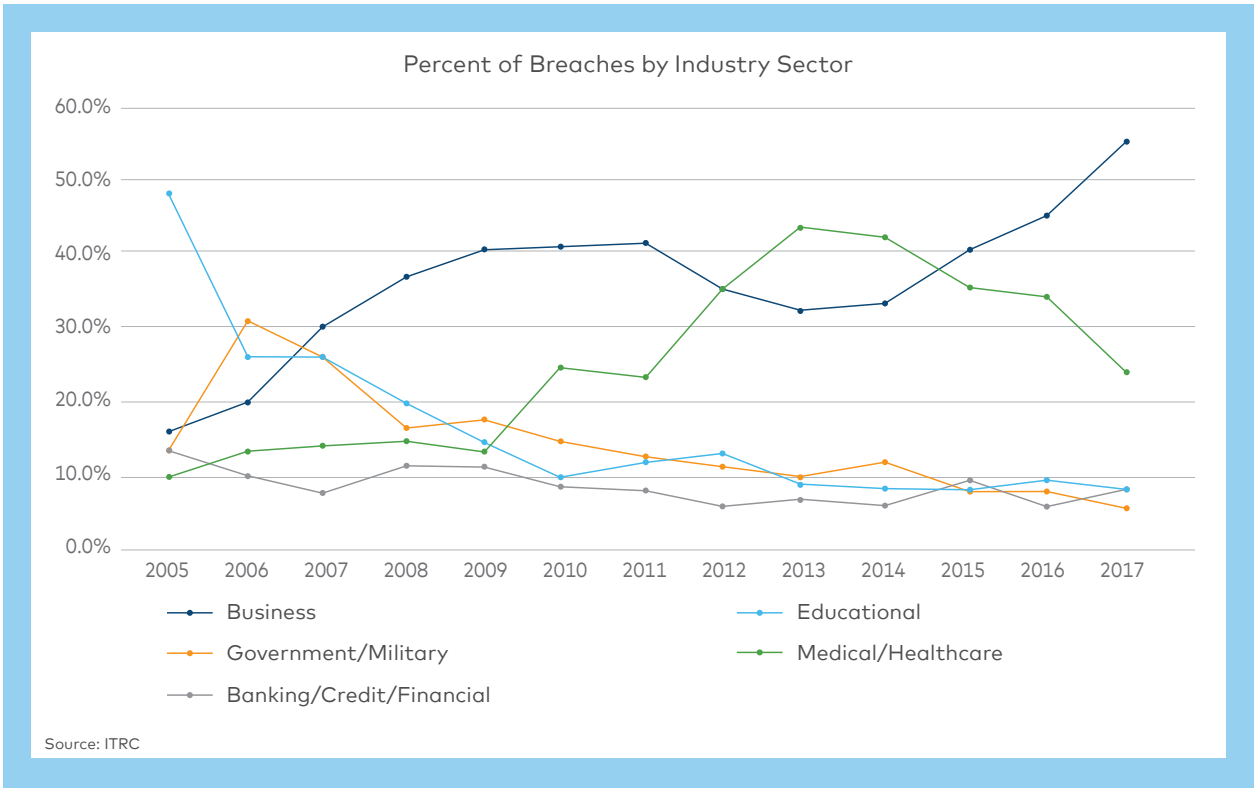
[3] Experian® Data Breach Industry Forecast 2018 (**2018-experian-data-breach-industry-forecast.pdf**)

[4] Newman, L.H. (2017, July 1). The biggest cybersecurity disasters of 2017 so far. Wired. Retrieved from **https://www.wired.com**.

Data Breach Evolution and Forecast

Breaches at all-time high

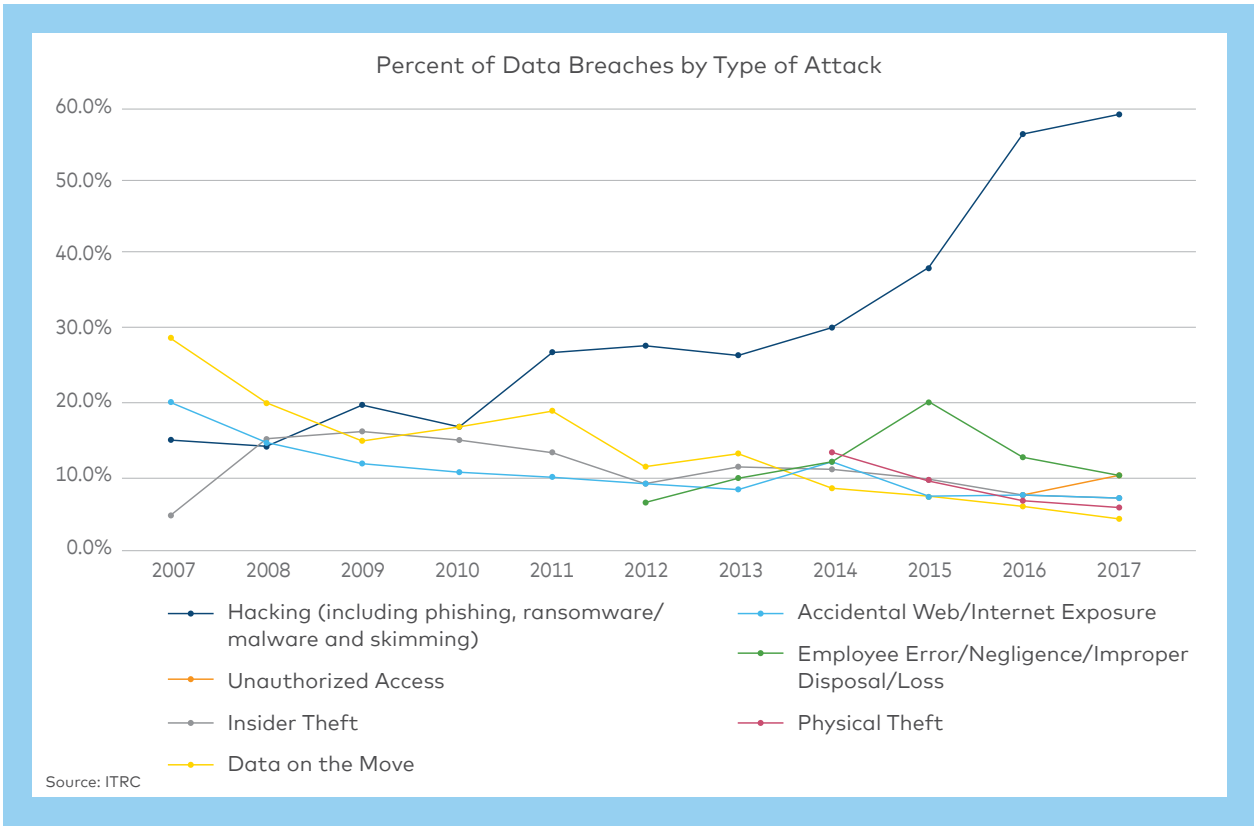
According to the Identity Theft Resource Center (ITRC), the number of U.S. data breaches in 2017 hit a new record high of 1,579, with over 178 million records exposed. That averages about four data breaches a day for 2017, a drastic overall increase of 44.7% over 2016's reported figures.



Of the five industry sectors the ITRC tracks, the medical/healthcare industry had the second highest percentage with 23.7 percent (374 breaches) of the overall total number of breaches.[1]

Modern Healthcare, a leader in healthcare business news, research and data, reported in 2017 that by 2024, everyone in the U.S. will have their healthcare data compromised if online theft keeps accelerating at the current pace.[5]

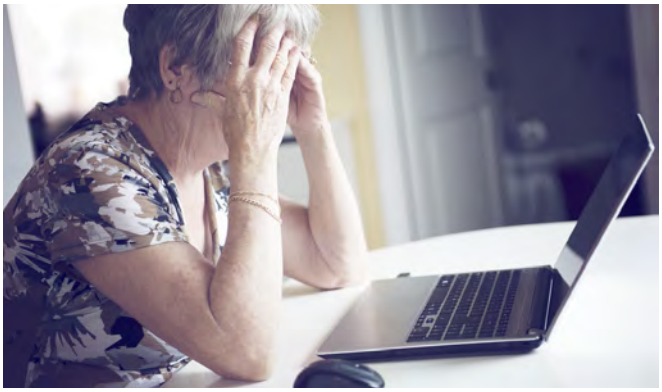
[5] Sweeney, B. (2017, April 10). The frightening new frontier for hackers: medical records. Modern Healthcare. Retrieved from **http: www.modernhealthcare.com**.

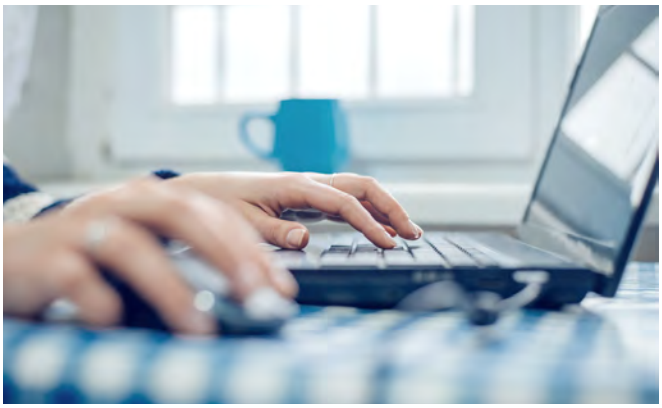


Hacking continued to rank highest in the type of attack, at 59.4 percent of the breaches, an increase of 3.2 percent over 2016 figures. Of the 940 breaches attributed to hacking, 21.4 percent involved phishing and 12.4 percent involved ransomware/malware. Unauthorized access, which was newly added as a method of attack in 2016, represented nearly 11 percent of the overall total of breaches for a 3.4 percent increase over 2016 figures.

Vulnerabilities in Senior Living

Network penetration leaves data at risk





The network

Problem: Poor network protection and preparation

Whether it is a phishing scheme or a compromised password, once a network's security has been penetrated, all the data stored within it is at risk. Historically, organizations may have felt safe using perimeter protection like firewalls and tightening access at network entry points. Unfortunately, hackers are constantly developing new techniques, and companies can struggle to keep up. Hackers can now pass unnoticed even though the strongest perimeter protection. Once malware infects the network, it can stay dormant for months. The malicious code works slowly and invisibly, seeking out weak points and probing for vulnerabilities as it travels laterally through the network in search of databases and file servers. Once it finds something valuable, it can exfiltrate 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."

real time, and role-based application security verifies users can only access data they are authorized to see. In addition, multiple encryption layers of both data at rest and data in motion guarantee that if a breach occurs, the data remains protected.

> *"Hackers are constantly deploying attacks, and you never know where it's going to hit. It's akin to trying to open every car in a parking lot."*
>
> - Jay Shobe, VP of Technology at Yardi

Solution: A trusted cloud provider

Within the Yardi cloud, client data resides behind multiple layers of firewalls and intrusion prevention systems. Strong password policies and SSO integration ensure that users are authenticated in

Yardi constantly backs up and replicates all data to an off-site center to ensure business continuity. Yardi partners with world-class data centers providers, and exclusively hosts in Tier 3 co-location spaces to establish full redundancy of all components, including power, internet connectivity and more.

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 back up in the event the main database is compromised?

The end user

Problem: Weak security awareness

Another issue with a perimeter-only approach to data security is that access through a single entry point 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 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 and security tests

It's not enough to simply identify the threat and create a set of security strategies. 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 of their error, and directing them to online security awareness training.

Are paper records a safety measure?

As Shobe explains, moving to electronic health records opens up the risk of a data breach. Nevertheless, the reality is that the demand for improved data accuracy, productivity and convenience will not diminish in the near future. It is important to create flexible and adaptable applications backed by powerful security protocols able to evolve as new threats emerge. Companies need to make data secure while also making sure the right people can access the right information.

Portability

Problem: No mobile device management

Due to the changing nature of the healthcare industry, mobile applications and even laptops have exponentially increased the amount 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. Having the ability to really 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. MDM also allows for enforcement of 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.

The software

Problem: Inadequate front-end security

Using multiple software from multiple vendors can heighten risk exposure, especially when sensitive data is shared across different platforms with disparate security levels. A weak password or inadequate authorization policies could allow users, or malicious parties, to access information they are not authorized to see. Switching between multiple systems creates additional layers of vulnerability, making comprehensive network security difficult to maintain.

Solution: Front-end security administration

The Yardi Voyager platform features a comprehensive security system that allows system administrators to apply granular settings to users and groups. System administrators use a convenient front-end administrative tool to assign resources and privileges, so users can access only relevant, authorized information and tasks. Data security easily creates multiple levels of access (e.g., read-only, read/write) for users or groups of users.

Voyager security layers

1. Data sent over the internet is always encrypted.
2. Defense-in-depth security with multiple layers of protection from the network exterior to the application and database servers.
3. Real-time anti-virus and anti-malware software safeguards all Yardi servers.
4. Active Directory Security ensures users only have access to their organization's specific applications.
5. Multiple layers of database encryption ensure security of data at rest. The system authenticates any attempt to log in to the database server.
6. User-defined access allows system administrators to authorize users from within the program to access program features and reports and can define "idle" periods for session timeouts.
7. Strong password policies including password length, complexity rules, and change policy can be defined by system administrators.

Conclusion: The best defense is a good offense

Data security presents a moving target

Data security presents a moving target: every time an attack is thwarted or a breach is mended, the invaders evolve. As a result, one of the biggest threats to data security is complacency. It is not enough to put security protocols in place. Organizations need to be proactive. Staying informed of recent trends in data breaches is essential. As Experian explains in their report, "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."

Staying on top of the latest developments in database security is one of the many vital services Yardi provides to its cloud customers. With more than a decade of cloud computer experience, Yardi's award-winning Cloud Services division manages over 5,000 clients in 12 datacenters around the world. Our dedicated cloud support team focuses on delivering clients the most secure environment possible, and are subject to regular rigorous security audits. By providing a deeper understanding of the solutions available for companies tasked with recording, utilizing and storing sensitive data, Yardi can help you prepare for any security challenges.

Conclusions:

1. *You need to implement a program of continuing education to keep staff educated on evolving security threats.*

2. *You need a world-class cloud provider ensuring your data is secure.*

The Yardi Senior Living Suite is delivered with multiple levels of security designed to meet or exceed industry best practices and employ the latest security protocols and techniques.

Clients can operate all aspects of their senior living business feeling confident that all their data – from patient records to accounting information and other sensitive material – is protected by the most effective security measures available. Peace of mind is enhanced by guaranteed data recovery and around-the-clock monitoring of server operation, even in the event of an unexpected natural disaster, such as a hurricane, earthquake or wildfire.

Leading Business-Wide Real Estate Management Software and Services

At Yardi our mission is to provide our clients with superior products and outstanding customer service, while we take care of our employees and the communities where we work and live. With that commitment, Yardi leads the industry in providing full business software solutions for real estate investment management, property management, financial accounting, asset management, and ancillary services.

Organizations like yours have been using our proven and mature software with confidence for decades.

YARDI | Energized for Tomorrow

Yardi Systems, Inc. 430 South Fairview Avenue, Santa Barbara, California 93117
phone: +1 800 866 1144 | email: sales@yardi.com | Yardi.com

SLDataSecurity_090718_6210 10/1/2018