Data Security for Affordable Housing & PHA Clients

Cloud technology supports nearly every modern industry. It is the safest way to store data, the most convenient way to do business, and the most cost-effective way to mitigate risk. Hosting your data and software internally is risky. Learn why now is the perfect time to transition your business to the cloud.

What Is the Cloud?

The term "cloud" visualizes the convenience of having data and software available wherever you are. It represents secure servers in a remote physical location, with users connecting securely via the internet.

Cloud computing is common, and you may not even know you are working in the cloud. When you check your email via your web browser or your stock portfolio from your smartphone, you are using cloud computing. Whenever you receive news or data over the internet, you are accessing information from the cloud.

What the Cloud Is Not

Local servers and connectivity are the alternative to cloud-based data. Examples are hardwired or wireless local area networks that keep data available in-house only. Data can be synced with mobile devices periodically but is not readily available in real time.

What Does the Cloud Have to Do with Security?

Cloud-based software and data environments are often more secure than private hosting. Cloud providers are dedicated to keeping up with security threats and evolving technology trends. A top cloud computing company's expertise and resources likely surpass what could be expected of any in-house IT staff.

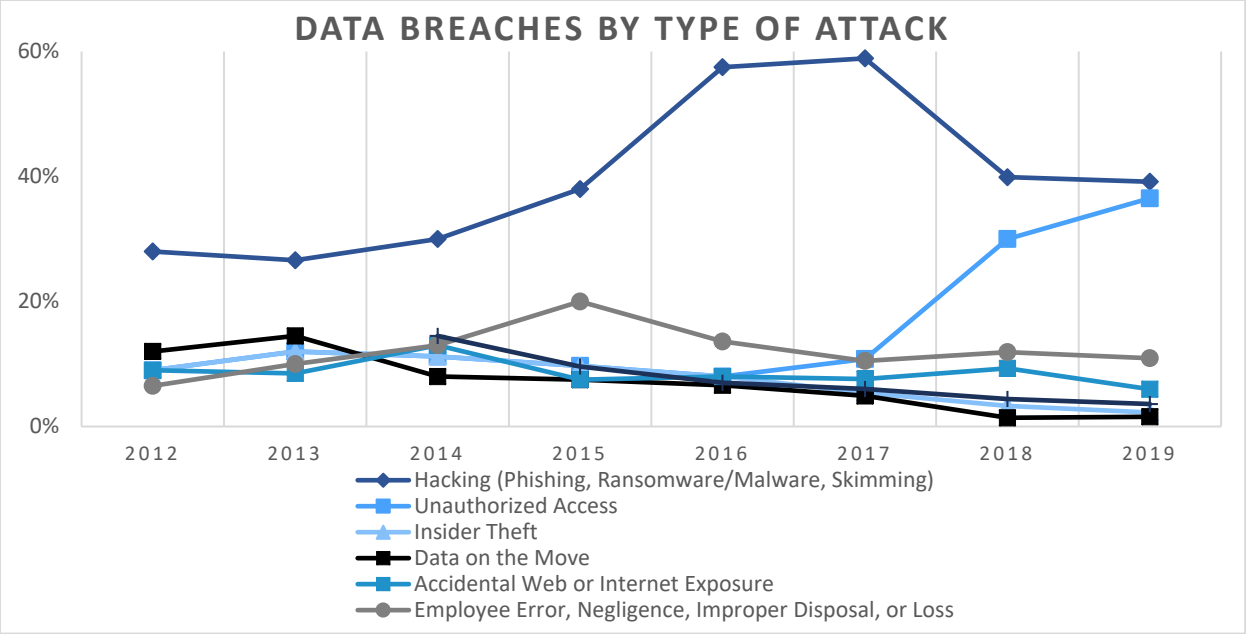
What the Numbers Tell Us

Data security is of the highest importance for every industry. According to the Identity Theft Resource Center (ITRC), U.S. data breaches rose by 17% in 2019. By October, figures for 2019 had already exceeded the total for 2018. The biggest factor in that rise was more people having access to various technology.

As illustrated on the next page, the leading causes of data breach incidents in 2019 were hacking, skimming, and phishing attacks. These methods all have a common purpose: to obtain user names, passwords, and personally identifiable information (PII). PII presents an alluring target to hackers because Social Security numbers and birth dates can be used to fake entire individual profiles and have monetary and other value for many illicit activities. When hackers gain access to non-sensitive accounts, they know the same credentials may be used for sensitive accounts, which exposes a variety of personal information.

Your organization is not immune to these threats. Names, identification numbers, and bank account details are just some of the sensitive data that could make an enticing target for hackers.

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



Data Breaches in 2020

The Experian Data Breach Industry Forecast 2020 identifies trends in how scammers attempt to steal personal information. Here are the top 5 for 2020, according to the report.

Text-Based Scams

Companies increasingly use text messages to advertise products. This is an effective marketing tool because it requires little writing and no illustrations. Recipients also read text ads by at a much higher rate that email ads. Text ads offer scammers an easy opportunity to deploy phishing scams without writing or designing an email. All it takes is a list of mobile numbers, a short text message, and a link to a phishing site.

Free Public Wi-Fi

The convenience of free wireless internet offers hackers a new way to steal personal information and login credentials. Experian notes that Wi-Fi in outdoor public spaces is a prime opportunity for data thieves to peek into user sessions. Drones equipped with cameras could soon record user names and passwords on free Wi-Fi.

Deepfakes

It has never been easier to use connected technology to share audio or video files. Deepfake technology is cutting-edge artificial intelligence that replaces a person in an existing image or video with someone else's likeness, making it possible to depict a false reality. Deepfakes can create opportunities for scammers to exploit fake news, hoaxes, and commit financial fraud.

Hacktivism

Groups form online to discuss shared interests via chat, forums, and social networking sites. When online groups are ideologically based, members may incite real-world activism to further a political opinion or dispute another

group's messages. Hacktivism is an effort by which a group disrupts another group using technology, and Experian predicted an uptick in 2020.

Point-of-Sale Skimming

How we pay for everyday items is evolving. Device-based payments include mobile tools for accepting debit cards or wireless communication via mobile devices. These new types of transactions are attractive to data thieves, especially at events with many people making purchases, such as concerts and sporting events.

Recent Attacks

Recent high-profile events have involved ransomware. An attacker invades a network through spam email, a camouflaged link, or a Trojan Horse attachment, encrypts data, and locks 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. In 2019, Emsisoft reported a barrage of ransomware attacks in the U.S. affecting 113 government agencies, 89 educational institutions, and 764 healthcare providers at a potential cost in the billions. For perpetrators, ransomware is a pure moneymaking enterprise, but for public entities, attacks could have catastrophic ramifications. Incidents can put people's health, safety, and lives at risk.

The Benefits of the Cloud

Cloud-based technology offers key benefits around security, cost savings, and convenience.

Work Securely

Using software products from multiple vendors can heighten risk exposure, especially when sensitive data is shared across platforms with disparate security levels. When hackers attempt to penetrate an organization, they look for weak applications and then move laterally to the hacked organization's other systems. Therefore, hackers can use an improperly hardened system to access a valuable target, even if it does not contain sensitive data.

For end users, differences between cloud-based and locally hosted software are minor and often unnoticeable. Users log in with a unique name and password and use the software to work with their organizational data.

Spend Smarter

Outsourced hosting services are a proven strategy to get more value from an IT budget. For most organizations, building in-house services and security infrastructure comparable to a large cloud provider is cost-prohibitive.

The best cloud companies offer seamless security and back up data in interregional locations. They have teams of security experts constantly monitoring the environment to block attacks and investigate anomalies.

Gain Efficiency

The cloud offers a unique opportunity to work with live data from anywhere with an internet connection. For example, reports with live data offer stakeholders a real-time, single version of the truth. Executives can review reports, approve expenses, and authorize payments when and where it's convenient for them, instead of being tied to a desk.

The Yardi Solution

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 all data to an off-site center to ensure business continuity. We exclusively host in Tier 3 co-location spaces from leading providers, with end-to-end redundancy for power, internet connectivity, and more.

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.

Track Record of Success

Yardi has been named to the Forbes Cloud 100 list of world leaders in private cloud computing every year since the list's launch. A panel of judges representing leading public cloud companies selects awardees, using qualitative and quantitative data along with third-party data sources. The evaluation involves four factors: market leadership (35%), estimated valuation (30%), operating metrics (20%), and people and culture (15%).

Conclusion

Complacency is one of the biggest threats to data security. There is no time to celebrate once an attack is averted or a breach is sealed. Attackers have likely already moved on to more advanced techniques.

Working with a successful cloud service provider is a great way to gain peace of mind without a large investment in time and staff. Staying on top of the latest developments in data security is one of Yardi's many vital services for its cloud customers. 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.

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.

Copyright Notice: This document contains confidential and proprietary information and is intended solely for the entity and specific purpose for which it was made available and not for any other purpose. No part of this document may be disclosed to any third party without the prior written authorization of Yardi Systems, Inc. Information is subject to change without notice and does not represent a commitment on the part of Yardi Systems, Inc. Yardi, the Yardi logo, and all Yardi product names are trademarks of Yardi Systems, Inc.
© 2020 Yardi Systems, Inc. All rights reserved. Revised: December 15, 2020.