Cloud security and your enterprise

Information security isn't something you have—it's something you do. Security is also not ensured by one or two things you did in the past then forgot about. As your chief information security officer will tell you, security is a permanent, ongoing process that requires long-term vigilance. Successful security depends on having committed people consistently applying the most reliable tools, technologies, and processes to reduce risk to a reasonable level. You'll never reduce risk to zero, but it is possible to lower your risk to a level that corresponds with the probability and impact of a security breach, at a reasonable cost.

In that context, the debate about whether cloud computing is more or less secure than on-premise data is an abstraction that misses the point. As long as your system is connected to the public Internet, whether it's a cloud solution or on-premise software, you incur some risk of a data security breach. The essential issue is whether you've put appropriate controls in place to minimize risk to the confidentiality, integrity, and availability of your data.

The importance and urgency of data security and privacy can't be overstated. In 2017 some of the largest data breaches in history took place, while the direct cost of resolving a data breach averaged **$3.62 million**. But the direct costs are a trifle compared to the incalculable, lasting brand, reputation, and business damage that a data security incident can cause.

Table of Contents

Understanding the threat

Risks associated with information security threats increase daily. The number of potential attackers is also expanding to include not only independent attackers and small groups, but also state-sponsored hacking organizations that are much better organized and funded. These larger groups can afford to devote multiple resources to breaching the defenses of small and large organizations over a long period of time—a level of commitment attackers once reserved only for the most strategic targets.

Unless your organization maintains an environment that prohibits any external Internet access, odds are your corporate environment has already suffered a successful attack of some type, even if it's something as simple as the unauthorized release of some personal data. As **Cisco CEO John Chambers** put it, "There are only two kinds of companies: Those that were hacked and those that don't yet know they were hacked."

This isn't the fault of your internal IT organization. Today's business environment demands a level of agility and efficiency that requires organizations to open their networks in ways that would have been unimaginable until recently. That openness, while essential for keeping a business competitive, has made the job of maintaining a secure network even more difficult.

Organizations like the Cloud Security Alliance, and other research groups, frequently cite compelling reasons to aim for the best possible security, whether you use cloud-based software or on-premise solutions.

The top 5 reasons to upgrade your security:

1. **There's a high likelihood your organization will experience disruption**—**Experts agree** that an expanding array of security threats increase nearly every company's risk of disruption. The most expensive disruptions result from denial of service, malicious insiders, and web-based attacks. However a wide variety of causes can trigger costly disruptions to the confidentiality, integrity, and availability of your data.
2. **Malicious insiders cause a surprising proportion of attacks**—Employees are the most frequently cited culprits of data security attacks, according to **research by PWC**. In that respect, on-premise data and cloud-based data are equally vulnerable. That makes it essential for an organization's security infrastructure to encompass both cloud and on-premise data with equal vigilance.
3. **Cyber attacks remain costly**—A study by the **Ponemon Institute** showed that the cost of a cyber attack averaged $3.62 million in 2016.
4. **Shadow IT is on the rise**—More than 80% of employees use cloud or SaaS applications that haven't been approved by IT, according to a study by **Frost & Sullivan**. That habit persists, despite the fact that 15% of employees say they've personally experienced security incidents (including malware infections and data loss) resulting from using those applications.

5. **BYOD practices add new risks**—Nearly every employee today arrives at work with one or more web-connected computing devices, mostly smartphones and tablets, that can create security risks beyond the control of the IT department. Whether or not there's an official "bring your own device (BYOD)" policy, the risks created by the profusion of employee-owned devices in the workplace pose an ongoing challenge to your information security process.

The power of standards and compliance

Standards play a vital role in information security, ensuring that practices are thorough, consistent, and effective. Arguably, the best known world-wide standards that prescribe an effective information security management system and the detailed controls, are ISO/IEC 27001:2013 and ISO/IEC 27002:2013—although many organizations choose to rely upon NIST 800-53, the Cloud Security Alliance, SSAE 18, SOC 1, SOC 2, or other standards that typically prescribe similar controls. These standards describe, in extensive detail, the security controls, procedures, and processes that an organization must follow to consider itself compliant with currently prevailing best practices. An ISO 27001-compliant cloud host should also meet the standard across several key domains, including:

- **Security policies**—All employees should be held responsible for the security of non-public information and follow the practices defined within the information security management system.
- **Information security organization**—Management must be committed to security and establish an organization that is responsible for the security of non-public information.
- **Asset management**—Assets should be strictly controlled and all data classified, in order to determine appropriate requirements for access and handling.
- **Human resources security practices**—The organization must conduct a comprehensive background check at the time each employee is hired, and require that employees maintain familiarity and compliance with security responsibilities. When employees leave or transfer, a formal process must be in place to remove or update their physical and virtual access to the company infrastructure.
- **Physical and environmental security**—Critical components must be placed in physically controlled spaces with sufficient access controls to secure infrastructure. Organizations must also implement policies about who has access to controlled spaces, under what circumstances, and consistently monitor compliance with those policies. Physical and environmental security measures may include identification cards, badges, or biometric access controls, and should limit access to secure locations based on job function.
- **Operations management**—The organization must establish controls regarding system planning, protection from malicious code, backup processes, network security, media handling, and information exchange. Those controls should be constantly analyzed and monitored to ensure they provide reasonable protection for covered data. Third-party service providers with access to confidential information must adhere to security and privacy requirements that are consistent with, and at least as restrictive, as the organization's own policies and procedures regarding the protection of confidential information.

- **Access control**—All access to systems, networks, and applications should be controlled down to the user and resource level with role-based privilege techniques. This access should be reviewed on a periodic basis to ensure that a change of personnel or a change of role has not modified the access needs of the individual.
- **System development**—Security requirements of all applications that handle confidential information must be defined early in the development stage. Appropriate data protection techniques should be designed into the application, and changes to developed software must go through a mature change management process.
- **Incident management**—In the event of an actual or reasonably suspected security incident, teams must immediately begin work to identify the scope of impact, mitigate any exposure, determine the root cause of the incident, and take appropriate corrective action, including escalation and notification of affected parties, as necessary.

Remaining vigilant

If information security were scored based on risk, the perfect score would be zero—and unachievable. Too many threats arise every day to ever expect a year with no exposure to risk. But you can aspire to a similar ideal by taking some essential precautions:

- **Adopt a secure cloud framework**. Put as much of your computing capability as possible within a framework that has been certified for compliance with recognized standards such as ISO 27001, ITAR, and FedRAMP. Top-tier cloud infrastructure providers typically comply with those standards and maintain an ongoing process for staying compliant with appropriate security standards.
- **Make sure your organization follows the current security standards of your industry**. Standards such as HIPAA and ITAR, and FDA regulations are designed to optimize security around the types of information that are most critical in specific industries. To achieve effective security, both you and your cloud infrastructure provider need to meet the security standards that are most relevant to your industry. The chain of security is only as strong as its weakest link. Security standards also evolve over time, and they provide a benchmark that helps measure whether your organization's security practices and procedures are sufficient to keep your risks as low as they can reasonably be at any given time.
- **Consider a compliance validation service**. Third-party consultants that specialize in evaluating regulatory and security compliance can provide a useful, impartial yardstick for ensuring that your security efforts are putting your organization in the right position.
- **Make sure all of your cloud vendors observe the latest security standards**. Cloud technology is making it easy for a business to adopt many different cloud-based services for different functions—sales automation, ERP, asset management, payroll, and more. It's essential that all cloud vendors support the security standards that cover your industry and understand the specific security requirements of your business.

By seeking compliance with accepted standards wherever possible, you can reduce your organization's exposure to risks and be prepared to resolve problems quickly and at the lowest possible cost.

In summary

Review the standards

By staying compliant with security standards such as ISO/IEC 27001:2013 and NIST 800-53, and keeping up with the latest recommendations in those standards, you reduce your risk of a disruptive cyberattack.

Learn more about the Infor Cloud at infor.com/cloud

Share this :

641 Avenue of the Americas, New York, NY 10011

INF-1475040-en-US-0218-2