CYBER READINESS
INSTITUTE

Cloud FAQ:

Improving Cybersecurity for Remote Workers

In response to the COVID-19 pandemic, the workforces of most companies have become remote. Remote work introduces new cybersecurity risks, especially as employees access information in new ways, including through the cloud.

Now is the time to evaluate how your organization uses the cloud. The cloud has multiple capabilities that can help make remote work more practical, efficient and secure. This FAQ is designed to help senior management of small and mid-sized enterprises (SMEs) become familiar with cloud terminology and understand the basics of how the cloud can improve cybersecurity for your remote workforce.

I hear a lot about "the Cloud," but what are the basics I need to know?

The "cloud" refers to a group of computers (known collectively as servers) owned and operated by a company (typically referred to as a Cloud Service Provider or "CSP") that provides you with software or storage. A customer or business licenses the use of the software and/or storage, typically on a monthly basis with costs changing based on usage similar to monthly utility costs.

The CSP is responsible for operating, maintaining and upgrading the computer hardware (e.g. storage, servers), which is physically located in a data center and not on the customer's premises. As a customer, you pay for using their services.

guide@cyberreadinessinstitute.com

What are some common terms I'll hear when I talk to people about the cloud?

DATA CENTERS

Think big warehouses filled with computers connected to the internet and known collectively as "servers." When you as a customer use a service (e.g. Outlook) you are essentially renting both space (storage) and services (email) to write, read and send emails.

SERVERS

A collection of computers and hardware connected to the internet which provide some kind of service, storage, or other function.

CLOUD SERVICE PROVIDERS (CSPS)

The companies that provide services to you as the customer. Some well-known examples are Microsoft, Google, or Amazon Web Services (AWS).

SOFTWARE AS A SERVICE (SAAS) (pronounced "sass")

A CSP hosts on its servers the software your company accesses over the internet. It is common for companies to license the use of many types of software such as email (Google Mail), word processing (Microsoft Word), spreadsheets (Google Sheets), accounting (QuickBooks), and sales management (Salesforce). This is the most common way for small businesses to use the cloud and requires the least amount of upkeep for the customer.

PLATFORM AS A SERVICE (PAAS) (pronounced "paz")

A CSP provides the infrastructure (e.g. an operating system like Windows) and the software that enables you to develop, manage and use customized applications (for example, inventory management applications or customer mobile orders).

INFRASTRUCTURE AS A SERVICE (IAAS) (pronounced "eye-azz")

A cloud service provider physically hosts components that traditionally were in an "on-premise" data center, including servers, storage, networking hardware and server software.

What are the overall security benefits of moving operations and information to the cloud?

CSPs view security as a ***core business function*** and recognize that trust is a fundamental part of their business model. They focus on continually updating the services and infrastructure provided to enable secure solutions for their customers. You benefit from their expertise and continual focus on security.

The physical infrastructure (e.g. servers, routers, networking devices) is housed in data centers owned and maintained by the CSP. This typically a.) lowers the costs associated with upkeep, including building fees and maintenance, but also b.) provides dedicated resources to protect the location from physical security issues.

CSPs enable the ***economies of scale*** allowing you to access resources and services that exceed what any individual user may be able to deploy. For example, CSPs pool resources to better understand the latest cyber-attacks hackers are using and to deploy solutions to protect their services and your data.

Most reputable cloud providers will clearly define what security controls they have in place and what your responsibilities are when it comes to using their service. If they don't, or if that information is not forthcoming from a cloud provider you're considering, you might want to look at another provider.

As we move to the cloud, what are my organization's ongoing cybersecurity responsibilities?

Your primary responsibility is for the behavior of your employees. You are responsible for training your people on how to prevent problems and what to do if there is a problem. You need to make sure they understand that being cyber ready is a priority for your company.

There are core tenets to understand when it comes to the security responsibilities for your organization when using a CSP:

- First, outsourcing services, functionality or infrastructure to a CSP, does not mean you outsource your security responsibility. A simple example that applies to almost everyone is employee awareness and access. Do your employees know how to detect suspicious emails? Does your organization limit/restrict employees' access to software (e.g. accounting applications) based on need and their responsibilities?)
- Second, attackers are focusing on fooling people (known as "phishing") as a way to gain unauthorized access. More than 90% of successful hacks start by someone clicking on a suspicious email link. Cybersecurity training for employees goes a long way, including practicing good "cyber hygiene" like not clicking on links from unknown senders or validating with managers emails that ask for sensitive information.
- Third, what happens to the data is almost always the customer's responsibility. For example, the leak of poorly protected sensitive customer financial data (think credit card information) that is uploaded to a CSP is the responsibility of the customer, not the CSP. And, the reputational, legal, financial, and compliance impacts, to name a few, are also the responsibility of the customer.

How does moving to the cloud improve our cyber readiness related to managing user identity (e.g. passwords and authentication)?

Many cloud providers have teams dedicated to cybersecurity and can respond to incidents in real-time, identifying when issues start and take steps to mitigate the amount of damage. One large cloud service provider receives more than 200 million sign-on attempts **per day**. This provider can learn quickly when a new type of attack threatens your passwords and take steps to prevent it from impacting you or your users.

How does moving to the cloud improve cyber readiness related to keeping software up to date?

Keeping software up to date is a huge benefit for customers and often a key selling point for cloud providers, especially when deploying a SaaS or PaaS solution. When you move to a cloud service, the provider is responsible for maintaining current software updates without you having to take any action.

However, this feature can have a downside since users may not be ready to adapt to new features as fast as cloud companies roll them out. If that applies to your company, you should ask if there is a **deferred update option** to your cloud software license. Remember, employees may still be responsible to update software that is on their individual computer, tablet or phone.

How does moving to the cloud improve our cyber readiness related to preventing phishing e-mails?

Phishing is difficult to address as it uses social engineering deception (sometimes, specifically tailored to the individual, called ***spear-phishing***) for entry into an application or access to sensitive data (e.g. login and password information).

That said, the cloud e-mail providers can learn and respond quickly to phishing attacks **once they are known**. Cloud e-mail providers can provide services to help report and block known phishing e-mails from reaching your employees. Ultimately, the best line of defense is a ***well-trained user*** who knows what phishing e-mails look like and what to do (and not do!) when they see one.

Using a cloud service provider, improves your company's cyber readiness in managing user identity, keeping software up to date and preventing phishing emails.

How does moving to the cloud improve our cyber readiness related to the use of USBs and removable media?

Moving to the cloud represents a dramatic improvement as there are no removable “media” devices required to use cloud-based software. All the cloud requires is a user with a login, a browser, and an internet connection. USBs and removable media become largely irrelevant as long as you train your users on how to use the cloud for storing, transferring and accessing the information they need.

You will still be responsible for maintaining security on physical devices, which enable removable media and might prevent the customer from accessing services. A benefit, however, is that while an individual device (e.g. desktop) could be compromised by a USB attack, the services “live” in the cloud and are accessible from a non-infected device. This is a powerful cloud feature that helps protect your business continuity.

How does the cloud help me if we do have a cyber incident?

Cloud providers spend a lot of time and money ensuring that their services cannot be brought down by a cyber incident. CSPs offer software tools that can help you isolate the root cause (e.g. event logging services, suspicious activity) of an incident to reduce the chance it happens again. The CSP data centers also have strong physical security, power protection, and fire prevention controls so you can be assured that the actual physical IT infrastructure is well-protected.

Our employees are using their smartphones for work. How does using cloud services help me reduce the related cybersecurity risk?

You do need to be aware of how your users are accessing your applications, systems, and information. You should create a mobile security policy that applies to all users regardless of the device they are using. The cloud provides the same overall security benefits for employees regardless of whether they are using their smartphone or another type of device. It is important to remember that smartphones offer the greatest threat surface and each company should be diligent in its mobile security policy.

About the Cyber Readiness Institute

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). The self-guided, online Cyber Readiness Program is available in Chinese, English, French, Spanish, Portuguese, Arabic, and Japanese. Please contact us with questions, comments or success stories (**guides@cyberreadinessinstitute.org**).

How do I prioritize what to move to the cloud?

There is no “one-size-fits-all” answer. Most organizations have what is called a “hybrid” environment that uses a mix of cloud services with self-managed, on-premise solutions (e.g. a company might use their network set-up for a small office and CSP-provided e-mail service.) Here are some considerations:

- Does the software or service interface directly with the Internet? A lot of companies move their e-mail and their customer relationship management (CRM) applications to the cloud, as those are mission-critical applications whose servers traditionally require a lot of upkeep and maintenance. Most companies today also get their basic business software (i.e. word processing, spreadsheets, accounting) through a SaaS subscription.
- How difficult or disruptive would it be? Some functions are much easier to migrate than others. For example, moving your e-mail or your file storage to the cloud is straightforward. However, moving systems like payroll or accounting that involve a lot of historical data can be much more complex.
- What are the relative costs? In comparing the costs between using the cloud and doing it yourself, make sure to also count the time and expense of doing it on-premise. It is not just the hardware and software cost – it is the time to set-up, update, maintain and troubleshoot your system.
- Evaluate the enhanced security aspects of using the cloud. Think about possible disruptions to your business, as well as the loss of your information – especially your most valuable information.

How will moving to the cloud impact our current workflow and what our employees need to do?

The answer to this question will depend on what you move to the cloud. Moving e-mail to the cloud typically results in very little change, whereas moving your accounting software to the cloud could represent a dramatic disruption requiring change management for your users and your organization.

What is the impact of using the cloud, if any, on how I interact with my suppliers and customers?

The simple answer is, it depends. Companies use the cloud to achieve different objectives across very diverse projects. However, moving to the cloud often frees up time and money that you would be spending on IT resources (servers, networks, etc.). In most cases, using the cloud will make it easier and more secure to transfer or share information with your customers and suppliers.