Cyber Risks & Liabilities

Fourth Quarter 2019

3 Risks Associated With Removable Media Devices

Portable hard drives, USB flash drives, memory cards and other types of removable media are vital for the quick storage and transportation of data. For many businesses, removable media can be used as backup storage for critical digital files or even free up additional storage space for work computers.

While removable media is easy to use and has many business applications, it isn't without its share of risks. The following are some considerations to keep in mind when using removable media at your organization:

- **Data security**—Because removeable media devices are typically small and easy to transport, they can easily be lost or stolen. In fact, every time you allow an employee to use a USB flash drive or other small storage device, your organization's critical or sensitive information could fall into the wrong hands. What's more, even if you encrypt your removable storage devices, you will not be able to recover lost files once the USB flash drive or other device is lost.
- **Malware**—Simply put, when employees use removable media devices, they can unknowingly spread malware between devices. This is because malicious software can easily be installed on USB flash drives and other storage devices. In addition, it just takes one infected device to infiltrate your company's entire network.
- **Media failure**—Despite its low cost and convenience, removable media is inherently risky. This is because many devices have short life spans and can fail without warning. As such, if a device fails and your organization doesn't have the files backed up, you could lose key files and data.

Thankfully, there are ways to mitigate risks associated with removable media. To use these devices effectively while maintaining data security, consider doing the following:

- Develop a policy for related to removable media use.
- Install anti-virus software that scans removable media devices.
- Ensure all removable media devices are encrypted. Passwords to these devices should never be shared.
- Instruct employees to never use unapproved removable media in a computer.
- Have employees keep personal and business data separate.
- Establish a process for wiping all portable media devices when they are no longer needed.

CONNOR & GALLAGHER OneSource

Connor & Gallagher OneSource
750 Warrenville Road, Suite #400
https://www.gocgo.com

Cloud Computing 101

There are many benefits to adopting cloud computing at your organization, such as reduced IT costs and increased scalability. However, it's important to note that there are different cloud service and deployment models, each with their own benefits and risks. There is no single type of cloud computing that will work best for everyone, so it's important to conduct research to determine the right fit for your organization.

Types of Cloud Computing Service Models

There are three distinct cloud computing service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

The SaaS distribution model provides you with an application that is managed by the service provider and accessible through the internet. As such, SaaS applications need not be installed or updated on individual computers.

The PaaS model allows organizations to safely develop, test and deploy applications without needing to manage the underlying infrastructure. This provides flexibility that allows deployments to scale quickly.

The IaaS model provides organizations with a specified amount of cloud storage space to do with whatever they want. This allows the greatest amount of flexibility, as the organization is responsible for accessing, monitoring and managing their data that is stored in the cloud. In this case, the service provider typically only manages hardware, storage and networking, though other services may be provided at additional costs.

Types of Cloud Deployment Models

Just like with service models, there are various different ways that a cloud can be deployed. This includes a public cloud, which is cost-effective and efficient but means that your data may be stored on the same server as others'. A private cloud, however, allows your organization greater control over infrastructure and computational resources by having them located on private networks.

Lastly, a hybrid cloud combines on-site infrastructure with a cloud environment. This allows organizations to utilize different types of service providers based on what is ideal for each business requirement.

Best Practices for Contracting With Managed Service Providers (MSPs)

While working with a managed service provider (MSP) can be efficient and cost-effective, it's important to carefully consider the organization that you plan on working with and get a holistic view of its operations and security. Because an MSP has direct access to sensitive systems and information, working with one is not to be taken lightly. While doing so puts your IT infrastructure in the hands of experts, it also comes with its own risks. For example, MSPs may be a target for cyber criminals, as compromising one MSP potentially compromises every organization that it works with.

To help keep your organization's digital information and resources secure, there are a number of best practices and security considerations to keep in mind when contracting with managed service providers:

- Perform a detailed risk assessment and enforce associated mitigations before working with a managed service provider. Some considerations include:
    - How a cloud service (if used) is implemented and managed
    - Who has access to data and how it is secured
    - The intended purpose of engaging with the managed service provider
    - Potential challenges that may arise during incident detection and response, such as the managed service provider's availability during off hours
- Keep operating systems and software up to date.
- Ensure that an MSP follows organizational security, privacy and legislative requirements.
- Find out how closely the MSP adheres to an IT security management framework.
- Use secure computers with multifactor authentication, strong passwords, few access privileges and encrypted network traffic to administer the cloud service.
- Do not provide the MSP with account credentials or access to systems outside of their responsibility.
- Use cryptographic controls to protect data in transit to and from the MSP.
- Consider full data encryption for critical information while at rest and while maintaining control of encryption keys.
- Employ full hard-drive encryption to ensure data at rest on storage media is not recoverable should the MSP replace or upgrade physical hard drives.

For more risk management strategies related to cyber exposures, contact Connor & Gallagher OneSource today.