Newsletter

RJ2 TECHNOLOGIES

What's Inside:

This month's perspective is brought to you by:
RJ2 Technologies President, Jeff Dann

What is the best way to save your electronic materials, content, photos, etc.? You don't want to overload your computer or collect a stack of hard drives. It can become expensive and unsafe over time. So, where can you put

Is My Data Safe in the Cloud?

your data and know that it is secure? With technology at your fingertips 24/7, there is always talk about the cloud. You may want to know how safe cloud data security truly is? Is it the right route for your needs? A simple answer to sum it up for you and give you some reassurance is that information stored in the cloud is likely to be more secure than anything stored on your own device. How so? Again, a quick answer is that cloud companies rely on far more robust and structured cybersecurity measures to protect your sensitive data than yourself or most other avenues. Let's dive deeper into these answers though.

First Things First: What is the Cloud?

The cloud is defined as a network of servers all across the world that do heavy lifting that companies and individuals essentially may not be interested in. To clarify, these servers do not exist in the sky; they exist on the ground. What exactly are these servers capable of? They can store data, compute data, as well as give people access to files and apps across different devices. How is that possible? Simply because the information is not stored on the devices themselves but rather in the cloud's servers. This enables you to utilize storage and power beyond your device's normal capabilities, which is always a plus. Some describe the cloud as any type of service or software that runs on the Internet and is not located on your device. The cloud is truly helping solve the ever-present need for more storage space in holding your digital property nowadays.

Who is Responsible for the Cloud & Data Security?

The cloud is defined as a network of servers all across the world that do heavy lifting that companies and individuals essentially may not be interested in. To clarify, these servers do not exist on the ground. What exactly are these servers capable of? They can store data, compute data, as well as give people access to files and apps across different devices. How is that possible? Simply because the information is not stored on the devices themselves but rather in the cloud's servers. This enables you to utilize storage and power beyond your device's normal capabilities, which is always a plus. Some describe the cloud as any type of service or software that runs on the Internet and is not located on your device. The cloud is truly helping solve the ever-present need for more storage space in holding your digital property nowadays.

What Does Cloud Data Security Entail?

As mentioned previously, there are various cloud service providers (and more than the recognizable ones), which means you'll need to shop around for the right cloud storage services for your own data. You will most likely want to start by considering what exactly you plan to store as well as how you need to access it. When shopping around for your business, you will want certain safety features to exist for cloud data security purposes. Here are some qualities to look for:

CONTINUED...

- Redundancy across multiple geographic locations. Why? This gives you the opportunity for your data to still be available and accessible in the case of a natural disaster destroying your data in a specific location.
- Multiple-level redundancy. What is this? Multiple copies of your data will exist in the case that a single disk or server fails, it prevents a complete loss of your data.
- Length of time it takes to delete a file across redundant servers within the cloud. Better yet, it's best to know if your file will ever really be deleted from storage banks in the cloud.
- Find a company with a reputation for exceptional network and physical security overall. This is generally always a good factor to know with any party having access to any piece of you business, especially in regard to your cloud data security provider.

You will want to consult with your managed services provider. They will be able to help you quickly and efficiently find the best options for you and your company's needs. The cloud is a great option; however, it is not bulletproof. When it comes to your company, you will want and need enterprise-level clouds. Each cloud provider has its own limitations, which means you must take precautions in continuing your overall information protection and cloud data security.

Healthy Security Habits for Your Teams With The Cloud:

Cloud data security is the practice of protecting and securing a company's data in your cloud environment, no matter the data location (rest or in motion) and management type (internally or externally by a third party). You want to avoid security breaches, loss or theft of sensitive data, application vulnerabilities and malware propagation. What are the top risks for cloud data security? Those risks being human error, malicious intruders, insider threats, transfer errors, compromised hardware, and configuration errors. Your managed services provider can help you navigate ways to minimize those risks appearing as much as possible. In the meantime, here are some ways you can help yourself boost your cloud data security:

1. Discover and categorize your data, especially sensitive data
2. Use data masking such as encryption
3. Implement the least privilege model
4. Audit activity
5. Strong password security and habits

Top cloud providers can keep your data safe and consistently accessible. Your company must find a provider that does not have a history of data loss or security breaches. Consult with your IT team and/or managed services provider to find the right fit for your cloud data security needs.

Conclusion:

If you want more information regarding cloud options and cloud data security that will benefit you and your organization, contact us today. Regardless of your business size, the benefits of a long-term relationship with a knowledgeable and reliable provider are essential for creating a thriving company. RJ2 Technologies can provide that to you.

RJ2 SPOTLIGHT

Jeff Dunham
IT Systems Engineer

Jeff Dunham has been working in and around technology since 2001. He got his start in the construction industry, working with installing Smart homes.
Prior to joining the RJ2, Jeff was an integral part of a small IT firm focused on both residential and SMB developing a wide variety of skill sets in variety of different Industries. Since joining RJ2 Technologies in 2017, as a Systems Engineer, Jeff has continued to develop his technical knowledge, to become a go to asset for physical infrastructure, and Telephonic needs.
Fun Fact: Jeff had the opportunity to visit Yokosuka, Japan and was able to tour around the Asia Pacific.

Where's your favorite place in the world?
- Anywhere with a good view to watch storms, sunset/rises

What do you like to do when you aren't working?
- Enjoy the outdoors, and tinkering projects

What is the best career lesson you've learned so far?
- Don't stress the little things.

If you could meet anyone in the world, dead or alive, who would it be and why?
- Probably someone from ancient times like Ramesses II to learn how the Pyramids were built, or maybe even some from Stonehenge era to see how it was built and used.

What is your favorite part of working at RJ2?
- The moment when a client realizes some piece of technology, that they were fighting, can work for them.

Why an IT Security Audit is Necessary for Your Business:

Within the last 10 years, businesses have seen huge advancements in computer technology and this trend shows no signs of slowing down. The online business landscape has seen innovative advancements largely contributed by the introduction of cloud-based resources that have helped companies smoothly manage their operations through a practical online IT environment. As organizations transfer their infrastructures to the cloud, they open the door to potential cyber threats that can have drastic impacts on company operations/performance.

Recently, United States leaders have issued warnings regarding the expectation of Russian cyber attacks due to current foreign affairs. With that being said, cybercriminals are constantly discovering new hacking techniques and we have seen a steady increase in cyber attacks over the last decade. That is why it is paramount to have a team of experts conduct security audits to ensure that your company is taking the proper precautions to protect yourself from potential threats.

Featured Partner:
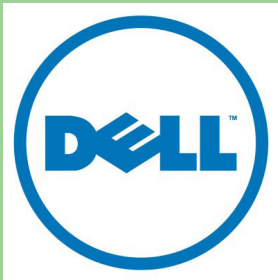
Dell

Dell listens to customers and delivers innovative technology and services they trust and value, offering a broad range of product categories, including desktop computer systems, servers and networking products, software and peripherals and enhanced services.

WHAT IS AN IT SECURITY AUDIT?

A true cyber security program is focused on two things: detection and prevention. By narrowing the goals to detect and respond to threats, a strong cyber security plan becomes a bastion against digital assault. An IT security audit analyzes your current network infrastructure for weak points both virtually and mundane. Basically, the security audit is an in depth assessment of an organization's current cybersecurity measures.

Here are some of the ways your existing network is reviewed:

- Comprehensive penetration testing: we try and break into your network using known techniques.
- Risk assessment: We investigate your current standards of security and assess their efficacy.
- Historical Auditing: We review your network activity for any signs of previous intrusion.

TYPES OF IT SECURITY AUDITS:

There are two forms of IT security audits, namely:

- **Internal audit:**
In an internal IT security audit, a company uses its own resources and auditors to conduct the assessment. The organization conducts an internal audit to determine if its systems and cybersecurity policies are compliant with its own rules and procedures.

- **External audit:**
An external audit is carried out by a third-party. External audits are performed when a company needs to ensure that it's complying with industry standards and government regulations.

WHY IS AN IT SECURITY AUDIT IMPORTANT?

Conducting an IT security audit produces a guideline for your businesses key

cybersecurity vulnerabilities. This audit details the areas where your company is meeting the cybersecurity requirements and shows the areas where you are falling behind. The key element is providing information to businesses that shows a personalized description of how current prevention and detection measures match up with cybersecurity standards. These audits are essential for creating a risk assessment plan that will give you a road map on how to keep your business protected.

WHAT IS THE OUTCOME OF AN IT SECURITY AUDIT?

Once we understand your network and review its security measures, we go to work on improving and strengthening your defenses. A few ways we do this are:

- Comprehensive Auditing – We watch your network to detect any signs of attack or attempts to bypass protections
- Multi-factor Authentication – We implement a simple multi-factor system for employees, reducing the opportunity for physical data breeches
- Updated Threat Analysis – Our team reviews and designs defenses for the most cutting edge intrusion techniques using threat intelligence tools
- Behavior Monitoring – We observe IP addresses, password logs, and MACs to ensure no suspicious traffic gains access.

Ultimately, each security audit provides different results for each business. The benefit is that the audit and plan are personalized for your business and will show you the measures that need to be taken to ensure adequate cyber protection.

If you need help in conducting an IT security audit for your business, contact us today to see how our managed solutions can help.

Newsletter

How to Collect Customer Data Securely and Effectively :

One of the most important aspects in business today is having and collecting accurate customer data. This data can help a business better understand their audience to make predictions about how to effectively reach them and what channel to reach them through. However, it is important that the business is practicing good data generating habits that focus on compliance with data protection laws. Before a company can collect, use, and generate revenue from lists, they need to take the proper precautions to avoid legal fines and penalties. Use these tips to comply with data protection laws.

1. PRIORITIZE SECURITY

According to IBM, the global average cost of a data breach was found to be $4.24 million in 2021, which is up 10% from the previous year of $3.86 million. For smaller to medium sized companies, the average cost of a data breach is $120,000 per incident.

To avoid the costs associated with a data breach and to protect the personal data of your customer, it is paramount to invest in proper security systems with employee training on data privacy best practices.

2. EXERCISE ETHICAL DATA COLLECTION

In order to ethically collect consumer data, you must be upfront and transparent about what you plan to do with their data, give an option for the customer to choose what information they would like to share, and offer a clear privacy policy. Implementing these three things will help your business to ethically collect information while maintaining compliance with data protection laws.

3. COLLECT ONLY THE DATA YOU NEED

Approximately 60% to 73% of customer information collected by organizations is unused during the analysis process. Collecting too much data can result in what is referred to as information overload. Information overload is a state of being overwhelmed by too much data, making it difficult to sort and validate which aspects of the data are specifically important. The downside to collecting too much data is that it makes it difficult for management to make effective, informed decisions. It is generally a good practice for businesses to decide the following:

- What information to prioritize
- How the information aligns with business objectives
- How the data will be analyzed
- How this data can help improve the business

4. BACK UP ALL DATA

Your customer data list is one of the most important assets to a business and losing it to some sort of disaster would prove to be a waste of both time and resources that went into acquiring the data. This is why your business needs to invest in an effective and reliable backup and disaster recovery plan that stores your data for you in the event of a cyber attack, natural disaster, IT failure, etc. Investing in this service will offer you the peace of mind in knowing that all your data is being backed up and can be reached quickly in the event of a disaster.

5. UPDATE CUSTOMER DATA REGULARLY

Outdated or incorrect information such as wrong email, phone number, address, name, and job title can prevent your business from further developing relationships and can prove to be inefficient in day to day operations. For this reason, it is necessary to go through and scrub your list regularly to validate that the information is up to date. Sometimes people change jobs, move locations, and get new numbers or emails and it is necessary to update that contact information.

Having valid customer data that you can analyze will greatly benefit your company's overall marketing strategy. If you are in need of an IT company/solution that can protect, monitor, and maintain your data, then give us a call today or click here to get in touch.

Tech Tips of the Month:

- Don't want anyone looking at your screen while you're away from your desk? On your keyboard, hit the Windows logo + L to instantly lock you screen.

- Need to see a document up close? On your keyboard hold down Ctrl and scroll on your mouse to zoom in and out instantly.

- Can't afford any downtime in your business operations? Ensure you are making consistent, recoverable backups to your data to protect your company from a potential cyber attack. This way you'll be able to quickly restore your data to keep your business up and running.

Recent Company Photos:

RJ2 Staff with Paul Nadeau at the ASCII MSP Success Summit 2022

RJ2 Staff with Hall of Famer Emmit Smith at the Robin Robin's 2022 Bootcamp Conference

How to Pick the Best Cloud Service Model for Your Business:

There are a variety of different cloud computing services and selecting the best one for your business can be challenging. In this blog, we dill go over a few different types of cloud computing service models, their benefits, and some important factors to consider when selecting one for your business.

1. SOFTWARE-AS-A-SERVICE (SAAS)

One of the most common types of cloud computing services is known as Software-as-a-service (SaaS). The difference between the software that you install on your computer and SaaS is that this solution is hosted on your provider's servers, giving you access to applications through the Internet instead of installing them yourself. When you access the web through whatever browser of your choice, the device sends inputs to a data center. This data center is responsible for processing the inputs and sending the outputs back to your device. There isn't much processing that is done directly on your device and the nice thing is that as long as you have an Internet connection, you can access this software through any device at any time.

A nice feature of SaaS is that you, the end user, is not responsible for any sort of maintenance, installations, or updates. This is all done by the provider and they are in charge of mass updating the software so users all have the same version at the same time. This means that you won't have to waste time and resources with manually updating your software.

For improved efficiency and productivity, SaaS software solutions typically include document creation suites, accounting software, email services, HR solutions, content management tools, customer relationship management systems, and more.

In a nutshell, SaaS is:

• Available any time over the Internet
• Hosted on a third-party's remote server
• Scalable for different business sizes and needs
• Inclusive, offering security, compliance, and maintenance as part of the cost

2. PLATFORM-AS-A-SERVICE (PAAS)

Platform-as-a-Service is mostly used by developers for testing their own software or apps in a virtual environment.

This means developers don't need to build and maintain their own infrastructure consisting of networking devices, storage, servers, an operating system, and other necessary hardware and software when developing applications. This saves them time and money.

Aside from helping businesses improve the quality of their products, PaaS enables businesses to shorten their product development cycles, leading to faster time to market for new products.

Most companies that utilize PaaS do so to either host or develop their own software solutions or provide support for software used by their employees. But while PaaS is gaining popularity with many small businesses, most won't have firsthand interactions with this type of cloud unless they need to build their own software or app.

Generally speaking, Platform-as-a-service solutions are:

Accessible to multiple users for enhanced collaboration
Scalable, with various tiers of resources to suit the size of your business
Built on virtualization technology
Easy to run without extensive system administration knowledge

3. INFRASTRUCTURE-AS-A-SERVICE (IAAS)

IaaS is considered one of the most flexible cloud models, as it gives the most ideal options when it comes to IT hardware infrastructure. IaaS offers services such as pay-as-you-go storage, networking, and virtualization. The most popular and well-known type of IaaS is the virtual machine — a digital version of a computer or server that is accessed over the Internet. IaaS gives you cloud-based alternatives to expensive on-premises infrastructure, so you can use your funds to invest in other things.

In other words, if you are looking to virtualize your systems via the cloud, IaaS is a good place to start, as it allows you to easily move existing support systems. Other solutions can then be migrated or introduced as needed.

IaaS is:

Highly flexible and scalable
Accessible by multiple users
Cost-effective
While the cloud offers a wide variety of benefits and solutions, choosing the service model that best fits your company's needs can be daunting. Get in touch with us today and we'll help you find