ISSUE 57 ■ OCTOBER ■ 2022

RJ2 TECHNOLOGIES

Newsletter

What's Inside:

Cybersecurity: What is it and why do you need it?

Cybersecurity is a complex area of computer security that focuses on protecting systems, data and networks from attacks. A cyberattack is any attempt to gain access to a system or network with malicious intent. Cybersecurity can be very technical, but there are some basic things you can do to protect yourself against cyberthreats.

October is National Cybersecurity Awareness Month (NCSAM). The NCSAM campaign is an annual awareness initiative, led by the Department of Homeland Security and a coalition of government agencies and private-sector partners, to help Americans better protect their online activities. With it being cybersecurity awareness month, we would like to take the time to inform you about the threats, solutions, and importance of cybersecurity.

What is Cybersecurity?

Cybersecurity is the protection of computer networks, devices and data from theft or damage to maintain the integrity and confidentiality of data. It also encompasses many sub-disciplines and areas of study. The practice of cybersecurity encompasses an array of specialties and fields that include internet security, network security, information security, risk management, systems analysis, and design (for example secure coding), cryptography, physical security (for example locks) and law enforcement investigations.

Why Should You Care About Cybersecurity?

It has become common knowledge that our personal information is not safe online. Credit card numbers have been stolen; social media accounts have been hacked; private photographs have been leaked onto public forums where anyone can view them without permission. While these incidents are alarming for those affected personally by them and indeed may be devastating for some individuals, they also pose a threat to businesses and the data of their employees and customers.

Increase in Cyber-Attacks Over the Years

As you can imagine, there has been a significant increase in cyber-attacks over the years. This is due to many reasons, but mainly it's a result of cyber criminals becoming more organized, more sophisticated, and more lucrative. It is estimated that the total global costs from cybercrime last year (2021) was $6 trillion. This is a number that is expected to only grow larger over the years and is estimated to reach $10.5 trillion in damages by 2025. This is an area that is going to continue to grow and needs to become a priority of focus for businesses around the world.

Continued on page 2.

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

CONTINUED...

However, the main reason for this increase is due to human error. Our world has changed so much in the last decade and so have our habits when it comes to technology use at work or home. For example, people are now used to working from different devices with multiple platforms and accessing data from them at all times of day or night. This can lead us down a dangerous road if we're not careful enough about how we handle our personal information online (or even offline).

There are also new technologies being developed everyday which make accessing sensitive business information easier than ever before – such as cloud-based storage systems like Dropbox where employees can share files between each other without any security measures put in place by their employer! But these aren't just problems that affect companies either – they also affect individuals too!

Threats, Attacks, and Vulnerabilities

Cyber threats are often thought of as being synonymous with cyberattacks, but they're actually different. An attack is a malicious action that exploits vulnerabilities in an application or system to gain access to sensitive data, disrupt normal operations, or steal money. A vulnerability is a weakness in an application that enables an attacker to carry out an attack. Cyberthreats can also be classified by their level of risk.

Types of Cybersecurity Threats

- **Malware**: Any software designed to infiltrate your computer and cause harm.
- **Phishing scams**: Emails that appear like they come from legitimate sources but really contain links to websites hosting malware or other types of malicious content.
- **Spyware/adware**: Software installed on computers without the owner's consent, which then tracks personal information such as keystrokes entered and web forms, then sends this data back to the attacker.
- **Man in the middle**: This type of attack occurs when an offender positions him/herself in a conversation between a user and an application usually with the intention of eavesdropping or impersonating one of the members to steal information.
- **Denial of Service (DoS)**: This is a type of attack where the computer or network is "flooded" so it is unable to process requests. Also known as a Distributed Denial of Service (DDoS) where there are multiple computers or machines involved that are used to specifically target and flood a resource.

What Could Happen if Your Business is Breached?

If your business is breached, the most likely result is that you will have to pay a ransom to get back the stolen data. The hackers could also sell the data for profit or use it for malicious purposes. These are only some of the things that can happen if you don't take steps to protect yourself. A breach can also cause damage to your reputation, which will surely hurt your bottom line. If customers think their personal information was compromised by an attack on one of your systems and they believe you didn't do enough to protect them from harm, they may choose not to do business with you anymore. This means losing potential revenue and other potential customers as you have now violated that level of trust between business and customer. The best way to avoid these types of issues is by having a solid cybersecurity policy in place. This will help you protect your business and its customers from cyberattacks.

How Has Cybercrime Evolved Over the Years?

Over the past few years, cybercrime has evolved from simple attacks to more sophisticated and complex attacks. It has become a global problem that affects businesses, governments, and individuals. Cybercrime is now one of the biggest challenges facing business today.

Cybercriminals are using ever more sophisticated methods to commit their crimes. They can easily hide their identity or location by using remote access software to gain access to others' machines without leaving a trace of themselves behind.

Organized crime gangs are increasingly targeting small businesses for cyber-attacks because they are easier targets than large corporations with stronger security systems in place specifically designed to mitigate this type of risk - so what can you do?

One of the Best Means of Reducing an Organization's Risk of Being Attacked is Through Regular Employee Training and Testing

It's important to teach your employees how to identify phishing scams, which can be as simple as an email asking for sensitive information or login credentials. When you encourage employees to follow a few simple steps, you're teaching them the importance of cybersecurity awareness, which will help protect your company from potential threats.

In addition to providing cybersecurity awareness training for employees, it's also important that businesses provide opportunities for their teams to practice what they've learned. This allows everyone involved in maintaining the security of your company's networks to stay up-to-date on current threats and learn new methods for preventing them from happening again in future situations—or worse yet—from spreading across multiple systems at once!

Partner With a Managed Service Provider (MSP):

One of the best ways to keep your business protected is by partnering with a managed service provider (MSP). An MSP will conduct a cybersecurity risk assessment specifically for your business to come up with a comprehensive security plan tailored just for you. This involves exploiting your vulnerabilities, assessing the potential impact, and suggesting the proper solutions to ensure your data and customers are protected at all times. Also, partnering with an MSP means you'll not only have access to their support team 24/7, but also have a team of trained experts who will monitor your networks for suspicious activity to ensure you really are protected. In our line of work, it is better (and cheaper) to be prepared and secured rather than trying to clean up the mess left behind from a ransomware attack.

How a Cybersecurity Risk Assessment Can Benefit Your Business:

What is a Cybersecurity Risk Assessment?

A cybersecurity risk assessment can help you identify potential cybersecurity threats and prioritize where to focus your security efforts. A well-designed risk assessment process can also help you understand the potential impact of a cyberattack, which is important when determining how much of your budget should be allocated toward cybersecurity efforts.

The goal of a risk assessment is to determine what assets are most critical for the organization, as well as their value in terms of financial loss or damage to reputation. It will also identify risks associated with those assets, like whether they're vulnerable to attack by hackers or malware attacks; whether they're protected by appropriate security measures; and whether there's adequate backup in place if something happens (for example, if someone accidentally deletes data on a server).

A Cybersecurity Risk Assessment Can Help You Identify Weaknesses, Assess Your Risk Level, & Determine Where to Focus Your Security Efforts

The process of conducting an assessment may include:

- Reviewing policies, procedures, and guidelines to determine if they're implemented properly. This is important because violations or gaps in these types of documents can lead to security breaches.
- Looking at the physical environment for any potential points of weakness (such as entrances that aren't protected by biometrics).
- Conducting vulnerability scans on key systems (such as databases) to see if there are any known vulnerabilities for which patches are available but not installed yet.

A Cybersecurity Risk Assessment Can Focus on Both the Physical and Digital Components of Your Business

A cybersecurity audit is a comprehensive examination of the security of your organization's digital assets. It's important to note that the scope of a cybersecurity audit can vary greatly depending on the nature and size of your business, as well as its specific needs and objectives.

A cybersecurity audit may focus on any or all these components:

- **Physical security**: how well you protect buildings, equipment, and data centers from unauthorized access through physical means such as locks or CCTV cameras.
- **Digital security**: how well you protect against hackers who want to steal sensitive data by accessing it remotely over the Internet or other networks such as wireless local area networks (WLANs) or mobile devices such as laptops or smartphones. This includes firewalls that prevent unauthorized users from accessing network resources (such as websites) within an organization's intranet; anti-virus programs that scan incoming emails for viruses before they reach employees' inboxes; encryption software which scrambles data into codes so only authorized individuals have access to it; etcetera).
- **Cloud computing infrastructure**: whether any applications used by your organization run on cloud servers rather than being installed locally on individual computers at each office location around town. If so, then this could mean more vulnerabilities because cloud providers often don't provide adequate security measures for protecting their clients' information systems against hackers due to budget constraints.

Cybersecurity is an Important Issue for Any Business, So It's Critical That You Have a Plan in Place to Protect Yourself.

A cybersecurity risk assessment is a process that helps companies identify potential cyber risks, prioritize them and determine the appropriate controls to mitigate the risks. A good starting point is to understand the types of data you have, where it resides, who has access to it and how this information could potentially be used if exposed during a breach.

The goal is to minimize the impact of a cyberattack on your business by reducing your attack surface area so that hackers have less opportunity for success. This means making sure that all of your resources (people, processes and technology) are aligned with your business objectives so you can mitigate threats at each stage in their lifecycle – from identity theft through incident response – before an attacker even gets started

The first step is to identify which data is sensitive, what assets are critical, and what infrastructure the organization depends on. Once you understand all of these elements, you can use them as part of your risk assessment process.

A cybersecurity risk assessment is a formalized evaluation of how likely it is that an organization will be attacked by hackers or malware and how well prepared they are to defend against such attacks. This type of assessment helps organizations identify vulnerabilities within their network architecture, as well as determine where improvements need to be made in order to reduce their exposure to cyberattacks.

Conducting this kind of analysis regularly can help keep your business secure from potential threats by providing an overview of current risks and addressing any potential issues before they become serious problems.

What You Need to Know About Endpoint Protection

Introduction

Endpoint security is a topic that's rapidly gaining in popularity. With the increasing number of cyberattacks, it's now more important than ever to ensure that your company's data is safe from hackers and malware. Let's take a look at some of the most important things you need to know about endpoint protection:

What is Endpoint Protection?

Endpoint protection is a form of network security that protects an organization's devices against malware, viruses, and other forms of malicious code. This process is designed to quickly detect, analyze, and block potential attacks on your company's infrastructure and sensitive data.

Endpoint protection helps stop threats before they reach your internal network or cloud environment by using intelligence from its cloud-based database about known bad behavior patterns across millions of endpoints worldwide. When an endpoint encounters something suspicious during normal operation (like opening email attachments), it sends hashes of these suspicious processes back to the cloud database for analysis against similar activity seen at other locations around the world at that moment in time; if there's a match between this new information and what was previously seen elsewhere then action will be taken immediately based on predetermined policies set up by system administrators who want their systems protected in particular ways (e.g., blocking certain applications).

Endpoint protection software can perform real-time scanning of files as they are downloaded or executed on an endpoint device such as a laptop, desktop computer, or any device connected to the network.

Why is Endpoint Security Important?

All organizations today are under siege by hackers, and data is a valuable asset that needs to be protected. The number of endpoints in your organization is growing rapidly and with it the risk of breaches. Endpoint security provides a layer of protection for your network and business, but it's only one part of an overall strategy.

When it comes to endpoint security, there are two main types: software and hardware. The software-based options include traditional antivirus (AV) software and endpoint detection and response (EDR). Hardware-based solutions include firewalls, intrusion prevention systems (IPS), network access control (NAC), anti-spyware and anti-malware tools. It's a balancing act between the two, but ultimately you need both to protect your business.

The best-in-class endpoint security solutions provide a combination of both software and hardware, as well as advanced threat protection. They also offer additional features that are critical to protecting your organization from modern threats.

What are Endpoints and Endpoint Devices?

Endpoint protection refers to the software and hardware that protect your network from threats.

Endpoints are the parts of a network that are not part of the server, and they include mobile devices, laptops, desktops, tablets, smartphones, printers, IoT (internet of things) devices, smart devices such as watches, etc. These devices connect to a network through an endpoint security system. Endpoint security protects these devices from malware and other potential threats.

How Do You Secure Endpoints?

There are a number of ways to secure endpoints. Here's how:

- Install and update endpoint security software. Endpoint detection allows you to identify threats before they reach your network, allowing you to stop the attack before any damage is done.
- Use strong passwords on every device that connects to your network. If a hacker can get into one device, they can use that device as a gateway into your entire network, so it's important to make sure that each machine has its own password and is only accessible by authorized users.
- Install antivirus software on all devices connected to the internet—not just computers but also smartphones or tablets—to ensure that harmful programs do not infiltrate your system or spread externally when used by an infected user who goes online elsewhere (such as at work). You should also look into anti-spyware programs designed specifically for mobile devices; these apps are able to protect against malware such as keyloggers (which records what people type on their keyboards) and adware (which displays unwanted ads) without hindering functionality or performance in any way!

How is Endpoint Protection Different From Antivirus?

Endpoint protection is a set of tools that protect your devices from cyber threats. Antivirus software protects against malware, but it doesn't protect against other types of threats like phishing scams or ransomware. Endpoint protection is more comprehensive than antivirus software because it can protect against many different types of threats that antivirus alone cannot defend.

Conclusion

This is just the beginning of what endpoint protection can do for your business. There are many other benefits to this type of software, such as increased productivity and reduced costs. We also suggest combing endpoint protection with zero trust security, which means that no individual can be trusted to join the network until they have been 100% identified as an individual with the correct credentials. This provides a more layered, secure approach to security to better protect your company and data from potential breaches.

The Importance of Developing a Backup & Disaster Recovery Plan

Introduction

If you haven't developed a data backup and disaster recovery plan, now is the time to do so. As we've seen in recent years, natural disasters like Hurricane Harvey, tornadoes in Oklahoma, earthquakes in Mexico City and more have left businesses without access to critical information. These events can be devastating—but they don't have to permanently disrupt your business operations. That's where a data backup and disaster recovery plan comes in.

What is a Backup and Disaster Recovery Plan?

A backup and disaster recovery plan is a document that outlines the procedures used to protect your business data and ensure its availability in the event of a disaster. It's also referred to as a business continuity plan (BCP). A BCP can help you prepare for crisis situations, such as sudden power outages, natural disasters, hardware failures, and even cyber threats.

The goal of any BCP is to create processes that will enable you to recover from an emergency situation quickly so that you can continue operating normally without missing any deadlines or appointments with customers or clients.

A Data Backup and Disaster Recovery Plan Can Help You Save Your Business

Data loss can be devastating. It could mean losing customer data, which will cause you to lose loyalty and repeat sales.

It's important that you prepare for a disaster before it happens so that you know exactly how to recover data when the time comes. If a disaster occurs and your business doesn't have a plan in place, it can be extremely difficult and costly (if not impossible) to recover your data.

There are many ways that businesses lose their data—from employee error or malware attacks all the way up to natural disasters like hurricanes or earthquakes. No matter what kind of catastrophe occurs, having an effective backup solution will help ensure that your business is protected from any type of loss at any time of day or night; it takes just one second for everything important about your company's operation to go down – forever!

How Critical is Your Data?

The data you have stored on your computer is your company's most valuable asset. It can be used to improve customer satisfaction, increase employee productivity, and even reduce costs.

The following are just a few examples of how data can benefit your business:

- Data analytics can help you better understand your customers and potential customers by identifying trends in their buying habits or communication preferences. This information can be used to improve customer satisfaction by providing products that meet their needs and wants more effectively than before.
- After analyzing the data from surveys and reviews submitted by employees or customers, companies may find areas where they need improvement—such as training programs or work hours—and make changes accordingly. For example, if many employees are working overtime with no compensation due to an overflow of work in certain departments, then management may decide to hire additional staff members so that these workers aren't required reaching out for assistance every time something comes up unexpectedly at an inconvenient hour (elevated stress levels). In turn there will be less strain on existing resources which contributes positively towards job satisfaction among those who remain employed but also reduces costs overall since benefits such as health care coverage aren't provided automatically without extra effort being exerted beforehand; thus saving money over time while simultaneously improving productivity rates due mostly thanks to improved morale among those who choose not get fired because they don't feel like having fun anymore because all they do nowadays is work!

What Are You Losing if Your Data is Unavailable?

- Financial loss
- Loss of customers
- Loss of reputation and brand value
- Business continuity issues, including decreased revenue and increased costs due to downtime, not being able to deliver on a project deadline or other contractual obligation (e.g., an e-commerce site), etc.
- Loss of employee productivity, morale and loyalty

Tech Tips of the Month:

- **Keep your software up to date:** Updates provide new fixes, features, and upgraded security.
- **Be on the lookout for websites with HTTPS:** Be sure to check that a website is using HTTPS to ensure the transfer of information between you and the site is secure.
- **Have anti-virus and anti-malware solutions in place.**
- **Turn off your Bluetooth when you don't need it**: Your device can be hacked through Bluetooth, so if you aren't using it, turn it off.

Continued on page 6.

CONTINUED...

The Reality of Potential Disasters

The importance of backups:

It's important to make sure your data is safe, especially in the event of a disaster. If you don't have backups, or if those backups are outdated and missing critical pieces, then you may lose all or part of your business. Having consistent data backups in place helps to keep your business running if the worst happens.

The reality is disasters can happen at any given time and have serious consequences. Whether it is a natural disaster, malware, or simply human error, your data needs to be protected and backed up to ensure your business is still able to operate.

A Data Backup and Disaster Recovery Plan Can be Key to a Company's Survival in the Event of a Natural Disaster, Fire, Cyberattack or Other Potentially Devastating Event.

A data backup and disaster recovery plan is a key component to any company's survival in the event of a natural disaster, fire or cyberattack. Backups are your first line of defense against loss of important data. A backup plan should detail what data you need to back up and who is responsible for performing backups. It should also identify where the backups will be stored, how long they will be retained and what procedures should be followed if you need to restore data from backups.

It is imperative that all companies have a good understanding of their own specific requirements before developing an effective backup strategy because no two businesses face the same challenges when it comes to protecting their information assets from harm.

Conclusion

Whether you accept it or not, disasters can happen, and when they do, your data is one of the most critical aspects of your business. Having a plan in place to help make sure that no matter what disaster strikes you're going to be prepared. If you're looking to develop a business continuity plan for your business, get in touch with our team today to ensure your data is protected from the unexpected.

RJ2 SPOTLIGHT

Adam Arbuckle

Project Engineer

Adam has been working in I.T. since 2010. He started his career working for Geek Squad at Best Buy in both Indiana and California. When he moved to Chicago from California, he continued work in I.T. with local gas station chains on their Help Desk teams. Adam joined RJ2 in November of 2017 as a full-time Systems Engineer. May of 2019, he transitioned into a Project Engineer role.

Fun Fact: Adam has done stunt riding on motorcycles since the age of 21.

Where's your favorite place in the world?

- Favorite place is anywhere with my family

What do you like to do when you aren't working?

- When I'm not working, I like to either spend time with my family or go out and do stunt riding with motorcycles

What is the best career lesson you've learned so far?

- One of the best career lessons I've learned is to not give up when things get tough. It has helped me to grow and learn quickly.

If you could meet anyone in the world, dead or alive, who would it be and why?

- My grandfather on my dad's side. He passed before I was born, but always heard crazy stories about my family. Would be interesting to have heard what really happened from his perspective.

Vendor of the Month

HUNTRESS

Huntress delivers a powerful suite of endpoint protection, detection, and response capabilities that are backed by a team of 24/7 threat hunters to protect your business from today's determined cybercriminals.

Effectively hunting attackers and rooting them out demands a new approach. Through unique focus on attacker persistence, Huntress uses innovative algorithms and human intelligence to help you pursue and challenge these threats.