NEWSLETTER

RJ2 Technologies Monthly Newsletter
June 2024

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 60008

847-303-1194

www.rj2t.com

Jeff Dann
President

In this newsletter:

Why Cybersecurity for the Insurance Industry should be a Top Priority

In today's digital landscape, cybersecurity is more than just implementing a couple of software tools and believing that you're protected. **You are Not!!** As a company in the insurance industry, you understand the importance of risk management, but the risks associated with cyber threats extend far beyond financial costs.

While insurance can mitigate financial losses, a breach can have a ripple effect. It may compromise not only your organization but also impact carriers, vendors, customers, not to mention the increase to your own premiums. The impact to your reputation may take years to rebuild trust.

Cybersecurity isn't just about technology—it's about people, processes, and trust. By prioritizing your security practices, you protect not only your business but also the relationships you've built over the years. Creating a security-minded culture within your organization will educate employees on what to look for and how to respond to potential threats.

It's critical that you take your cybersecurity seriously and make sure your clients and vendors know it's a priority for you as well. Here are some tips on how to do just that:

Make cybersecurity part of your everyday culture. In order to protect yourself from cyber attacks, it helps if everyone in the company knows what's going on and knows what to do when something happens. Make sure your employees are educated about security threats by offering training courses or providing periodic updates on current threats through email or newsletters. Be proactive about security measures at all times — not just during emergencies. Make sure all employees understand their roles in protecting the company from cyberattacks by providing regular updates on current threats through email or newsletters, holding meetings or presenting videos highlighting best practices for staying safe online and reminding them to update software regularly.

Potential Data Breaches in the Insurance Sector

The insurance industry is at a higher risk of data breaches than other sectors and a recent study by Accenture revealed that the insurance industry could lose as much as $400 billion in revenue.

Insurance companies have a lot of sensitive data to protect, including personally identifiable information (PII), credit card numbers, bank account information and more. These companies are also heavily regulated by state and federal agencies, which means they have strict privacy policies in place and must comply with many different laws regarding the protection of customer data. If you work for an insurance company, you need to be aware of the potential risks your company faces in terms of cybersecurity. Here are some of the most common types of cyberattacks on insurance companies:

Phishing attacks – The most common form of phishing attack involves an email that looks as if it's coming from within the company but is actually from someone trying to gather sensitive information such as usernames, passwords or other PII from employees. This type of attack could result in theft or loss of data or money and can lead to identity theft or fraud against customers or employees.

Malware – Malware includes viruses, worms, trojans, rootkits or spyware that can infiltrate a computer system through various means including email attachments or links to malicious websites. Malware often has the ability to access sensitive information stored on your computer without your knowledge.

Data breaches are a growing concern for businesses, but they can be especially damaging to insurance companies. If a breach results in the loss of customer records, it could potentially harm the company's reputation and result in a significant drop in sales. As such, cyber security is critical for insurance companies to protect their data and ensure that their customers remain confident in their services.

The industry has a significant amount of data and sensitive information on its hands, which makes it an attractive target for hackers and cyber criminals. Insurance companies have always been among the most attractive targets for cybercriminals because they have access to confidential data about their clients, such as their personal information (names, addresses and Social Security numbers) and financial records (bank accounts). This can be used maliciously by criminals who want to commit fraud or steal money from unsuspecting customers.

Consumer Confidence Can Affect an Insurer's Financial Performance

Cybersecurity is a critical component of any business, but it's especially important for insurance companies. Cybersecurity is an integral part of an insurer's operations. It's how they protect their customers' data and their own systems. If a cyber-attack impacts an insurer's ability to fulfill its obligations to their customers, it can have a significant, negative impact on the company's financial performance. Insurers also face reputational harm when they fall victim to a cyberattack or fail to prevent one from happening. This can lead customers to question an insurer's ability to protect them against cybercrime, which may cause them to shop around for coverage elsewhere.

IA recent study by Marsh found that 80% of consumers said they would consider switching insurance companies if they had personal information stolen from one carrier and not another. In addition, consumer confidence can affect an insurer's financial performance through higher claims costs associated with fraud and identity theft or lower premiums because consumers feel more secure about their personal information being protected by the company that insures them.

Why Are Cyber Threats Different For Insurance Companies?

Insurance companies have unique risks associated with cyberattacks because they handle sensitive personal data — including medical information — that can be used by thieves to commit identity theft or fraud. The Equifax breach revealed the vulnerability of our personal data when it's collected by credit agencies like Equifax, Experian and TransUnion. Credit reports are used by enders when deciding whether to grant loans or mortgages, so it's critical that this information stay secure at all times. In addition to identity theft, stolen credit card numbers also put consumers at risk for fraudulent purchases made with their accounts without their knowledge or consent.

Vendor Partner Highlight - Microsoft

Founded in 1975, Microsoft is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

Recently, Microsoft released their own AI chatbot called Copilot. With their new AI-powered productivity tool called Graph-grounded chat, it allows the user to bring their work content and context to Microsoft Copilot's chat capabilities.

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.

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.

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

Recognizing Excellence

Employee Recognition

Here at RJ2 Technologies we recognize those who put in hard work and dedication not only towards our services, but to the teamwork they build amongst themselves.

Heather Simek - Vice President of Operations & COO

Heather has been with RJ2 Technologies for over 13 years and has played a crucial role in the growth and success of our business. Heather has been in the IT field for over 40 years. Heather has said there is no other area in IT that has such a strong community, knowledge, or passion as the Managed Service (MSP) Industry.

When Heather is not working, she focuses on her family which includes weekly dinners with all her children and grandchildren. Heather enjoys reading, traveling, and cooking when she wants to decompress

5 Tech Tips to Avoid Scams

1. Secure your personal information
Before you provide any personal information to a website such as your date of birth, social security number, account number, or passwords, be certain that the website is secure.

2. Stay informed on the latest cyber threats
Keep up with current scams through the news or through The Cybersecurity and Infrastructure Security Agency (CISA).

3. Keep your software up to date and maintain preventative software programs
Keep all software programs up to date on your computers and mobile devices. Install software that provides antivirus, firewall, and email filter services.

4. Be careful with links and new website addresses
Malicious website addresses may appear almost identical to legitimate sites. Scammers often use a slight variation in spelling or logo to lure you. Malicious links can also come from friends whose email has unknowingly been compromised, so be careful.

5. Update the operating systems on your electronic devices
Make sure your operating systems (OSs) and applications are up to date on all of your electronic devices. Older and unpatched versions of OSs and software are the target of many hacks.

Stay Connected with RJ2 Technologies

Stay up to date with the latest tech trends, company updates, tech tips, and more by following us on our social media accounts below. We strongly encourage you to stay connected with the RJ2T family and show your support!

@RJ2Technologies
http://www.linkedin.com/company/rj2-technologies/

@RJ2Technologies
https://www.facebook.com/rj2technologies/

@RJ2Technologies
https://twitter.com/RJ2Technologies

@RJ2Technologies532
https://www.youtube.com/@rj2technologies532

Follow us on our socials by either clicking the user name or copying the link!