NEWSLETTER

RJ2 Technologies Monthly Newsletter
October 2024

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

(847) 303 -1194

www.rj2t.com

In this newsletter:

Everything You Need to Know About Cybersecurity and Compliance in 2024

October is Cybersecurity Awareness month, and we want to give you the most up to date information on cybersecurity and the importance it has to the growth of your business. Every company worldwide needs a solid cybersecurity and compliance program that enables it to fulfill regulatory requirements. Your MSP knows that the point isn't just to apply compliance measures that allow organizations to operate legally - but to deliver cybersecurity frameworks that go beyond industry standards and help clients follow best practices. Lets take a look at what a small to medium sized business needs to know about cybersecurity and compliance to stay safe.

What is cybersecurity compliance?
Cybersecurity compliance is a form of organizational risk management that ensures companies protect the confidentiality, integrity, and availability of the data to which they have access. For MSPs, cybersecurity compliance involves understanding specific industries and sectors' major cybersecurity compliance requirements and the approaches that adhere to key regulators and legislation. Safeguarding sensitive data involves grasping the standards and frameworks of regulatory bodies like the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), the National Institute of Standards and Technology (NIST), or the Health Insurance Portability and Accountability Act (HIPAA).

Why is compliance important in cybersecurity?
Nowadays, most organizations, if not all, work with data, and all have a digital attack surface that consistently increases. Access to intelligence and critical information, like email addresses, bank accounts, cardholder data, and more, puts companies at risk, making them vulnerable to cyberattacks.

Cybersecurity compliance allows businesses to protect their resources while ensuring they are legally entitled to operate their business. Conversely, a lack of compliance with cybersecurity standards and frameworks may translate into significant fines that can affect a company's bottom line and even lead to bankruptcy.

Types of Data Subject to Cybersecurity Compliance

Personal Identifiable Information (PII)
Personal Identifiable Information is any data that may contribute to identifying a specific individual, distinguishing one person from another, and deanonymizing previously anonymous data.

Personal Identifiable Information may include names, addresses, social security numbers, or driver's license numbers.

Personal Health Information (PHI)
PHI, personal health information or protected health information, is defined by HIPAA as data relating to an individual's past, present, or future health. This category includes insurance information, healthcare records, and other data to which medical providers have access.

Financial Information
There is some overlapping between financial and PII, but financial information refers to bank account numbers, credit card data, or other data about a person or a company's monetary

Benefits of Having A Cybersecurity Compliance Program

All companies need a cybersecurity program to identify and adhere to industry-specific and regional regulations. To bring added value, MSPs combine mandatory standards and frameworks with other security measures and technologies to create cyber resilience. These services prepare clients for potential cyberattacks and minimize losses, penalties, and fines should a data breach occur.

Cyber resilience has several benefits for businesses:

Cybersecurity resilience protects reputation and trust capital.
Some of a company's greatest assets are its reputation and trust capital, as these are the values that attract and retain consumers. Although their worth is often inestimable, they are crucial for good business. A cybersecurity incident can affect these metrics, sometimes to the point of no return.

Cybersecurity compliance supports smooth business and the bottom line.
A good cyber security resilience program enables companies to keep their data safe and avoid up to millions of dollars in losses that would disrupt business operations and impact profitability.

Cybersecurity compliance keeps companies away from fines.
Many companies focus on understanding and accommodating compliance costs without realizing that those associated with noncompliance are significantly higher. The more sensitive the information they access and manage, the more stringent the potential fines.

For example, each HIPAA violation costs between $100 and $50,000, while PCI DSS violations require companies to pay up to $10,000 monthly until compliance is proven.

With the GDPR infringements, companies may also pay up to $22 million or 4% of their annual turnover. Amazon made headlines in 2021 when the company announced a GDPR fine of $887 million.

An effective cybersecurity program improves the organization's security posture.
Security posture defines an organization’s cybersecurity status, focusing on everything from networks to systems and people’s capabilities. The term showcases how prepared the company is to respond to ever-changing cyber threats.

Cybersecurity compliance enables MSPs to adopt strategies and tools contributing to better security posture.

6 Steps to Create a Cybersecurity Compliance Program

Creating a program that ensures regulatory compliance is a challenging task, especially since each initiative needs to adapt to the organization's business, industry, and regional regulations. Still, there is a step-by-step model that MSPs can take into account and incorporate into their workflows:

1. Identify the types of data and requirements

The first step to regulatory compliance is to identify with what types of data the company handles, in what locations it operates, and with what regulations it must comply. This information sets the premise for future endeavors.

MSPs often involve compliance specialists or attorneys in this stage to ensure they identify all the requirements and regulatory bodies companies need to comply with.

2. Define the cybersecurity and compliance team

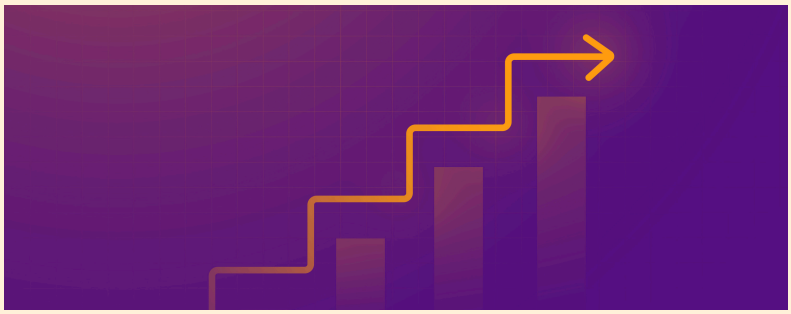
Creating a compliance team starts with naming the CISO or Chief Information Security Officer. SMBs with outsourced IT functions rely on their MSP as their CISO. That's why MSPs must prioritize cybersecurity compliance as part of their service offerings. The vendors and solutions that MSPs work with must support these standards and regulations.

Additional cybersecurity and compliance team members include IT experts like the Chief Technology Officer, Chief Information Officer, Chief Operating Officer, or IT Manager.

3. Perform risk assessments

During an initial risk analysis, MSPs identify vulnerabilities and cybersecurity risks and talk to the SMB about their risk tolerance, business continuity and disaster recovery (BCDR) needs, and available budgets. This approach enables them to identify the best solution for each company. MSPs might use different tests, including internal and external penetration testing when assessing cybersecurity readiness.

Just as MSPs test their clients to increase security and close open doors, MSPs must also assess their vendors. Axcient brings in third-party threat and security management providers to complete unbiased testing on products and specific product features, data centers, and corporate networks to ensure that they perform as expected.



4. Implement technical security controls

After determining the risk tolerance and regulations a business needs to comply with, the next step is to put technical control measures in place. Examples include standardizing anti-virus protections, implementing firewalls, encrypting sensitive data, training employees, performing patch management, or creating access control lists based on credentials and passwords.

5. Create and deploy policies

Once technical controls are in place, it is time to address how to use them and what are the mandatory requirements. To do so, you must document policies that set guidelines for IT teams, employees, and any third party accessing the network or customer data. The best way to ensure these policies get followed is through constant internal or external audits.

6. Monitor and respond

Because the digital environment evolves quickly, so do cyber threats. That's why legislation and security requirements can change rapidly. MSPs and cybersecurity and compliance teams are responsible for reviewing legal frameworks, staying connected to updates, and discovering new technologies and safety strategies. Moreover, disaster recovery planning and testing should be part of any business's regular processes to ensure rapid recovery.

While no one wants attacks to happen, it's an MSPs job to prepare clients for a data breach and develop business continuity processes that enable them to respond quickly.

Looking to start a cybersecurity and compliance plan specifically tailored to your business needs? **Email marketing@rj2t.com or call 847-303-1194** and we will get you connected to one of our IT experts to help you secure your data. Compliments to our partner, Axcient, for giving us permission to post this article.

Recognizing Excellence

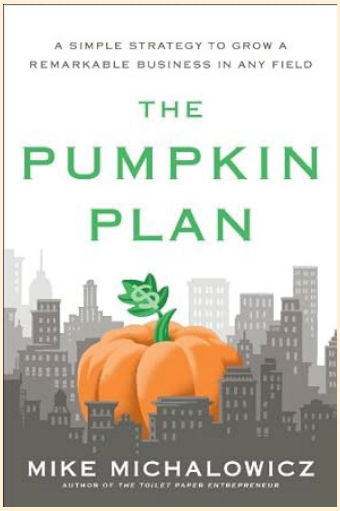
Employee Recognition

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.

Janine Aquino - Marketing Coordinator

Janine has been working with RJ2 Technologies since September 2023 as an intern and became our full time Marketing Coordinator this past May. In the short amount of time she has been here, she has learned alot about the marketing world and the growth of IT. She says, "The community of IT marketers have such unqiue and successful approaches to their marketing campaigns. I can't wait to network with them on how to improve on myself and the connections with our customers."

To keep herself busy outside of work, Janine enjoys reading, traveling, and golfing. She also likes to bake, some of her favorite goodies being cinnamon rolls and banana bread.



The Pumpkin Plan: A Simple Strategy To Grow A Remarkable Business In Any Field by Mike Michalowicz

The Pumpkin Plan, by Mike Michalowicz, is a must-read for small business leaders wanting to carve out a niche and grow their business effectively, especially during the bustling holiday season. Michalowicz presents a straightforward, actionable strategy to cultivate a remarkable business by focusing on top clients and eliminating unprofitable ones. The book is filled with practical advice and real-world examples, making complex business concepts easy to understand and implement. His engaging storytelling and clear, step-by-step approach provide a refreshing take on business growth. This book is a valuable resource for any small business owner looking to streamline operations, maximize profits and achieve sustainable success.

Vendor Partner Highlight - INFIMA

Infima is a leading provider of automated Security Awareness Training, designed to help organizations combat cyber threats such as phishing, ransomware, and social engineering attacks. This platform stands out for its automated training and phishing simulations, which require minimal management, allowing companies to focus on their core operations while ensuring their employees are well-prepared to handle potential cyber threats. With streamlined onboarding and automatic user synchronization, Infima makes it easy for organizations to integrate their security training into daily operations seamlessly.

At RJ2 Technologies, we are committed to providing our clients with the best in cybersecurity solutions. Partnering with Infima allows us to offer top-tier security awareness training that is both engaging and effective. By leveraging Infima's expertise and innovative platform, our clients are equipped to defend against evolving cyber threats. Together, RJ2 Technologies and Infima are dedicated to creating a safer digital environment for businesses of all sizes. During this month we observe Cybersecurity Awareness Month and we dedicate time to reinforce the importance of cybersecurity through special training sessions and awareness campaigns. **Call RJ2 Technologies at 847-303-1194 or email marketing@rj2t.com** to learn more about cybersecurity for your business.

Biz Buzz

Lights Out For Business: Resiliency Amid Internet Outages

Businesses are increasingly reliant on the Internet. CRM platforms, virtual meeting apps, online sales, POS systems and even office printers require the Internet so you can do everything you need to deliver high-quality products and services to your customers. However, Catchpoint's 2024 Internet Resilience Report states that 43% of businesses estimated they lost "more than $1 million due to Internet outages or degradations in the month prior to the survey."

It's tempting to blame the Internet provider when the Internet goes out. Unfortunately, outages happen. Pointing fingers at vendors won't change that. Instead, the solution must come from within.

What's Going On With Internet Connectivity

In July, a global Internet outage forced millions of computers offline, including at major airlines, banks and hospitals. The root cause of the disruption was a single software update deployed by cyber security firm CrowdStrike.

Cyber security reporter Brian Krebs famously described the Internet as "held together with spit and baling wire." It's easy to forget that the Internet, like other tech, is evolving and complex. It connects countless systems and devices globally, creating a web of dependencies. A disruption in one part of the network can ripple through and affect other systems, as seen with the CrowdStrike update. Internet outages can have serious financial and security consequences, so preparing for an outage is crucial.

Resilience Comes From Within

After an outage, you may be tempted to fire your service provider. However, Catchpoint CEO and co-founder Mehdi Daoudi explained in an interview with Tech Brew that it's not a good solution (unless they prove unreliable). Daoudi said that after an outage, it's better to work with your vendors to figure out what went wrong and how to be better prepared. Some companies have hired chief resilience officers, but the title doesn't matter as much as having a leader in your company who spends time thinking about resiliency.

"It's important that companies embrace resiliency and reliability. How? By encouraging the learning from failures, by not firing," Daoudi told Tech Brew. "What did we learn from this outage? What can we do to strengthen our postures going forward?"

The Internet is complex, and outages happen. To safeguard against the inevitable, businesses must cultivate resilience internally and proactively collaborate with Internet vendors to avoid damaging consequences.

GADGET OF THE MONTH

The Ring Video Doorbell Camera

Is it a trick-or-treater or your annoying neighbor? Find out with a Ring doorbell camera. The Ring Video Doorbell Camera offers crsip 1080p HD video, enhanced motion detection and night vision. It's easily set up with its rechargeable battery or existing doorbell wires and lets you see, hear, and speak to visitors via your phone.

Receive instant alerts for trick-or-treaters or package deliveries. Pair with Alexa for hands-free convenience and enjoy peace of mind with the Ring Protect Plan, which records and stores your videos. A must-have for a safe, festive season!

Haunted Smartwatches

It's Halloween, and Apple Watch users are getting a bit of a scare. "Ghostly" taps, swipes and calls are happening on smartwatches without physical touch. It's either their late great-granny trying to say hello from the afterlife, or…it's a glitch. Apple is leaning toward the latter. MacRumors shared an internal memo stating, "Some customers may report their Apple Watch Series 9 or Apple Watch Ultra 2 is experiencing false touches on their display." Sometimes, these phantom activities prevent users from entering their passcode. If you experience "ghost" glitches on your smartwatch, Apple recommends restarting your device and keeping your software up-to-date.

8 Essential Cybersecurity Tech Tips to Help You Stay Protected

Cybersecurity Awareness Month is observed every October, a time to focus on protecting your digital life. In 2024, human error contributed to 55% of data breaches, highlighting the critical need for cybersecurity education. With over 75% of targeted cyberattacks starting with phishing emails, implementing strong passwords, multi-factor authentications, and regular software updates are essential steps to safeguard personal and organizational data. These measures not only reduce the risk of cyber threats but also promote a culture of security awareness and resilience.

1. **Use Strong Passwords and a Password Manager:**
   - Create complex passwords using a mix of upper and lower case letters, numbers, and special characters.
   - Avoid using the same password for multiple accounts.
   - Use the password manager provided by your company to securely store and manage your passwords.
2. **Enable Multi-Factor Authentication (MFA):**
   - Add an extra layer to your business security by enabling MFA on all employee accounts. This typically involves receiving a code on your phone or email that you must enter in addition to your password.
3. **Keep Software Updated:**
   - Regularly update your operating system, browsers, and other software to protect against the latest threats. Many updates include security patches that fix vulnerabilities.
4. **Be Cautious with Links and Attachments:**
   - Avoid clicking on links or downloading attachments from unknown or suspicious emails. Phishing attacks often use these methods to steal your information.
5. **Avoid Using Public Wifi:**
   - Avoid using public Wi-Fi as they are often unsecure making it easier for hackers to intercept your data. Use a personal hotspot as your phone will create a secure Wi-Fi network that is more secure and private.
6. **Secure Your Home Network:**
   - Change the default password on your router and use a strong, unique password.
   - Enable network encryption (WPA3 is the latest standard) to protect your Wi-Fi network.
   - Create a separate wireless network when working from home to secure your home network.
7. **Regularly Back Up Your Data:**
   - Ensure you have regular backups of important data. Use cloud storage to safeguard against data loss.
8. **Educate Yourself and Others:**
   - Stay informed about the latest cybersecurity threats and best practices. Share this knowledge with family, friends, and colleagues to help them stay safe online.

Want More Insider Information in the World of IT?

Follow us on our social media pages for more IT content, latest tech trends, company updates, tech tips and more. Connect with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532