the NetWork

LeadingIT

Chicagoland CybersecurITy Support

July 2024

The Hidden Pitfalls of Cyber Insurance: How Incorrect Information Can Void Your Coverage

Understanding and Mitigating Third-Party Risks: Ensuring the Security of External Partnerships

Insights and Strategies for Combating Top Cyber Threats to Local Governments

5 Things to Do Today to Secure Your Hybrid Work Environment

LeadingIT Core Values Victor of the Month

GoLeadingIT.com ☎ 815-788-6041 in @goleadingit

The Hidden Pitfalls of Cyber Insurance:

How Incorrect Information Can Void Your Coverage

Cyberattacks have become a crucial risk for any company, no matter its size: the global average cost of a data breach crested a record $4.35 million in 2023. As cyber threats proliferate, cyber insurance continues to grow in popularity as a way to help reduce the financial fallout stemming from data breaches, network outages, and other cyber losses.

But cyber insurance policies can be tricky and, in fact, they come with hidden pitfalls that can leave your business unprotected despite having a policy.

The dangers of misinformation and a lack of understanding of cyber insurance applications will be tackled in this article, alongside how LeadingIT can help you overcome this important step.

The Importance of Understanding the Fine Print

After a May 2021 data breach at a Canadian social service agency – involving the online publication of confidential reports to Facebook – the agency sought approximately $75 million in damages but was denied cyber insurance coverage because of a policy exclusion for the display of breached data on websites.

Larger corporations might have the financial means to absorb the cost of such a data breach. However, many businesses would be bankrupted by such a loss, which is why it's important to understand the fine print.

Cyber insurance policies are seldom the 'set-it-and-forget-it' products they're portrayed as in ads. They are legal documents filled with exclusions, limitations, and specific requirements. In addition to the long list of coverage features that can be bought as separate add-ons, there are a number of specific details that can be critical to the policy journey. Here are some of them:

- **Coverage Exclusions:** Cyber insurance policies typically exclude certain types of losses, such as cyberattacks caused by employee negligence or acts of war. Make sure you understand what is and is not covered by your policy.
- **Security Requirements:** Many cyber insurance policies require businesses to implement specific security controls, such as firewalls, intrusion detection systems, and data encryption. Failure to meet these requirements could result in a denied claim.
- **Data Breach Notification:** Most policies require businesses to notify the insurer promptly in the event of a cyberattack. Failure to do so could jeopardize your coverage.

Continue reading on page 7

Pictured on the cover: Kelly, Mark, Mallory

Understanding and Mitigating Third-Party Risks:

Ensuring the Security of External Partnerships

Imagine shaking hands with a potential business partner, only to realize later they have a nasty case of digital plague. That's the hidden danger of third-party risk: seemingly innocuous partnerships can introduce major security headaches for your organization and, more importantly, your clients.

Companies use third-party vendors to provide anything from cloud storage to social media advertising campaigns. This outsourcing brings many benefits, yet it creates new security risks. According to a 2024 survey, 61% of companies suffered a third-party data breach or a cybersecurity incident in the past year. These incidents lead to the compromise of valuable data, disruption in operations, and reputational damage.

Just like fortifying your own cybersecurity, there are steps you can take to mitigate these risks. In this article, we'll examine how bad actors infiltrate your networks through third-party contractors and how it's possible to discover and reduce third-party risks.

The Importance of Identifying Third-Party Risks

Third-party breaches can expose sensitive data, disrupt operations, and damage your reputation. In a worst-case scenario, a successful attack on a vulnerable third-party vendor can provide a backdoor into your own network, compromising your data and putting your clients at risk.

Here are some of the common third-party risks to consider:

- **Data Breaches:** Third-party vendors may have access to your sensitive data, such as customer information or financial records. If their security measures are inadequate, this data could be compromised in a cyberattack.
- **Cybersecurity Weaknesses:** Inadequate security practices at a third-party vendor can create vulnerabilities in your own security posture. Outdated software, weak password management, and a lack of employee training can all leave your data and systems exposed.
- **Supply Chain Disruptions:** A cyberattack on a critical third-party vendor can disrupt their operations and impact your ability to deliver services to your clients.
- **Regulatory Compliance Issues:** Your organization may be held responsible for complying with data privacy regulations, even if a breach occurs at a third-party vendor.

Implementing Security Measures to Mitigate Third-Party Risks

Identifying and understanding potential risks is the first step toward effective mitigation. Here are some key strategies to implement:

- **Vendor Risk Assessment:** Before engaging with a third-party vendor, conduct a thorough risk assessment to evaluate their security posture. This should include assessing their security policies, procedures, and incident response plans.
- **Contractual Obligations:** Include strict security clauses in your contracts with third-party vendors. These clauses should outline their security responsibilities, data breach notification requirements, and potential consequences for non-compliance.

Continue reading on page 7

Insights and Strategies for Combating Top Cyber Threats to Local Governments

In recent years, cyberattacks targeting government bodies have surged drastically, with a staggering 95% increase since the second half of 2022. This trend should be sending alarm bells to local governments that might have less than optimal cyber security measures in place.

Here are a few of the biggest threats facing local governments today:

Legacy System Vulnerabilities

The Problem: One of the biggest challenges faced by local governments is the presence of legacy systems, which are often outdated and vulnerable to cyber threats. These systems lack the robust security features found in modern IT infrastructure, making them easy targets for cybercriminals.

Proposed Solution: Upgrading to secure, modernized systems is the best way to mitigate the risk of breaches and protect sensitive government data.

Phishing and Social Engineering

The Problem: Phishing attempts remain a prevalent threat to local governments, exploiting human vulnerabilities to gain unauthorized access to sensitive data. One of the most common phishing attempts is through business email compromise (BEC) to deceive employees and manipulate them into divulging confidential information or downloading malicious software.

Proposed Solution: Employee training and awareness programs are essential for educating staff about the dangers of phishing and enhancing their ability to identify and report suspicious emails.

Compliance Requirements

The Problem: Local governments must adhere to strict compliance regulations, such as HIPAA, GDPR, and PCI DSS, to ensure the security and privacy of citizen data. Failure to comply with these regulations can result in penalties and reputational damage.

Proposed Solution: Implementing strong cybersecurity solutions and regularly auditing systems for compliance are essential for not only staying compliant but also keeping sensitive information locked down.

Continue reading on page 6

5 Things to Do Today to Secure Your Hybrid Work Environment

1
Multi-Factor Authentication (MFA)

Think of MFA as a double-lock system for your digital assets. Besides a password, it requires an additional verification step, like a code sent to a mobile device. This added layer of security makes it significantly harder for hackers to access your accounts, even if they manage to steal your passwords.

2
Virtual Private Network (VPN)

Imagine a VPN as a secure tunnel that connects your remote employees to your company's network. When using a VPN, all data transmitted between the employee's device and your network is encrypted, making it difficult for hackers to intercept sensitive information. This is crucial for maintaining privacy and security when employees work from various locations.

3
Endpoint Protection

Every device that connects to your network – laptops, smartphones, tablets – is a potential entry point for cyber threats. Endpoint protection involves using software to secure these devices from malware, viruses, and other cyber attacks. This software can detect and neutralize threats before they cause harm, ensuring that all endpoints accessing your network are secure.

4
Security Training

One of the most effective ways to protect your business is to educate your employees about cybersecurity. Regular security training can help employees recognize phishing attempts, use strong passwords, and follow best practices for data protection. By making cybersecurity solutions a part of your company culture, you empower your team to act as the first line of defense against cyber threats.

5
Remote Work Policies

Establishing clear remote work policies is vital for maintaining security. These policies should outline the acceptable use of company devices, guidelines for accessing the network remotely, and procedures for reporting security incidents. Ensure that all employees are aware of these policies and understand the importance of adhering to them.

Combating Top Cyber Threats to Local Governments

continued from pg 4...

Ransomware Breeding Farms

The Problem: Ransomware attacks pose a significant threat to local governments. Think of ransomware like a termite infestation, infiltrating and damaging critical infrastructure. But, in this case, it doesn't take days, weeks, or months to cause catastrophic damage – it can be a matter of minutes or seconds.

Proposed Solution: Local governments should be implementing proactive ransomware prevention measures like regular backups, network segmentation, and employee training.

Supply Chain Management

The Problem: Local governments face unique challenges in managing their supply chains, including complex procurement processes, reliance on third-party vendors, and limited visibility into supply chain operations. These factors increase the risk of supply chain-related cyber attacks, such as ransomware infiltrating through vendor networks or compromised supply chain software.

Proposed Solution: To address these vulnerabilities, local governments can leverage industry best practices such as the Supply Chain Operations Reference (SCOR), the Council of Supply Chain Management Professionals (CSCMP), the Supply Chain Security Management Systems (ISO 28000), and the Cybersecurity Assurance Framework (CSAF).

The Hidden Pitfalls of Cyber Insurance continued from pg 2...

Why Accuracy Matters: The Risk of Policy Voidance

Applying for cyber insurance can be a complex process. When applying, the policyholder commits to answering extensive questions about the condition of their cybersecurity posture: what safeguards are in place, prior breaches, and incident response plans, for instance.

If your business makes an incorrect or false representation at the time you apply for a policy, an insurer may well have good reason to reject a claim or even rescind the policy itself. In the event of a breach, your business could potentially be open to a massive loss.

How LeadingIT Can Help You Navigate the Risk

LeadingIT can be your trusted partner in navigating the complexities of cyber insurance and ensuring you provide accurate information during the application process. Here's how we can help:

- **Cybersecurity Assessment:** We can conduct a comprehensive assessment of your cybersecurity posture to identify any vulnerabilities and ensure your security controls meet industry best practices.
- **Gap Analysis:** We can analyze your existing cyber insurance policy and identify any gaps in coverage based on your specific needs.
- **Policy Review:** We can review your cyber insurance policy and help you understand the fine print, including exclusions, limitations, and security requirements.
- **Application Assistance:** We can work with you to gather the necessary information for your cyber insurance application and ensure you provide accurate and complete information.

Cyber insurance is an incredible tool for mitigating the financial losses from a cyber attack. However, inaccurate information during the application process can render your policy useless. By understanding the fine print and working with a trusted partner like LeadingIT, you can avoid these pitfalls and ensure you have the cyber insurance coverage you need to protect your business.

Understanding and Mitigating Third-Party Risks continued from pg 3...

- **Access Controls:** Limit access to sensitive data only to authorized personnel at third-party vendors. Implement data encryption and multi-factor authentication protocols to strengthen access control measures.
- **Continuous Monitoring:** Don't rely on a one-time assessment. Monitor your third-party vendors on an ongoing basis to stay informed of any changes in their security posture.
- **Security Awareness Training:** Promote a culture of cybersecurity within your organization and provide your employees with training on how to identify and avoid risks associated with third-party vendors.

A Real-World Example: Microsoft

The attack: Microsoft is a common subject of cyberattacks that take advantage of the implicit trust most security tools place in anything signed by the tech giant.

The method: In March 2021, 30,000 global organizations had their on-premises Microsoft Exchange Servers breached by a group known as HAFNIUM. Employee email accounts were accessed and malware was installed for long-term access.

The impact: In less than a year, 38 million records were breached through Microsoft Power Apps. This vulnerability uncovered COVID-19 testing, tracing, and vaccination records as well as employee data for such organizations as Ford Motor Company, American Airlines, and the New York Metropolitan Transportation Authority.

Mitigate Risk, Build Trust

You don't have to stop using third-party vendors altogether. If you plan ahead and reduce third-party threats, it will help to protect your sensitive data, keep your business up and running, and maintain the trust of your clients. With these steps, your business will survive with secure partners in tandem with a cyber-landscape rife with bad actors.

LeadingIT Core Values Victor of the Month

Scott Sola - Level 2 Technician

We are thrilled to shine the spotlight on Level 2 Technician Scott Sola, Our latest Values Victor for embodying the principle of being Humbly Confident.

Scott truly exemplifies the ability to 'make it happen.' His commitment to continual learning allows him to adeptly navigate the ever-evolving challenges in our field, solving problems with a confident and knowledgeable approach.

What sets Scott apart is his humility; he's never hesitant to seek help when needed, ensuring that every solution is not just quick but also correct and well-informed.

Congratulations, Scott, on your well-deserved recognition and for being a role model in balancing confidence with humility.

LEADINGIT VALUES:

- We Are Driven
- We Chase Excellence
- We Are Humbly Confident
- We Are Accountable
- We Have A Positive/ Fun Mindset

LeadingIT

$1000 REFERRAL PROGRAM

WE LOVE REFERRALS!

Do you know an organization that needs fast + friendly IT and cybersecurity support?

If they sign up, you'll receive $1000!

LEARN MORE

GOLEADINGIT.COM/REFER

815-788-6041

Continue reading on our blog at goleadingit.com/blog

LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

WE ARE CELEBRATING!

Birthdays

Mark Seplowin - July 9th
Michael Seplowin - July 9th
Christopher Hansen - July 9th

Anniversaries

Matthew McMullan - 7/5/2023
Daniel Rabenold - 7/11/2023
Lori Yarnall - 7/24/2023