

CYBER ADVISOR

MORE THAN A NEWSLETTER

January 2024

Data-Tech Acquires Network Integrity Support

We're expanding! Data-Tech is thrilled to announce that we have successfully acquired Network Integrity Support, a leading Managed Service Provider (MSP) based in Brooksville, Florida. This strategic move is a significant step forward in our commitment to enhancing our services and extending our reach. With Network Integrity Support joining the Data-Tech family, we're combining forces to deliver unparalleled IT solutions, innovative technologies, and exceptional support to our valued clients. Together, we look forward to providing even more robust, secure, and efficient services, reaffirming our dedication to excellence in the ever-evolving tech landscape.



Pictured Left to Right: Data-Tech Owner, Chris Lietz, with Network Integrity Support Owner, Carl Brown.

New Year, New IT

**Start
the New Year
with a reliable
IT Partner!**

FREE Consultation

4 Reasons Companies Are Choosing Managed Service Providers in 2024

1

Cost Efficiency

MSPs often offer cost-effective solutions compared to hiring and maintaining an in-house IT team.

2

Scalability & Flexibility

MSPs offer scalable solutions that can adapt to a company's changing needs.

3

Specialized Expertise

MSPs specialize in providing IT services, offering expertise across various technologies, security protocols, and industry standards.

4

Focus on Core Business

Outsourcing IT services to MSPs enables companies to focus more on their core business operations and strategic initiatives.

Cyber Insurance & IT Providers

**STRONG
CYBER LIABILITY
INSURANCE
STARTS
WITH A RELIABLE
IT PROVIDER.**

Securing Cyber Liability Insurance is a vital step in safeguarding your business against unpredictable cyber threats, but the foundation for a robust defense begins with partnering with a trusted IT provider. These experts play a crucial role in not only assessing the unique cybersecurity needs of your business but also in implementing proactive measures to fortify your digital infrastructure. By collaborating with an IT provider before diving into the realm of Cyber Liability Insurance, you ensure that your coverage is tailored precisely to your vulnerabilities and potential risks. Their expertise not only enhances the insurability of your business but also ensures a rapid and effective response in the unfortunate event of a cyber incident. It's the

synergy between IT specialists and insurance that forms a comprehensive shield, providing peace of mind in an era where digital resilience is synonymous with business success.

Partnering with an experienced IT provider is a strategic move that can significantly impact the success of your Cyber Liability Insurance claims. By collaborating closely with IT professionals, businesses can proactively address vulnerabilities, implement robust cybersecurity measures, and ensure compliance with industry standards. This diligent approach not only minimizes the risk of denials but also maximizes the likelihood of successful claims payouts. IT providers play a pivotal role in establishing a comprehensive risk management strategy, documenting preventive measures, and swiftly responding to incidents, all while presenting insurers with a clear and well-documented case. This collaboration not only strengthens your overall cybersecurity posture but also enhances the credibility and transparency of your insurance claims, ultimately contributing to a smoother and more favorable claims process.

**MINIMIZE
DENIALS
MAXIMIZE
PAYOUTS
PARTNER
WITH DATA-TECH**

CYBER INSURANCE BUYERS CHECKLIST





BEWARE OF PHISHING EMAILS

Phishing emails represent a persistent cybersecurity threat, and employees can easily fall prey to the deceptive tactics employed by hackers. These malicious actors often craft emails that convincingly imitate legitimate communications from trusted sources, using tactics like spear-phishing, where messages are tailored to specific individuals within an organization.

PHISHING EMAIL EXAMPLE:

-----Original Message-----

From: Kaylee Lietz <iwalewaapati@gmail.com>

Sent: Tuesday, January 16, 2024 12:03 PM

To: Chris Lietz <chrislietz@datatechitp.com>

Subject: Change banking information

Hi Christopher

I want to change my banking information before the next payroll is completed. What details do you need?

Regards,

Kaylee Lietz

Service Operations Manager

Data-Tech, Specialized in Managed IT Security

A phishing email may contain urgent requests, alarming messages, or seemingly harmless prompts that encourage recipients to click on malicious links or provide sensitive information like the example above. Here's a few tips on how to detect a phishing email:

- The message is sent from a public email domain
- The domain name is misspelt
- The email is poorly written
- It is sent with suspicious attachments or links
- The message creates a sense of urgency

If you come across a phishing email, do not reply to the email or click on any links or attachments. It's best to delete the email right away and report it. Building a robust cybersecurity awareness program and providing regular training to employees are critical in fortifying the human firewall against these sophisticated phishing attempts. Please reach out to Data-Tech if you are need of any of these services.



KEEPING UP WITH DATA-TECH

DATA-TECH ACQUIRES NETWORK INTEGRITY SUPPORT



INTERNAL DATA-TECH EVENTS

