tenhats

Cybersecurity

Why Is It Important?

Cybersecurity is a critical component of any organization's operations. Global cybercrime will be responsible for an estimated $10.5 trillion of damages by 2025[1]. With these increasing threats, implementing a robust cybersecurity strategy is essential.

Many organizations make the mistake of focusing solely on implementing firewalls and antivirus software to protect their data and networks. However, these basic tools, while helpful, fall short of the requirements to protect from ever-evolving cyber threats.

Without an effective system, organizations risk losing valuable data, suffering financial losses, and damaging their reputation. Therefore, organizations must implement a truly robust cybersecurity system to protect their data and networks from malicious actors.

This paper will outline a robust cybersecurity plan and how TenHats helps its clients create a custom, proactive strategy from start to finish.

"There's no other IT firm that can do the level of work we do for large enterprises."

– Brian Strong, CEO

[1]https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

How You Should Approach Cybersecurity

"Our services are designed from the ground up to be reliable and secure to meet the needs of your company."
– Aaron Sherrill, CTO

Business leaders often look at cybersecurity as an IT problem as if it were akin to installing a Wi-Fi router. Instead, they should look at cybersecurity from a business point of view by considering a security incident's potential financial and reputational impact. The cost of a security incident goes beyond the money spent on recovering from the breach itself. It also includes the impact on the company's reputation, lost revenue, and potential legal and regulatory fines.

From a reputation perspective, business leaders must recognize that a security incident can significantly impact consumer trust and brand image. A crisis communication plan that includes transparency with customers and stakeholders about the incident serves a vital function in reducing damages.

Cybersecurity planning also helps build loyalty and profitability. A comprehensive cybersecurity strategy will strengthen customer trust, increasing sales and revenue. By taking a comprehensive approach to cybersecurity, organizations will benefit across all channels.

Challenges Businesses Face

Business leaders face a variety of challenges as they consider cybersecurity. One of the main challenges is a lack of understanding of the risks and the constantly evolving threat landscape. This makes it difficult to develop effective strategies to address the risks and to keep up with the latest developments. Business leaders may also face budget constraints and limited resources, creating barriers to implementing security technologies and practices.

A cybersecurity plan should also ensure the organization runs smoothly and achieves its goals while keeping data secure. Finding the right balance between aligning security efforts with the organization's overall business objectives takes careful planning.

Compliance and regulations are also challenging as business leaders must ensure their organization complies with relevant laws and regulations such as HIPAA, PCI-DSS, and GDPR.

Actuarial calculations and measuring the ROI of cybersecurity efforts can feel more complicated than other areas of business insurance. One advantage of a managed security solution is more data for business leaders to make informed decisions about their cybersecurity investments.

The TenHats Way

A comprehensive cybersecurity strategy includes risk management, security awareness training, and robust security policies. This requires significant expertise in the field of cybersecurity, and many companies do not have the necessary skills and knowledge to provide these services well. TenHats' seasoned experts can help organizations build a comprehensive cybersecurity strategy to protect their data and networks from malicious actors. Lets discuss how TenHats can provide support to these organizations.

Risk Assessment

Risk assessment in cybersecurity is the process of identifying, evaluating, and prioritizing potential risks to an organization's information assets and infrastructure in order to develop and implement appropriate security measures to mitigate or prevent those risks.

This involves identifying assets and potential threats and vulnerabilities, assessing the likelihood and impact of those threats and vulnerabilities, and prioritizing the risks to determine which ones need to be addressed first.

TenHats can conduct a thorough risk assessment to identify potential vulnerabilities and threats to an organization's information assets and infrastructure. The assessment will inform the development of security policies tailored to the organization's needs.

We Put on All the Hats **You Don't Want to Wear**

- **Manged IT Resources**
- **Helpdesk**
- **Cybersecurity**
- **Private & Public Cloud Hosting**
- **Backup & Disaster Recovery**
- **IT Procurement**

tenhats

The TenHats Way

Policy Development

Based on the risk assessment, TenHats can help organizations develop security policies addressing identified vulnerabilities and threats. This includes creating policies for incident response, data backup, password management, access controls, network security, and more.

TenHats will involve all relevant stakeholders in the policy development process to ensure that the policies are comprehensive, effective, and aligned with the organization's culture and operations. TenHats will regularly review and update the changing threat landscape to ensure they remain effective.

Implementation & Enforcement

TenHats can assist organizations in implementing and enforcing their security policies. This can include configuring security settings on network devices, providing employee training, and monitoring compliance with the procedures.

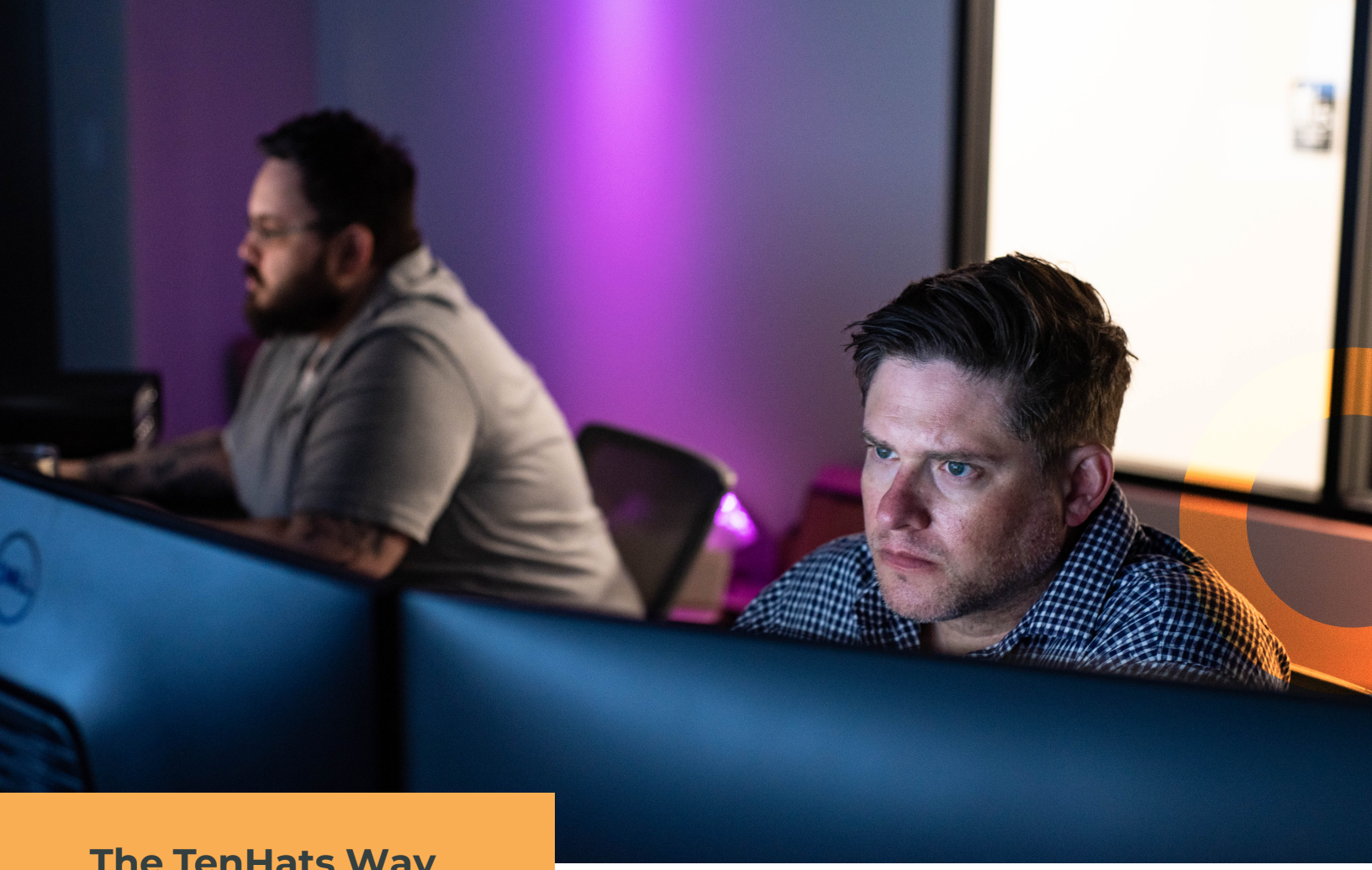
Regular Review & Updates

TenHats can help organizations review and update their security policies on a regular basis to ensure they remain relevant and effective in addressing the latest threats and vulnerabilities. TenHats can also assist in monitoring and reviewing the organization's security posture to detect any threats and vulnerabilities. Regular reviews and updates are important for organizations to ensure that their cybersecurity measures are effective and up-to-date against the evolving threat landscape.

We Put on All the Hats **You Don't Want to Wear**

- **Microsoft Licensing**
- **Internet Service Consulting**
- **Consulting Services**
- **Colocation**
- **Infrastructure as a Service**
- **Network Infrastructure**

tenhats



The TenHats Way

Managed Security Services

Cybersecurity is a three-part marriage of people, process, and technology. TenHats can also assist organizations with the technology portion by providing managed security services to offload that burden from your organization.

Security tools often require teams of people to properly manage, however TenHats has gone through the process of selecting best-in-class security tools to offer and has the expertise to properly configure and manage these tools. Tools include items such as endpoint detection and response, security information and event management, and vulnerability management.

Security Awareness Training

Security awareness training is a process of educating employees, contractors, and other stakeholders about the importance of cybersecurity and the role they play in protecting an organization's information assets and infrastructure. The training ensures that everyone with access to an organization's systems and data understands the risks they face and the steps they can take to mitigate them.

Security awareness training typically includes information on topics such as password security, phishing, social engineering, and safe browsing practices. It may also include training on the specific security policies and procedures of the organization, as well as guidance on how to report suspicious activity.

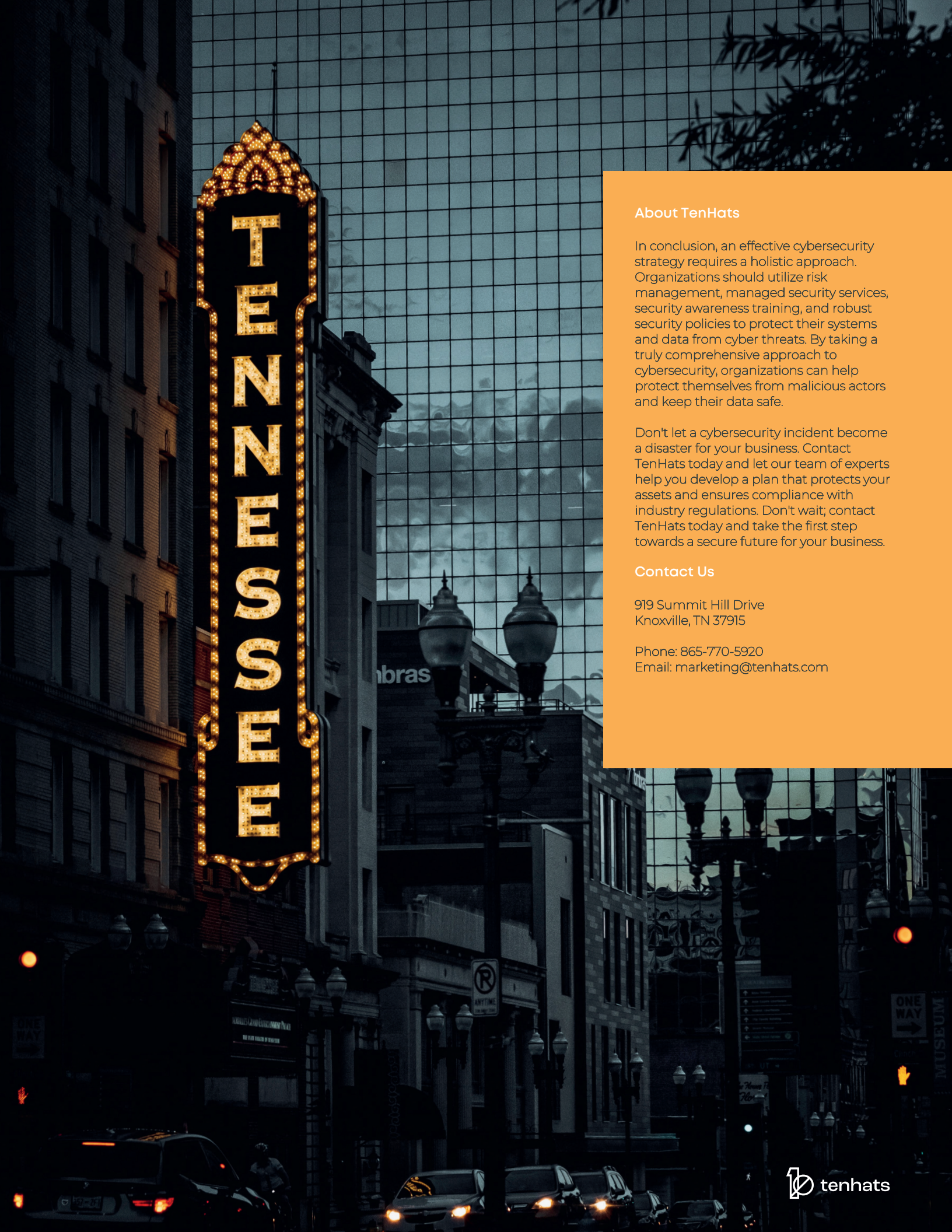
Training, typically given by a cybersecurity expert or service, should be regularly provided and updated as the threat landscape evolves. Many compliance certifications require regular training, and TenHats can help you meet those goals.

Compliance

TenHats helps organizations meet regulations such as:

- HIPAA
- PCI-DSS
- GDPR

They can also help organizations meet industry or regulatory compliance requirements related to the information security by providing support and documentation for audits and compliance reviews.



About TenHats

In conclusion, an effective cybersecurity strategy requires a holistic approach. Organizations should utilize risk management, managed security services, security awareness training, and robust security policies to protect their systems and data from cyber threats. By taking a truly comprehensive approach to cybersecurity, organizations can help protect themselves from malicious actors and keep their data safe.

Don't let a cybersecurity incident become a disaster for your business. Contact TenHats today and let our team of experts help you develop a plan that protects your assets and ensures compliance with industry regulations. Don't wait; contact TenHats today and take the first step towards a secure future for your business.

Contact Us

919 Summit Hill Drive
Knoxville, TN 37915

Phone: 865-770-5920
Email: marketing@tenhats.com

tenhats