WHAT WE DO…

We offer a comprehensive range of risk assessment/ management services, cyber audits, and policies & procedures drafting and review. Our expertise includes employee, customer, and vendor training, as well as online, space, and physical security. We specialize in database management, intrusion monitoring/detection, incident responses, and forensic management. With system testing/hardening, HMI development, and SCADA security, we ensure robust protection. Additional services include off-site back-up & recovery, robotic surveillance, GSaaS (Ground Support as a Service), and more. Rely on our tried, true, state-of-the-art tools and techniques to safeguard your investments effectively.

Houdini Security Global

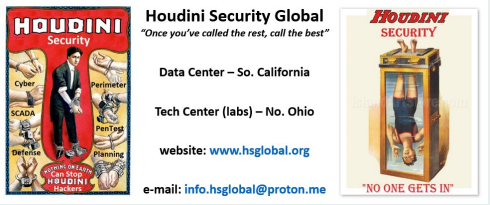
"Once you've called the rest, call the best"

Data Center – So. California

Tech Center (labs) – No. Ohio

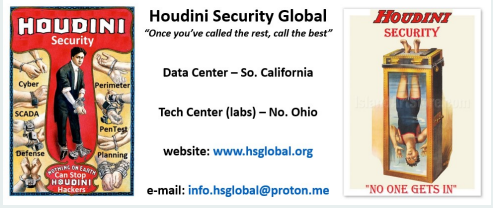
website: www.hsglobal.org

e-mail: info.hsglobal@proton.me



#5- Online Cyber Training (for employees, customers and vendors)

Online cyber training for employees, customers, and vendors is a comprehensive educational program focused on enhancing awareness of cybersecurity threats and best practices. Tailored to various roles, it covers topics such as phishing detection, secure password creation, data protection, and adherence to regulatory standards. This training is pivotal for safeguarding information, reinforcing a security-conscious culture, and minimizing the risk of cyber-attacks within an organization and its extended network.



Offering Cyber/IT/SCADA/ IoT/Satellite/Mobile Phone/ Physical security products & services

Training at a glance...

Online cyber training, targeted at employees, customers, and vendors, serves as an essential component of a modern organization's security posture. By promoting a comprehensive understanding of cybersecurity threats, best practices, and protective measures, it helps to foster a culture that prioritizes security and confidentiality. Here's a detailed description of what this training accomplishes for a company:

THERE'S MORE...

FOR EMPLOYEES

- **Enhancing Awareness:** By educating employees about the myriad of cybersecurity risks and the potential consequences of a breach, they become more vigilant. Training helps them recognize phishing emails, use strong passwords, and apply secure data handling techniques.
- **Compliance with Regulations:** Many industries are bound by legal requirements to ensure the privacy and security of data. Tailored cyber training ensures employees understand and adhere to these regulations, reducing legal liabilities.
- **Reducing Human Error:** Since human error is one of the leading causes of security breaches, focused training reduces this risk by equipping staff with the knowledge and tools needed to identify and respond to threats.
- **Building a Security Culture:** Regular cyber training sessions contribute to a security -first organizational culture where employees feel responsible for safeguarding information.

FOR CUSTOMERS

- **Enhancing Trust:** When customers know that a company provides cybersecurity education, it enhances their trust in the brand. This is especially important in sectors dealing with sensitive information like finance, healthcare, or e-commerce.
- **Empowering Customers:** Offering cyber training empowers customers to protect their data, making them less susceptible to common cyber threats like phishing and identity theft.
- **Improving Customer Experience:** Educated customers are more confident in using online services securely, which enhances their overall experience and satisfaction with the company's products or services.

And Finally.....

FOR VENDORS

- **Ensuring Secure Collaboration:** Vendors often have access to a company's internal data or systems. Training them in cybersecurity best practices ensures that they understand their responsibilities and maintain security standards.
- **Aligning Security Protocols:** By extending training to vendors, companies can ensure alignment in security practices across the supply chain, minimizing vulnerabilities that might be exploited.
- **Strengthening Relationships:** Collaborative training initiatives help foster a sense of partnership and trust between the company and its vendors, contributing to more robust and productive relationships.

TYPES OF TRAINING

- **General Cybersecurity Awareness Training:** These modules cover the basics of cybersecurity, including phishing detection, password management, and general internet safety.
- **Role-Specific Training:** This targets specific roles within the company, such as IT staff, management, or customer service representatives, providing tailored insights based on their unique responsibilities.
- **Simulation Exercises:** These are hands-on experiences that simulate real-world cyber attacks, allowing participants to practice their response in a controlled environment.
- **Compliance Training:** This focuses on the legal and regulatory requirements specific to an industry or jurisdiction.

BENEFITS TO THE COMPANY

- **Risk Mitigation:** Comprehensive cyber training reduces the risks associated with human error, external threats, and regulatory non-compliance.
- **Brand Protection:** A company that can demonstrate robust cybersecurity practices and education programs is likely to enjoy a positive reputation, building customer loyalty and competitive advantage.
- **Financial Savings:** Preventing breaches through education can save substantial costs related to legal compliance, data recovery, and brand damage.
- **Agile Response:** Well-trained staff can respond more quickly and effectively to a cyber incident, minimizing potential damage.
- **Vendor Reliability:** Ensuring that vendors are well-trained in cybersecurity helps maintain the integrity of the supply chain, reducing associated risks.