CYBERSECURITY TRAINING

Organizational Evaluation Checklist for Preferred Practices in Cybersecurity

Are you up to speed with preferred practices?

○ STRONG PASSWORD POLICIES

- Require the use of complex passwords with a mix of letters, numbers, and special characters.
- Encourage regular password changes and avoid reusing passwords across different sites.

○ MULTIFACTOR AUTHENTICATION (MFA)

- Add an extra layer of security by requiring two or more verification methods.
- Use MFA for all critical systems and sensitive data access.

○ REGULAR SOFTWARE AND FIRMWARE UPDATES

- Keep all software, including operating systems and applications, up to date.
- Apply security patches promptly to protect against vulnerabilities.

○ EMPLOYEE TRAINING AND AWARENESS

- Conduct regular cybersecurity training sessions.
- Educate stakeholders on how to recognize phishing attempts and other common cyberthreats.

○ DATA ENCRYPTION

- Encrypt sensitive data both in transit and at rest.
- Use strong encryption protocols to protect data from unauthorized access.

○ DATA BACKUPS

- Perform regular backups of critical data.
- Store backups securely and test them periodically to ensure data integrity.

○ NETWORK SECURITY MEASURES

- Implement firewalls, intrusion detection systems, and intrusion prevention systems.
- Segment networks to limit the spread of potential breaches.

○ INCIDENT RESPONSE PLAN

- Develop and maintain a comprehensive cyber incident response plan.
- Conduct regular drills to ensure readiness in case of a cyber incident.

○ ACCESS CONTROL

- Implement the principle of least privilege, granting users only the access they need.
- Regularly review and update access permissions.

CYBERSECURITY TRAINING

Organizational Evaluation Checklist for Preferred Practices in Cybersecurity

Cyber Risk Management Culture

1. THE RIGHT MINDSET

- Foster a mindset where cybersecurity is seen as a business imperative, not just an IT issue.
- Encourage stakeholders to think critically about cyber risks and take proactive measures to thwart potential cyberattacks.

2. THE WHOLE PICTURE

- Adopt a holistic approach to risk assessment, considering both internal and external factors.
- Stay informed about emerging threats and adapt defenses accordingly.

3. OPEN COMMUNICATION

- Break down silos and encourage seamless communication about cyber risks across the organization.
- Create a culture where stakeholders feel comfortable reporting potential threats. Foster a no-blame culture.

4. CONTINUOUS LEARNING AND IMPROVEMENT

- Regularly update training programs to reflect the latest cyberthreats and best practices for responding to them.
- Encourage a culture of continuous improvement and learning from past incidents.

5. LEADERSHIP INVOLVEMENT

- Ensure that leadership is actively involved in cybersecurity initiatives.
- Promote a top-down approach where leaders set the tone for a strong cyber risk management culture.

CYBERSECURITY TRAINING

Organizational Evaluation Checklist for Preferred Practices in Cybersecurity

DID YOU DISCOVER ANY "BREACHES?"

Proceed with designing and implementing improvements by following the 8 Pillars of Cyber Risk Culture Awareness:

1. **Outline your aspirations:** Understand your current cybersecurity culture, and set goals and aspirations for what you want it to be in the future.
2. **Secure support and investment:** Seek support from parts of the organization that already have capabilities to develop and implement goals, policies, and growth across all functions.
3. **Explore and experiment:** Identify the gaps in your current capabilities and explore new options for cyber risk management, cyber risk training, and cyber risk awareness.
4. **Prioritize and implement:** Focus on implementing the use cases that can have the most impact on driving a stronger cybersecurity culture and reducing risk.
5. **Collect and measure what matters:** An upfront focus on data, its quality, and broad stakeholder safety can help you get the best out of your mitigation efforts.
6. **Be mindful of new risks:** Consider what the new cyber risk management preferred practices, tools, and technologies can and can't do, and the risks that come with them.
7. **Prioritize the employee change journey:** Prioritize employee well-being throughout the change process by providing the right communications, training, and recognition.
8. **Be ahead of change and open to it:** Know that technology is ever-evolving, and proactively address mindset, culture, and delivery of knowledge to focus on constant growth and change.