CYBERSECURITY FOR BUSINESS CONTINUITY

ARE YOU PREPARED FOR CYBER INCIDENTS?

11:59 can help you plan and prepare for the worst. While robust technological defenses are crucial in the face of cyberattacks, a comprehensive cybersecurity strategy extends beyond the digital realm. Organizations must consider a multifaceted approach that encompasses human factors, organizational policies, and strategic decision-making. 11:59 can support your organization by reviewing the key process and people components to help close your gaps.

HAVE YOU CONSIDERED...

- **In the digital world, how you will communicate with your employees in the event of a cyber-attack?**
- **If you had to contact every employee in your organization without using their email, how would you do it?**
- **Do you know if your board would agree to negotiate a ransomware attack?**

SCAN ME

11:59 APPROACH:

11:59 can help develop detailed incident response plans, conducting regular cybersecurity awareness training for employees, and even formulating strategies for negotiating with ransomware attackers, should the worst-case scenario occur. By addressing these non-technical aspects, organizations can significantly bolster their resilience and minimize the impact of potential cyberattacks. With our help, you can be ready for tomorrow. 11:59 Can provide planning and support in the following areas to help bolster your tech defenses.

- **Identify Key Stakeholders**
- **Assess Risks and Threats**
- **Develop Response Procedures**
- **Establish Communication Channels**
- **Test and Train**
- **Consider External Resources**

www.1159.ai hello@1159.ai

CYBERSECURITY FOR BUSINESS CONTINUITY

KEY BENEFITS OF A CYBER INCIDENT RESPONSE PLAN

Incident Response Team:

- Establish a dedicated incident response team with clearly defined roles and responsibilities.
- Provide regular training on incident response procedures and cybersecurity best practices.

Detection and Containment:

- Implement robust monitoring tools to detect suspicious activity early.
- Quickly isolate affected systems to prevent further spread of the attack.
- Disable network access to compromised systems to contain the attack.

Ransomware Response:

- Develop a clear policy on whether to negotiate with attackers, considering legal and ethical implications.
- Prioritize recovery from backups to avoid paying a ransom.
- Report the incident to law enforcement authorities.

Business Continuity Plan (BCP):

- Create a detailed BCP outlining procedures for maintaining critical business functions during and after an attack.
- Regularly test the BCP to ensure its effectiveness.

Recovery and Restoration:

- Implement procedures for recovering lost or corrupted data from backups.
- Restore affected systems and applications from backups or alternative sources.
- Implement measures to strengthen security and prevent future attacks.

Communication and Notification:

- Establish clear communication channels within your organization to keep your employees informed.
- Develop a plan for communicating with customers, partners, and other stakeholders as needed.

Post-Incident Review:

- Conduct a thorough analysis of the incident to identify root causes and lessons learned.
- Implement necessary improvements to prevent similar attacks in the future.

Regular Updates:

- Regularly review and update the response plan to reflect changes in technology, threats, and best practices.

SCAN ME

www.1159.ai hello@1159.ai