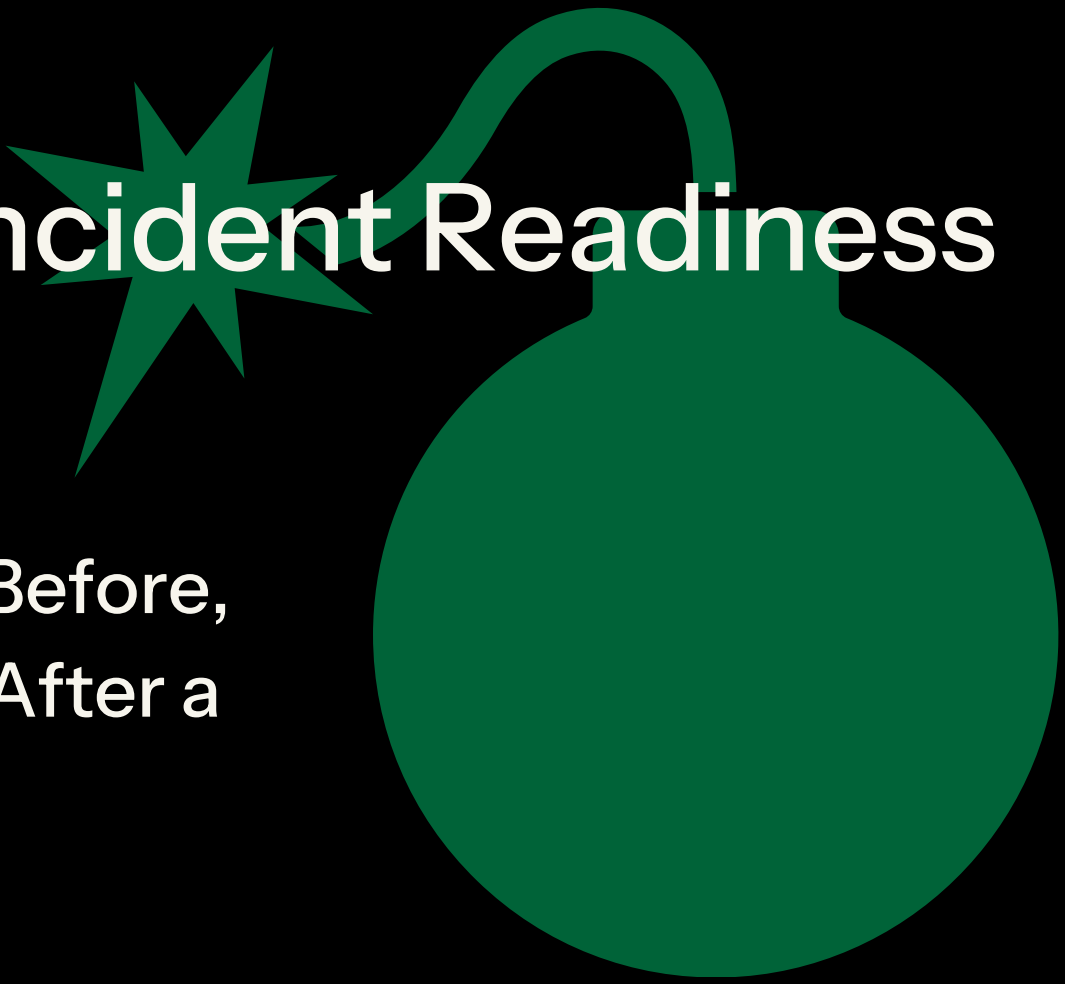
Cyber Incident Readiness

What to Do Before, During, and After a Cyber Event



A cyber incident—whether it's a data breach, ransomware attack, or unauthorized access—can cause significant financial and reputational damage for small and mid-sized businesses. Taking proactive measures before an incident occurs, knowing how to respond during a breach, and effectively recovering afterward can make all the difference in minimizing risk and ensuring business continuity.

MIS

Before: *Preparation is Key*

1. **Establish a Cyber Incident Response Team**
2. **Develop a Documented Incident Response Plan**
3. **Conduct Tabletop Exercises**
4. **Invest in Employee Cybersecurity Awareness Training**
5. **Implement Strong Cybersecurity Measures**
6. **Test and Verify Backups**
7. **Obtain Cyber Insurance Coverage**

It's never a matter of "if" a business will suffer a cyber incident, but "when." Preparing before the inevitable will reduce the risk of irreparable damage.

MIS

MIS

During: *Execute Plan*

8 Contain the Breach

9 Immediately Contact IT and Cybersecurity Experts

10 Consult with Legal Counsel

11 Notify Your Cyber Insurance Provider

After: *Strengthen Security*

12 Work with a PR or Crisis Communications Team

13 Notify Affected Parties

14 Restore Operations and Secure Systems

15 Conduct a Post-Mortem Analysis

Contact Us Today to Learn if You're Ready for a Cyber Incident

www.mis-solutions.com/discovery-call