ONSITE LOGIC

CYBERSECURE

EMPLOYEE BENEFITS SECURITY ADMINISTRATION UNITED STATES DEPARTMENT OF LABOR
CYBERSECURITY PROGRAM BEST PRACTICES
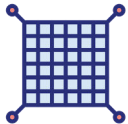
<u>Security Operations & Threat Management</u> is your business's "**cybersecurity SWAT team,**" offering a suite of powerful tools to protect your company from potential cyber-attacks.

2. Conduct prudent annual risk assessments.
3. Have a reliable annual third party audit of security controls.
12. Appropriately respond to any past cybersecurity incidents

<u>IT Infrastructure Management</u> serves as the "**night watchman**" for your business's IT infrastructure, ensuring that all doors are locked, and alarms are active.

10. Encrypt sensitive data, stored and in transit.
11. Implement strong technical controls in accordance with best security practices.
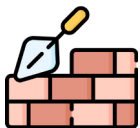
<u>BCDR</u> provides the "**last line of defense and safety net**" for your business in case of a disaster or disruption, helping you to quickly recover and get back to normal operations.

9. Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.

<u>Compliance & Risk Management</u> acts as your business's "**compliance officer,**" ensuring that you meet all necessary regulations and guidelines.

1. Have a formal, well documented cybersecurity program.
4. Clearly define and assign information security roles and responsibilities.
6. Ensure that any assets or data stored in a cloud or managed by a third party service provider are subject to appropriate security reviews and independent security assessments.

<u>Credentialing & Passwords</u> is your business's "**front-line defense**" against potential cyber threats.

<u>Employee Training & Awareness</u> is your business's "**cybersecurity foundation,**" providing comprehensive cybersecurity awareness training.

5. Have strong access control procedures.

<u>End-User Support & IT Strategy</u> acts as your business's "**IT doctor,**" providing end-user support and IT strategy for the day-to-day needs of your employees and end-users.

7. Conduct periodic cybersecurity awareness training.
8. Implement and manage a secure system development life cycle (SDLC) program.

ONSITELOGIC.COM