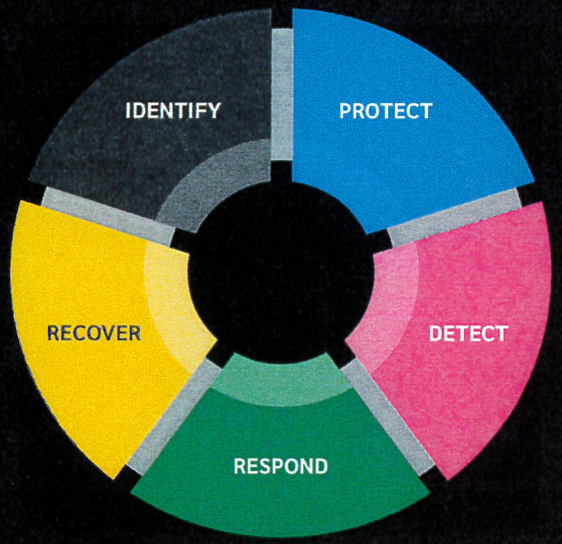
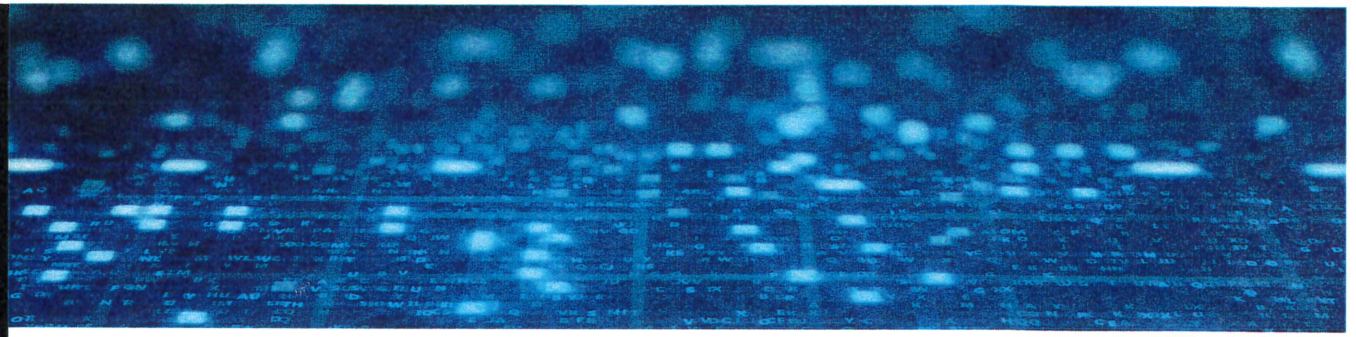
Global Cyber & Technology Practice

The National Institute of Standards and Technology (NIST) created a voluntary framework consisting of standard guidelines and best practices to address cybersecurity risks. NIST's framework was utilized to create this outline of considerations, recommendations and best practices for organizations navigating cyber risk management.





IDENTIFY

- Conduct data mapping exercise to determine how information and data, throughout their life cycles, flow through the organization, digitally and physically.
- Implement classification policy, including a determination of business impact related to most critical data and information.
- Prepare a regulatory map to determine the local, state, federal and international requirements applicable to the organization.

PROTECT

- Draft and implement privacy policies.
- Implement appropriate security controls over critical/classified data and information.
- Review and evaluate third-party vendor management programs, including:
  - Conducting vendor risk assessments.
  - Requiring vendors to protect data equivalent to how the organization protects its own data.
  - Exercising vendor audit rights to allow periodic review of vendor's cybersecurity protocols, controls and procedures.
  - Reviewing indemnification language in vendor contracts.
  - Ensuring vendors do not sell, share or utilize any data other than for the specific and limited business purpose identified in the contract.
- Create an incident response plan to address how the organization will specifically respond in the event of an incident.
- Create disaster recovery plan for each critical asset, e.g., how the data will be recovered in the event of compromise or attack.
- Create a business continuity plan in the event of attack or compromise.
- Budget for cyber insurance.

DETECT

- Monitor security controls and processes regularly for threats, vulnerabilities and risks.
- Establish routinely scheduled threat, vulnerability and risk assessments.
- Plan and budget for information security upgrades.
- Implement workforce (employee and contractors) security education, awareness and training programs, including:
  - General education program on all privacy and cybersecurity policies.
  - Specialized training programs for those handling sensitive information.
  - Recurring training campaigns, e.g., phishing and social engineering.

RESPOND

- Test all response plans.
- Ensure response plans are updated as needed.
- Coordinate response plans with vendors and third parties, including cyber insurers.

RECOVER

- Provide timely notification of incidents and/or claims to cyber insurers.
- Conduct thorough post-incident assessment to determine areas for improvement.
- Review incident response, disaster recovery and business continuity plans regularly and update as necessary.
- Ensure any necessary steps are taken to address damage to the organization's reputation.

For more information, contact cyber@lockton.com.

LOCKTON