Texas A&M Engineering Extension Service

CYBER READINESS CENTER

Cybersecurity Program Checklist

A free getting-started resource provided by the Texas A&M Engineering Extension Service Cyber Readiness Center.

For more information visit

cyberready.org

Consideration	Answers/Comments
Identify Specific Drivers Within the Organization	
Are there specific regulatory or compliance requirements around cybersecurity that apply?	
Has the organization considered their liability in the event of a breach?	
What would be the effect of prolonged downtime on critical business processes?	
How would the organization's reputation be affected by a breach?	
What can the organization do to be a good steward for protecting employees and customers?	
Does the organization maintain its own IT infrastructure or use a 3rd party?	
If using a 3rd party, what visibility does the organization have into the 3rd party's security procedures?	

Consideration	Answers/Comments
Define the Program Goals	
Meet regulatory, audit, and legal requirements.	
Identify and manage cyber risk.	
Prevent cyber attacks from occurring when possible.	
Reduce or mitigate the impact of successful cyber attacks.	
Protect critical data and business processes.	
Other goals based on your specific business model:	

Consideration	Answers/Comments
Define the Program Elements	
1. Technical Mitigations: Antivirus, patching, vulnerability scanning, email filtering, firewalls, intrusion detection.	
2. Processes and Plan: Disaster recovery, business continuity, incident response, acceptable use policy, training policies, bring your own device policies, 3rd party vendor policies, risk management.	
3. Education: Cybersecurity awareness training, news and updates about the latest trends, customized training for leaders, for IT, for those who handle sensitive data.	
4. Care and Feeding – Regular assessments and program reviews, updates to elements 1-3, making the cybersecurity program a regular agenda item in leadership meetings.	

Consideration	Answers/Comments
Identify Key Personnel	
Cybersecurity Champion	
Technical Lead	
Process/Policy Lead	
Education Lead	
Assessment Lead	

Consideration	Answers/Comments
Identify Existing Measures to be Leveraged	
Technical Mitigations	
Processes	
Policies	
Plans	

Consideration	Answers/Comments
Assess the Current State of the Organization	
Is our technical environment up to date and well maintained?	
Is our IT/security team adequately staffed?	
Do our employees take cybersecurity seriously?	
Has the organization ever performed a cybersecurity assessment?	
What are our critical business processes that could be disrupted by a cyber incident?	
Does the organization have a risk management process in place?	
How does the organization vet and oversee 3rd party vendors with access to the network or data?	

Consideration	Answers/Comments
Find a Framework	
Is the organization required to follow a specific framework?	
Does the organization have any future audit goals?	

Based on the above:
 	
• Choose a common cybersecurity governance framework such as:
  ○ NIST CSF
  ○ CIS Controls
  ○ COBIT
 	
• Or, choose an audit framework such as:
  • SOC2
  • CMMC
  • NISTSP800-53	

Consideration	Answers/Comments
Plan Out the Next Steps	
1. Organize the program team.	
2. Assess the organization holistically.	
3. Put together plans for improving cybersecurity.	
4. Develop processes and plans for incident response.	
5. Conduct training with the new processes.	
6. Test the processes and training with an exercise.	
7. Continue Assess, Plan, Train, Exercise process at regular intervals.	

Free Resources

- FTC Small Business- ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- NIST Cybersecurity Framework - nist.gov/cyberframework
- CIS Controls - cisecurity.org/controls
- KnowBe4 Phish Alert - knowbe4.com/phish-alert
- TEEX Cyber Training - teex.org/cyber
- Global Cyber Alliance - globalcyberalliance.org/use-a-tool/
- Remote Work Toolkit - gotomeeting.com/work-remote/resources

Cybersecurity News Sources

- MS-ISAC provides notifications and analysis of the latest threats- cisecurity.org /ms-isac/
- Threatpost is an independent news site covering cybersecurity - threatpost.com
- Krebs on Security is a security blog with breaking news - krebsonsecurity.com
- Dark Reading is a deeper, more technical news site - darkreading.com
- SC Magazine is a news site operated by the CyberRisk Alliance - scmagazine.com

Andrew "AJ" Jarrett | Program Manager
Texas A&M Engineering Extension Service (TEEX)
Andrew.Jarrett@teex.tamu.edu
(979) 458-6724
CyberReady.org