Information Technology Audit 2022

Summary

In October 2022, Barton Community College (“Barton”) selected Tandem Cyber Operations, LLC (“Tandem”) to perform an audit of Barton’s Information Technology (“IT”) department and to assist with the development of a blueprint for best practice adoption. The areas stemming from Tandem’s audit of Barton’s posture are summarized below:

Governance – Revise Information Security policies and procedures to be more relatable with industry and incorporate best practices, standards, and regulatory guidance.

Blueprint – Implement the immediate cyber security recommendations as a foundation for college and department-level security improvements.

Budget – Provide the necessary support to mature Barton’s IT program over the long-term. Continue providing the IT staff with the necessary resources to address their areas of responsibility.

Audit Recommendations

- Updating policy to reflect the Information Services Security Procedures
- Incident Response Team (CSIRT)
  - Train more Information Services employees to be part of CSIRT.
  - Practice response plan and evaluate steps for improvement
  - Continue training for all Information Services employees
- New onboard employee cybersecurity training for all departments.
- More frequent phishing testing for all departments and then additional training for employees that are happy clickers.

GLBA (Gramm-Leach-Bliley Act)

FTC Safeguards Rule: GLBA (Gramm-Leach-Bliley Act)

The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

The Rule defines customer information to mean "any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of you or your affiliates."

Information Security Program requirements.

a. Designate a qualified individual

b. Conduct a risk assessment

c. Design and implement safeguards to control the risks identified through your risk assessment
    1. Implement and periodically review access controls.
    2. Know what you have and where you have it
    3. Encrypt customer information on your system and when it's in transit
    4. Assess your apps
    5. Implement multi-factor authentication for anyone accessing customer information on your system.
    6. Dispose of customer information securely.
    7. Anticipate and evaluate changes to your information system or network.
    8. Maintain a log of authorized users' activity and keep an eye out for unauthorized access.

Information Security Program requirements – cont.

d. Regularly monitor and test the effectiveness of your safeguards.

e. Train your staff.

f. Monitor your service providers.

g. Keep your information security program current.

h. Create a written incident response plan.

1. Goals
2. The internal processes your company will activate in response to a security event;
3. Clear roles, responsibilities, and levels of decision-making authority;
4. Communications and information sharing both inside and outside your company;
5. A process to fix any identified weaknesses in your systems and controls;
6. Procedures for documenting and reporting security events and your company's response; and
7. A post mortem of what happened and a revision of your incident response plan and information security program based on what you learned.

i. Require your Qualified Individual to report to your Board of Directors.

Questions?