So You Want to Be an Information Security Officer?

Presented by:
Art Bakke
Information Security Officer
Background

• Personal

• Starion Bank
Art’s Goals

• Highlight the typical responsibilities of an Information Security Officer from technical to non-technical aspects

• Emphasize the soft-skills necessary to be effective and successful in this role

• Be Inspiring
Agenda

• Job Purpose
• Primary Accountabilities
• 5 Functional Responsibilities
  – Information Security Program
  – Business Continuity Program
  – Incident Response Program
  – Vendor Management Program
  – Audit
• Identify Soft Skills Needed to Be Effective
Job Purpose

• “Provide **oversight** and **management** to **protect** the **information assets** of the bank and support the information governance policies and processes, compliance, information security and business continuity plans.”
Job Purpose (continued)

• “Actively work with **business unit owners** and other service providers to **institutionalize a solid security and overall information technology governance framework.**”
Primary Accountabilities

• “Responsible for the development and ongoing management of the bank’s information security program to ensure it is compatible with applicable laws and regulations.”
5 Functional Responsibilities

1. Information Security Program
2. Business Continuity Program
3. Incident Response Program
4. Vendor Management Program
5. Audit
Information Security Program (1)

• Develop, implement and administer all segments of the Bank’s ISP

• Partner with business units and users to develop and enforce information security policy and procedures
Information Security Program (2)

- Provide consultation and written reports to Senior Management, Audit Committee and the Board of Directors

- Ensure proper training is provided to staff
Information Security Program (3)

• Proactive compliance with industry IS regulations

• Partner with the Bank’s Security Officer to ensure overall security of the bank
Information Security Program (4)

• IT Risk Assessment
  – Inherent Risk
  – Residual Risk
  – Future Risk
Business Continuity Program (1)

- **Business Continuity Plan (BCP)**
  - Business Continuity Steering Committee
  - Crisis Management Team
- **Business Impact Analysis**
Business Continuity Program (2)

• BCP Calendar (January)
  – Monthly DR Tests
  – Exercises
    • Table Top
    • Workplace Relocation/Recovery

• Education and Awareness
Incident Response Program

• Administer program in the event of a cyber security breach that compromises Confidentiality, Integrity, and/or Availability
Vendor Management Program

• Administer program to validate new and existing vendors to protect our organization and our customers
Audit

• *Conduct Audits of various IT processes*

• *Address requests from internal and external auditors*
Skills

- Technical
- Organizational
- Team Player
- Leadership
- Effective Communication
- Mentoring
- Creativity
- Attention to Detail

- Active Listening
- Inquisitive
- Analytical
- Proactive
- Positive Attitude
- Inspirational
- People Person
- Interpersonal Communication
Agenda Recap

• Job Purpose
• Primary Accountabilities
• 5 Functional Responsibilities
  – Information Security Program
  – Business Continuity Program
  – Incident Response Program
  – Vendor Management Program
  – Audit
• Skills Needed
Art’s Goals Recap

• Highlight the typical responsibilities of an Information Security Officer from technical to non-technical aspects

• Emphasize the soft-skills necessary to be effective and successful in this role

• Be Inspiring
Questions?
Thank You!

• Art Bakke
  Information Security Officer
  artb@starionbank.com
  (701) 667-7554