Colorado Springs

2018 COLORADO CHAMBER OF COMMERCE EXECUTIVES SPRING CONFERENCE

WEDNESDAY, MAY 2ND, 2018 | 10:15AM

Cybersecurity for Small Business

Dr. Shawn P. Murray, C|CISO, CISSP, CRISC

President & Chief Academic Officer, Murray Security Services

Agenda

- IT & Cyber
- Information Security
- Cybersecurity
- Governance
- Operations
- Risk Management
- Cultures and Attitudes
- Homework

IT & Cyber

- Information Technology
  - Information Technology (IT) refers to all of the computer systems and service support contract agreements that the business uses to be productive.
- Cyber
  - This is a concept that relates the computing environment to the business environment.
  - Cyber = Information Technology which is used to enable the business as described in the previous bullet

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Information Security

- The holistic approach for identifying, categorizing and protecting information related to business activities.
  - Written (hard copy),
    - patient files, business plans, engineering schematics, manifests
  - Electronic
    - computerized information that is processed, transmitted or stored using computing systems (Fax machines, computers, mobile devices)
  - All information that the organization creates, uses or receives should have an *information classification scheme*.
    - sensitive
    - propitiatory
    - confidential
    - PII
    - public

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Cybersecurity

- Cybersecurity is the new "*sexy*" term for information security.
- While the focus appears to be primarily related to the IT systems, most IT security professionals agree that all aspects of Information Security are encompassed into this new discipline "brand".
- It also includes contractual agreements for service providers of IT and cybersecurity.
  - Many small businesses don't do IT work and hire people or companies to provide these services which introduces risk.
    - Who has access to your data and information?
    - Do you have Non-disclosure Agreements (NDAs)?

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Governance

- What laws does the business need to comply with?
  - Based on Industry
    - HIPAA, FERPA, GLBA, FISMA
  - Based on business activities
    - HR, patients, clients, employee, credit card transactions
- What standards does the business need to comply with?
  - PCI-DSS
  - GAAP
  - NIST
  - ISO

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Governance

- How does your internal governance strategy align with external governance requirements?
  - Plans
  - Policies
  - Procedures
  - Standards
  - Guidelines

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Operations

- How do employees accomplish daily tasks?
  - Scenario - Chiropractor Credit Card Information
  - Scenario - Dentist and Front Desk PII Breach
  - Phishing - Scenario - Retail Organization Social Engineering Attack
- Cyber Security Awareness Program
  - includes annual training
  - Posters, articles tabletop exercises

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Operations

- Socialize what is important
  - Reward good behavior
  - Develop strategy to correct unacceptable behavior
- How do you conduct incident response and remediation?
  - Who needs to be notified?
    - Internal - Call Trees
    - External - Law enforcement, Federal or State

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Risk Management

IT & Cybersecurity Risk is a business process or activity

- Mitigate
- Accept
- Avoid
- Transfer

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Cultures and Attitudes

- What is the culture related to security in your organization?
  - Should be supported from the top
  - Should be enforced
  - Sometimes you need to slay a lion!
  - Be consistent

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Homework

- Develop a Checklist
  - Look at how your employees are accomplishing tasks identify risks
  - Create Acceptable Use policy - Audience is everyone
  - Create Privileged Use policy - Audience is IT personnel
  - Identify critical Resources, Information & Personnel (RIP Model)
    - Develop strategies to protect disruption to your business
      - Identify multiple resource sources
      - Protect and backup data & information
      - Cross train critical personnel

MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING

Homework

- Develop a Checklist (cont.)
  - Create an information classification scheme
    - Categorize the information
    - Identify the computer systems that inherit the scheme and protect them as well. (Process, transmit or store)
    - Do not make it complex
    - At least identify the important information that you think should be protected and categorize it.
  - How are you vetting your service providers?
    - Do you have signed SLAs?
    - Do they have insurance?
    - Do you have NDAs?

MURRAY SECURITY SERVICES
INFORMATION & CYBER SECURITY TRAINING & CONSULTING


Colorado Chamber of Commerce Executives
CCCE

Questions?


MURRAY
SECURITY SERVICES
INFORMATION & CYBER SECURITY
TRAINING & CONSULTING