Cyber CYA Webinar Series:

Cybersecurity for Small Businesses

CYBER: CYA
Education to *Cover Your Assets*

Colorado
SBDC
TECHSOURCE

THE PIKES PEAK SMALL BUSINESS DEVELOPMENT CENTER HAS BEEN DEDICATED TO HELPING EXISTING AND NEW BUSINESSES GROW AND PROSPER FOR MORE THAN 30 YEARS.

FREE
CONSULTING

PRACTICAL
TRAINING

BUSINESS
RESOURCES

EL PASO COUNTY
COLORADO

Ent
Business Banking

COLORADO
SPRINGS
OLYMPIC CITY USA

PSB Trust.COM
PARK STATE BANK & TRUST

POWERED BY
SBA
U.S. Small Business
Administration

VECTRABANK
COLORADO

Funded in part through a cooperative agreement with the U.S. Small Business Administration

WWW.PIKESPEAKSBDC.ORG/CONSULTING

WWW.PIKESPEAKSBDC.ORG/WORKSHOPS

Colorado Springs

CYBER CYA WEBINAR

WEDNESDAY, AUGUST 28, 2019 | 10:00 – 11:00 AM

Cybersecurity for Small Business

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

President & Chief Academic Officer, Murray Security Services

Colorado SBDC
Small Business Development Center Network

Agenda – 2019 Update!

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

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

Impact for Small Businesses – By the Numbers

- 61 percent of cyber attacks target small business.

- Only 14 percent of small businesses rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective.

- 60 percent of small companies go out of business within six months of a cyber attack.

- 48 percent of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

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

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)?

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

Governance

- What laws does the business need to comply with?
  - On September 1, 2018, the Colorado Protections for Consumer Data Privacy law, HB 18-1128, went into effect.
  - The new Privacy Law provisions are part of the Colorado Consumer Protection Act ("CCPA"), in a continued effort to protect personal data.

    - Ties cyber security to privacy, the strongest law in the U.S.
    - If you process, transmit or store a Colorado citizen's personal information, the law applies to you!

Governance

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

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

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

RIP Model

Info or Data

Critical

Resources

Personnel
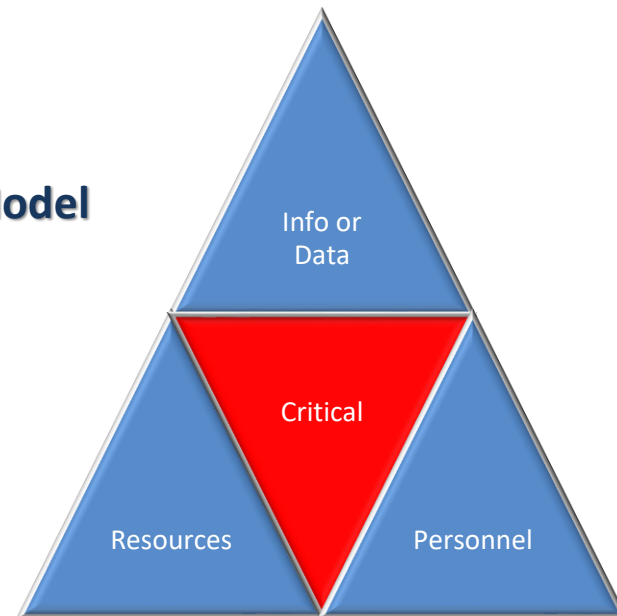
Risk Management

IT & Cybersecurity Risk is a business process or activity

- Mitigate – apply countermeasures to reduce risk

- Accept – risk is minimal

- Avoid – eliminate the risk, its to great

- Transfer – hire a service provider or purchase cyber insurance

Example: SBDC Customer: Fuel provider problem

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

Lack of Cybersecurity Training for Employees

- The good news is owners are aware of the problem as 86% believe digital risk will continue to grow. But this doesn't mean they are all doing something about it.

- Thirty percent of owners with 11-50 employees don't provide any kind of formal cybersecurity training for their workforce. And alarmingly 7% of businesses don't even update their software regularly.

- This complacency is translating to higher instances of successful cyberattacks. Almost two in three owners or 65% admit they have been a victim. In these cases, computer virus (33%) and phishing (29%) attacks are the top methods used by hackers.

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

Homework

- <u>Develop a Checklist (cont.)</u>
  - 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?

Homework

- Schedule an appointment with the Pikes Peak SBDC to speak to a cyber security consultant!
  - Advantages:
    - Our team of professionals are vetted.
    - We work in various industries and have a wealth of experience.
    - We will work with you to address your concerns.
    - 100% confidential
    - Most of our consultants are small business owners as well and work in our community!

Questions?

Pikes Peak Small Business Development Center

559 E. Pikes Peak Ave., Suite 101, Colorado Springs, CO 80903

719-667-3803
sbdc@elpasoco.com

www.pikespeaksbdc.org

OUR SPONSORS:

Funded in part through a cooperative agreement with the U.S. Small Business Administration