CYBERSECURITY SIMPLIFIED

WHAT YOUR SMALL BUSINESS NEEDS TO KNOW

CO-HOSTED BY:

TRI-LAKES
CHAMBER OF COMMERCE
ECONOMIC DEVELOPMENT
VISITOR CENTER

PRESENTED BY:

Colorado SBDC
TECHSOURCE

CYBER: CYA
Education to Cover Your Assets

FACILITATORS:

Coryn & Eric Mann
Owners, Corvus Technologies

719-667-3803
www.pikespeaksbdc.org

EL PASO COUNTY
COLORADO

COLORADO SPRINGS
OLYMPIC CITY USA

connect 2DOT

COLORADO
Office of Economic Development & International Trade
Minority Business Office

Ent
Business Banking

POWERED BY
SBA
U.S. Small Business Administration

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

Colorado SBDC
PIKES PEAK *Small Business Development Center*

About the Facilitators...

Eric A. Mann-CISSP

Co-Owner, Principle Security Consultant -- Corvus Technologies LLC

Eric A. Mann is the co-owner of Corvus Technologies, LLC. He has honed his Cybersecurity career and is a Subject Matter Expert (SME) with over 20 years combined experience in systems administration, enterprise computing optimization, systems certification and accreditation, systems hardening, vulnerability assessment, penetration testing, and information assurance.

His diverse background helps to uniquely position Corvus Technologies, LLC for projects that bridge the gap between Compliance and Cybersecurity. Eric leverages experience and best practices from multiple industries while adhering to customer specific rules and regulations.

Eric established Corvus Technologies, LLC with his wife Coryn to combine their talents and provide subject matter expertise in the fields of Compliance, Cybersecurity, NIST SP 800-171 and Subcontract Management services.

Coryn D. Mann-CISSP

Owner, Principal Subcontracts Manager -- Corvus Technologies LLC

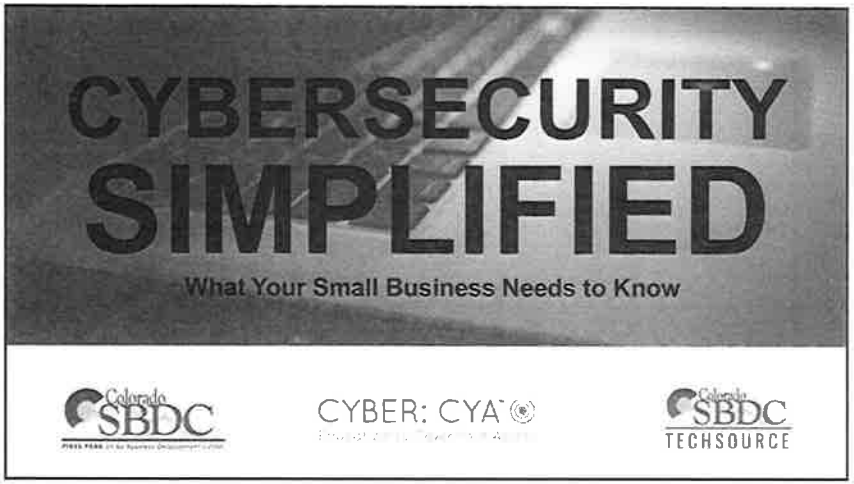
Coryn D. Mann is the owner of Corvus Technologies, LLC. She has extensive experience in Subcontract Management, Supply Chain Management and Procurement.

In her career Coryn has focused on serving the Federal Government for the past 25 years, leveraging her skills from 11 years of active duty U.S. Air Force and 14 years of Defense Subcontracting services. She is dedicated to lowering cost and fostering competition using Subcontract Management best practices thru the Subcontract Lifecycle.

Coryn established Corvus Technologies, LLC with her husband Eric to combine their talents and provide subject matter expertise in the fields of Compliance, Cybersecurity, NIST SP 800-171 and Subcontract Management services.

To register for free consulting: www.pikespeaksbdc.org/consulting

Pikes Peak Small Business Development Center
Phone: (719) 667-3803
Email: sbdc@elpasoco.com
Website: www.pikespeaksbdc.org



Cybersecurity 101

FOR SMALL BUSINESS

8 November 2018

Course Flow

- What is Cybersecurity?
- Who is at risk?
- Types of cyberattacks
- Where do we start?
- Core
- Ring 1
- Ring 2
- Ring 3
- Edge
- How well are you protected?
- Resources
- Q&A (free-for-all)

What is Cybersecurity?

- Defined as:
  - Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack[1]
- Broader concept of Information Assurance (IA):
  - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities[2]

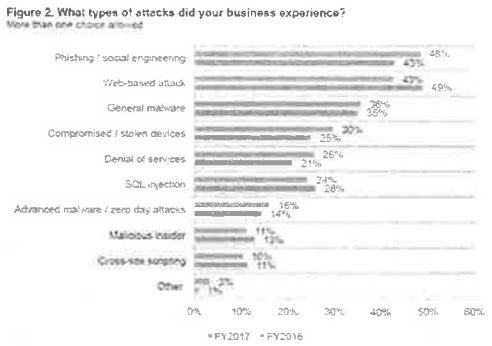
1 – Source: Merriam-Webster Dictionary
2 – Source: NIST SP 800-59 - Guideline for Identifying an Information System as a National Security System

Who is at risk?

- Everyone, but especially small businesses!
  - Lack of awareness
  - Lack of budget
  - Lack of formal processes
  - Reactive vs. Proactive
- 61% of Small & Medium-Sized Business (SMB) survey members (366/600) reported cyberattacks within last 12 months[3]:
  - Data breaches involved both employee and customer data
  - $1,027,053 average amount spent to respond to attacks (↑~14%)
  - $1,207,965 average cost of disruption to operations (↑~21%)

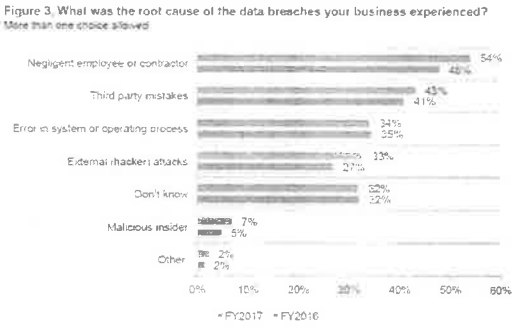
3 – Source: Ponemon Institute, 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), September 2017

Types of cyberattacks



4 – Source: Ponemon Institute, 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), September 2017

Types of cyberattacks (continued)



5 – Source: Ponemon Institute, 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), September 2017

Where do we start?

- Core to Edge Concept:
  - Core and Concentric Rings
  - Core = Easy/Quick/Cheap
  - Rings = Increased Effort
  - Edge = Most Effort
  - a.k.a. Defense in Depth
- Order/Priority of Implementation:
  - Cybersecurity to Information Assurance
  - Technical to Management
- All components are needed!
  - Work items in parallel

source: rgbstock.com

Core

- BACKUP your data!!!
  - Local AND Remote (Cloud)
  - Employ data-at-rest encryption
  - Frequency based on data volatility
- Cybersecurity Awareness Training
  - Normal user
  - Role-based (e.g. Incident Response, Security Administrator)
  - Social Engineering

Ring 1

- Deploy anti-virus/malware detection applications
  - Unified Threat Management (UTM)
- Enable system firewalls
- Enforce account password best practices:
  - Utilize long passwords with 4 points of complexity:
    - Numbers, Letters (upper/lower case), and Special Characters
  - Create unique passwords for each account/application
  - Utilize a password manager that encrypts data-at-rest
- Patch/update all system components (to include firmware!)
  - Where possible, enable auto-update!

Ring 2

- Employ data-at-rest encryption across environment:
  - Non-removable system drives
  - Removable media / USB devices
- Encrypt Email
  - Virtru (Office 365/G-Suite)
  - U.S. Government External Certificate Authority (ECA)
- Implement Multifactor Authentication:
  - Hardware key fob (e.g. RSA SecurID, Yubikey)
  - Software token (e.g. SAASPASS, Google Authenticator)

Ring 2 Continued

- Utilize Virtual Private Networks (VPNs)
  - The outside world is HOSTILE!
  - Use at ALL external locations
- Implement Wi-Fi Security
  - Wi-Fi Protected Access Version 2 (WPA2)
  - Change Pre-Shared Key (PSK) regularly
  - Media Access Controller (MAC) Address Whitelisting
  - WPA2 Enterprise:
    - Institute of Electrical and Electronics Engineers (IEEE) 802.1X = Port Security
    - Remote Authentication Dial-In User Service (RADIUS) = Secure Authentication
- Perform systems security hardening:
  - Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs)
  - Center for Internet Security (CIS) Benchmarks

Ring 3

Establish/Maintain:

- Systems auditing process
  - Include entire environment!
  - Balance system function against reporting fidelity
- Incident Detection and Response capability
  - Tailor based on customer requirements
- Systems Vulnerability Scanning and Remediation
  - Best practice is quarterly or more often

Edge

- Purchase Cybersecurity Liability Insurance
  - May require up-to-date Business Plan
- Develop/Maintain Cybersecurity/IA Policies and Procedures
  - Continuity of Operations Plan (COOP)
  - Disaster Recovery Plan (DRP)
  - Change Management (CM) Plan
- (If Possible) Assign dedicated cybersecurity resources
  - Maintain skills with advanced security training
- Continually assess, review, and adjust security posture
  - Annually
  - Continuous monitoring

How well are you protected?

- Percentage of core/ring/edge best practices implemented?
- Confidence level in current cybersecurity operations?
- Any success stories to share?
- Do you have any formal external customer cybersecurity requirements to meet? (e.g. HIPAA, PCI, GLBA, NIST 800-171)

Resources

- Core:
  - Data Backup Local – Time Machine (Apple), Backup and Restore (Microsoft)
  - Data At Rest Encryption – FileVault (Apple), Bitlocker (Microsoft)
  - Data Backup (Remote) – OneDrive (Microsoft), GoogleDrive (Google), Carbonite (https://www.carbonite.com)
  - Security Awareness Training – https://iase.disa.mil/eta/Pages/online-catalog.aspx
  - Security Awareness Training – https://www.cybrary.it
  - Security Awareness Training – https://www/cfisa.org
- Ring 1:
  - Antivirus/Malware Detection - https://www.av-comparatives.org
  - Account Password Best Practices - https://csrc.nist.gov/publications/detail/sp/800-63b/final
  - Password Managers - https://thewirecutter.com/reviews/best-password-managers
  - Password Managers - https://lifehacker.com/5529133/five-best-password-managers

Resources (continued)

- Ring 2:
  - Systems Hardening - https://iase.disa.mil/stigs/Pages/index.aspx
  - Systems Hardening - https://www.cisecurity.org/cis-benchmarks/
  - Multifactor Authentication - https://www.rsa.com/en-us/products/rsa-securid-suite
  - Multifactor Authentication - https://www.yubico.com/
  - Email Encryption - https://www.virtru.com/
  - External Certificate Authority - https://eca.orc.com/
  - Virtual Private Network - https://www.cnet.com/best-vpn-services-directory/
  - Virtual Private Network - https://www.pcmag.com/article2/0,2817,2403388,00.asp
  - Virtual Private Network - https://nordvpn.com/

Resources (continued)

- Ring 3:
  - Systems Auditing - https://csrc.nist.gov/publications/detail/sp/800-92/final
  - Incident Detection & Response - https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft
  - Incident Detection & Response - https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- Edge:
  - IA Policies and Procedures - http://www.i-assure.com/products/rmf-templates/
  - IA Policies and Procedures - https://www.sans.org/security-resources/policies
  - Advanced Training - https://certification.comptia.org/certifications/security
  - Advanced Training - https://www.sans.org/courses/

Q&A (free-for-all)

Questions/Comments/Concerns?