Cyber Fundamentals

21 September 2023

corvus
TECHNOLOGIES

Tailored Information Assurance, Cybersecurity, and Compliance Services

Coryn Mann BIO

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 800-53, NIST SP 800-171 services & Subcontract Management services.

Eric Mann BIO

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 800-53, NIST SP 800-171 & Subcontract Management services.

CORVUS TECHNOLOGIES

Agenda

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

Tailored Information Assurance, Cybersecurity, and Compliance Services

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]

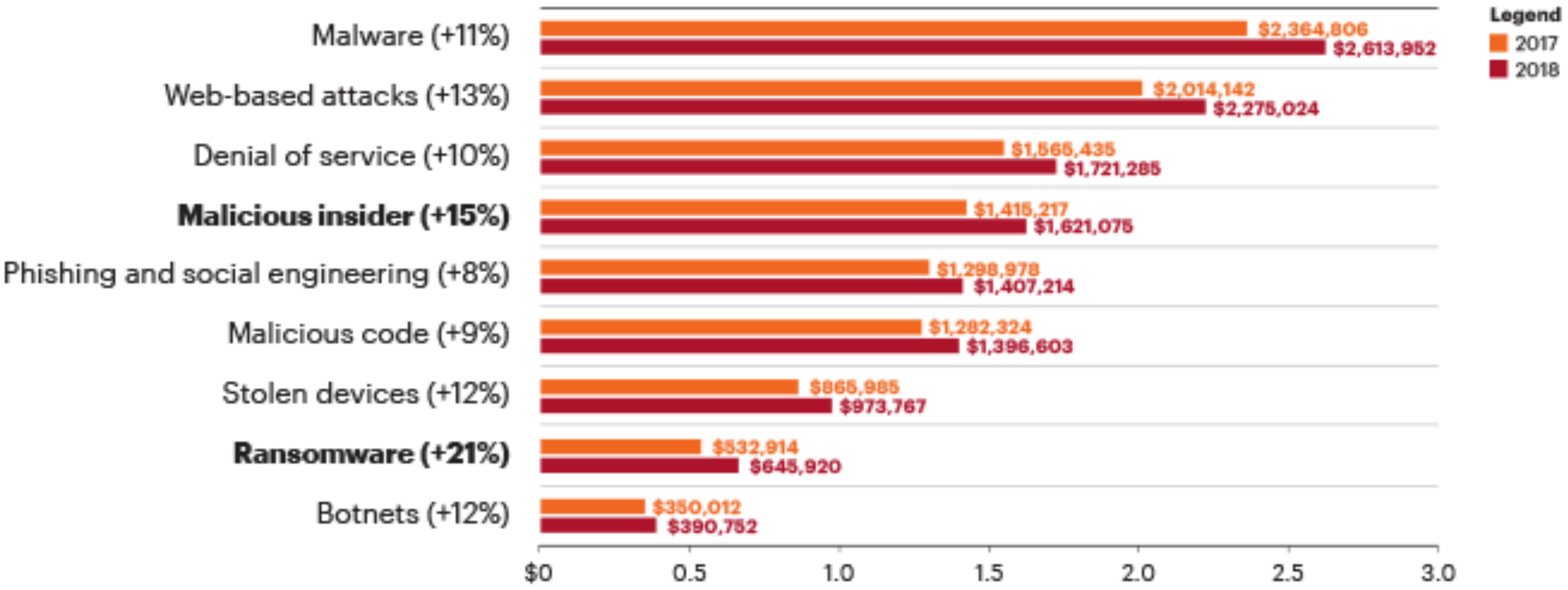
1 – Source: Merriam-Webster Dictionary
2 – Source: NIST SP 800-59 - Guideline for Identifying an Information System as a National Security System

Who is at risk?

- **Everyone, but especially small businesses!**
  - **Lack of awareness**
  - **Lack of budget**
  - **Lack of formal processes**
  - **Reactive vs. Proactive**
- **Cisco's 2021 Cyber Security Threat Trends[3]**
  - **Found that 69% of SMBs had experienced a cyber-attack**
- **IBM's 2022 Cost of Data Breach Report[4] revealed that the cost of a data breach averaged USD $4.35 million in 2022:**
  - **Represents a 2.6% increase from 2021 ($4.24 million)**
  - **Average cost has climbed 12.7% from 2020 ($3.86 million)**

3 – Source: Cisco's 2021 Cyber Security Threat Trends
*4 – Source: IBM 2022 Cost of Data Breach Report**

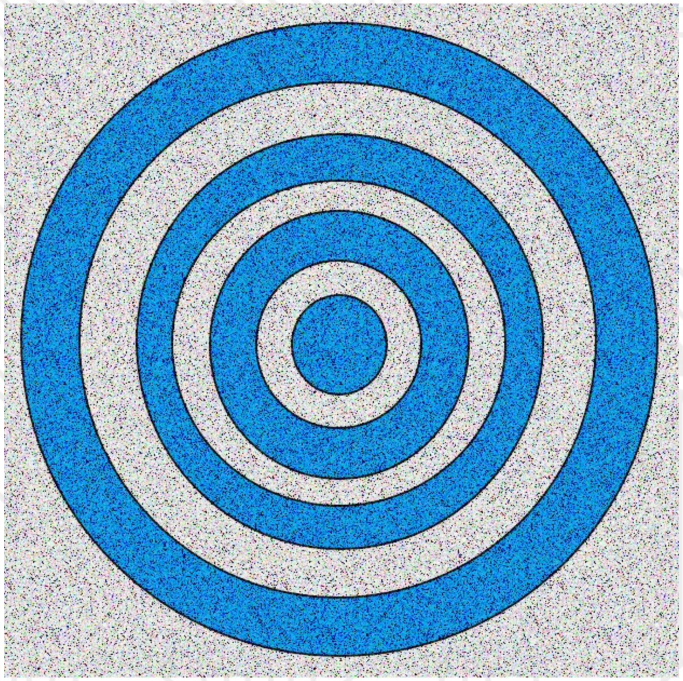
Types of Cyberattacks



CORVUS TECHNOLOGIES

Where do we start?

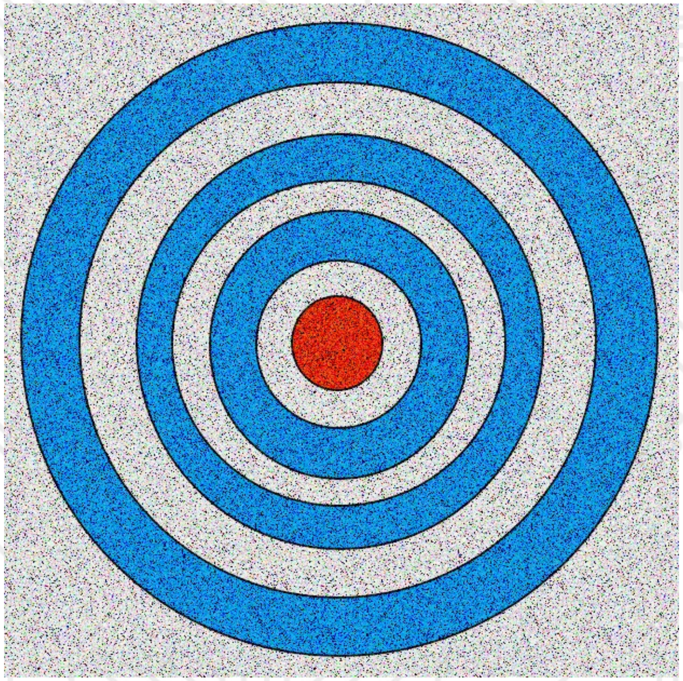
- ❖ Core to Edge Concept:
  - ➢ Core and Concentric Rings
  - ➢ Core = Easy/Quick/Cheap
  - ➢ Rings = Increased Effort
  - ➢ Edge = Most Effort
  - ➢ a.k.a. Defense in Depth
- ❖ Order/Priority of Implementation
  - ➢ Cybersecurity to Information Assurance
  - ➢ Technical to Management
- ❖ All components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



Tailored Information Assurance, Cybersecurity, and Compliance Services

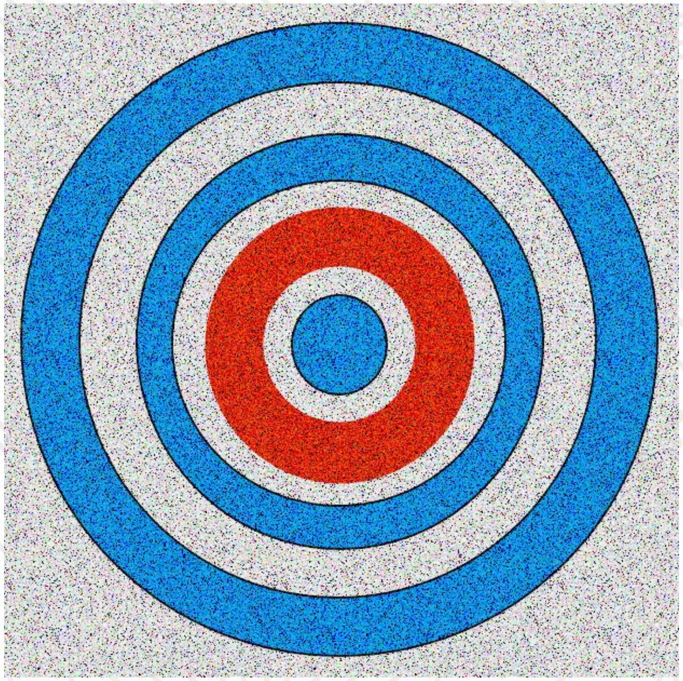
Core

- Identify and BACKUP your critical 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



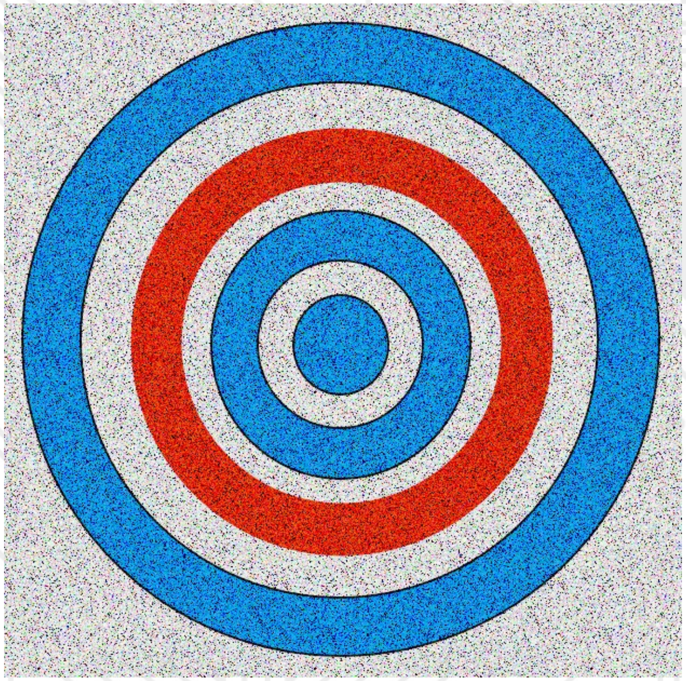
Ring 1

- Deploy anti-virus/malware detection applications
  - Unified Threat Management (UTM)
- Enable system firewalls
- Enforce account passwords 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 including firmware!
  - Where possible, enable auto-update!



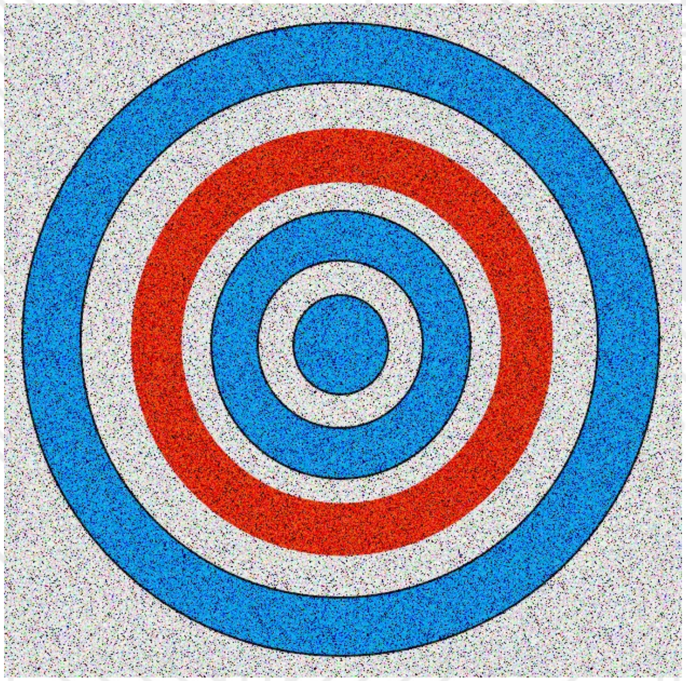
Ring 2

- Employ data-at-rest encryption across environment:
  - Non-removable system drives
  - Removable media / USB devices
- Encrypt Email:
  - Virtu (Office 365/G-Suite)
  - External Certificate Authority (EAC)
- Implement Multifactor Authentication:
  - Hardware key fob (e.g., RSA SecurID, Yubikey)
  - Software token (e.g., Google Authenticator)
- Utilize Virtual Private Networks (VPNs)
  - The outside world is HOSTILE!
  - Use at ALL external locations



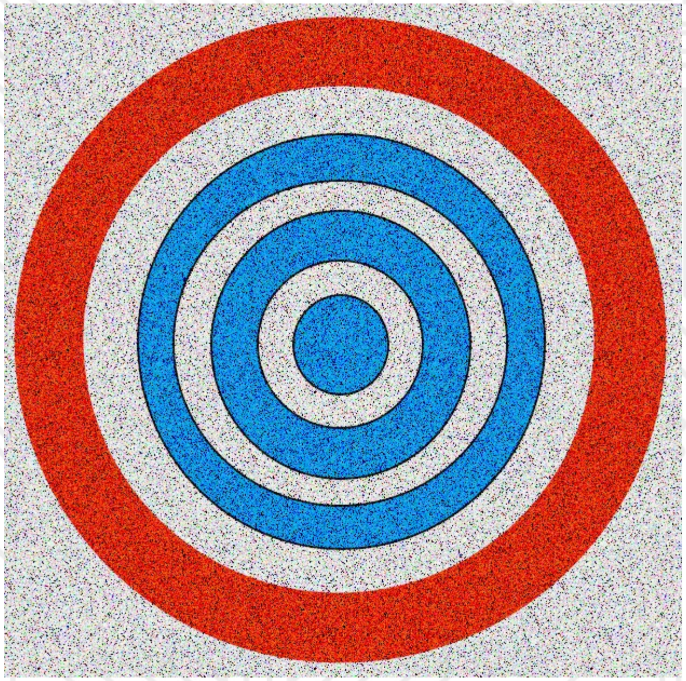
Ring 2 (continued)

- 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



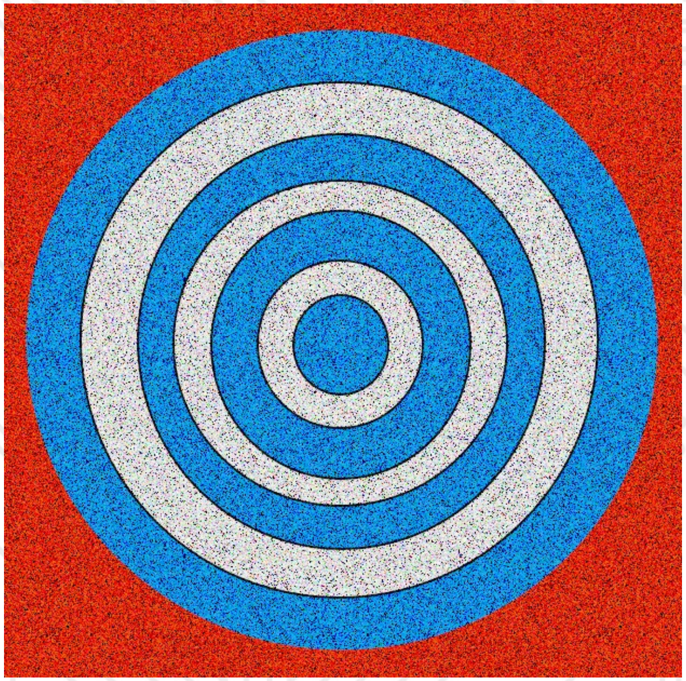
Ring 3

- ❖ Establish and Maintain:
  - ➢ Systems auditing process:
    - o Include entire environment!
    - o Balance system function against reporting fidelity
  - ➢ Incident Detection and Response capability:
    - o Tailor based on customer requirements
  - ➢ Systems Vulnerability Scanning and Remediation:
    - o 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



Artificial Intelligence

- **Mimicking Human Behavior:**
  - **Voice Deepfakes & Virtual Kidnappings.**

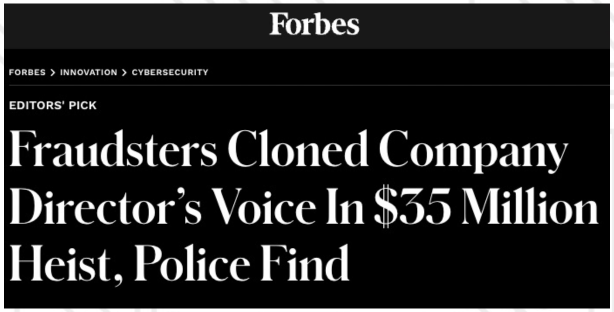
  https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions

- **Complex Social Engineering:**
  - **Attackers use social media like LinkedIn with GPT to create complex believable social engineering attacks or simply convince GPT to write malicious code.**

  https://www.forbes.com/sites/forbestechcouncil/2023/05/26/how-ai-is-changing-social-engineering-forever/

- **New Technology, New Vulnerabilities:**
  - **ChatGPT's Plugins Beta feature does not vet plugin creators.**
  - **Malicious or poorly written plugins can access and execute content from malicious web sites or extract data from your environment.**

  https://embracethered.com/blog/posts/2023/chatgpt-webpilot-data-exfil-via-markdown-injection/

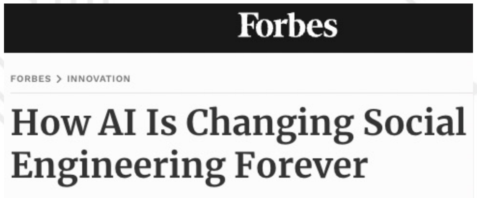


Forbes

FORBES > INNOVATION > CYBERSECURITY

EDITORS' PICK

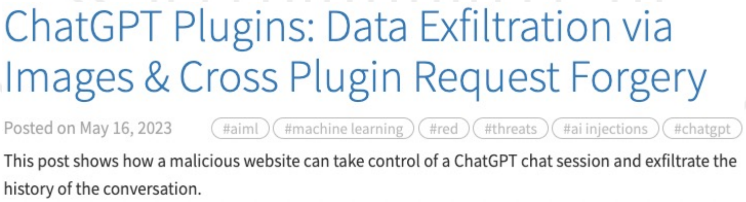
Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find



Forbes

FORBES > INNOVATION

How AI Is Changing Social Engineering Forever



ChatGPT Plugins: Data Exfiltration via Images & Cross Plugin Request Forgery

Posted on May 16, 2023 #aiml #machine learning #red #threats #ai injections #chatgpt

This post shows how a malicious website can take control of a ChatGPT chat session and exfiltrate the history of the conversation.

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., HIPPA, PCI, GLBA, NIST SP 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://public.cyber.mil/training/cyber-awareness-challenge/.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://public.cyber.mil/stigs/
  - Systems Hardening - https://www.cisecurity.org/cis-benchmarks/
  - Multifactor Authentication - https://duo.com/
  - 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/
  - Advanced Training - https://www.pluralsight.com/browse/information-cyber-security

Q&A

Any Questions?

You can reach us by phone or email. Check out our website (www.corvus-tech.net) for more information about us.