Cybersecurity Threats: Survival Tips for Management Accountants

Kristine Brands, CMA

March 7, 2022

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE

Tech-Talk Mondays Title Sponsor

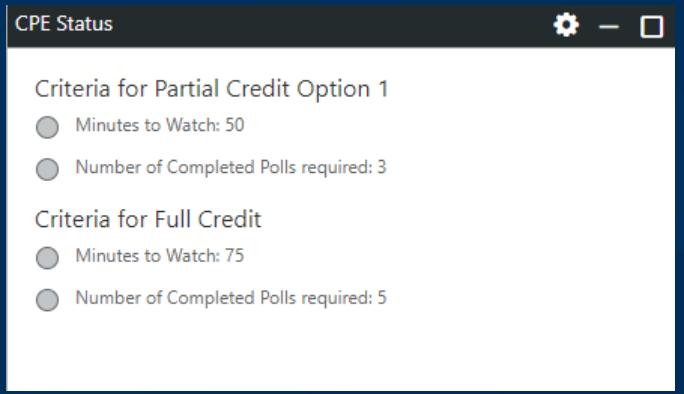
www.netsuite.com

Webinar Features and CPE Credit

Q&A Asking Questions

? Help

CPE Credit



ima® The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE

Moderator

Brad Hamilton

Co-Owner

Hamilton Accounting Services LLC

Member

IMA Technology Solutions & Practices Committee

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE

Featured Presenter

Kristine Brands, CMA

Assistant Professor

United States Air Force Academy

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE

Kristine Brands' Biography

- Kristine Brands is an Assistant Professor of Management at the United States Air Force Academy in Colorado Springs, CO where she teaches financial and managerial accounting, accounting ethics, AIS, and advanced auditing. She is a member of the Institute of Certified Management Accountants Board of Regents, the IMA's Technology Solutions and Practices Committee, and its Memorial Education Foundation. Kristine was also a subject matter expert for ISO 21378, Audit Data Collection. Her research interests include business analytics, accounting ethics, XBRL, accounting for sustainability, and the integration of technology in accounting courses.
- Ms. Brands has authored numerous columns for Strategic Finance, a dozen peer reviewed articles, and speaks nationally and internationally on accounting, technology, and ethics. She holds a BA in History from the University of Rochester, an MBA from Emory University, a Certificate in Applied Science from Harvard University Extension, and a Doctorate in Management from Colorado Technical University.

Learning Objectives

1. Give examples of cybersecurity risks and threats faced by companies and organizations.
2. Explain the cybersecurity triad of data security: confidentiality, integrity, and availability (CIA).
3. Describe the principles of cybersecurity.
4. Discuss how you can apply cybersecurity principles in your organization to safeguard data and information.
5. Identify how to implement a cybersecurity risk management framework in your organization.

ORACLE NETSUITE

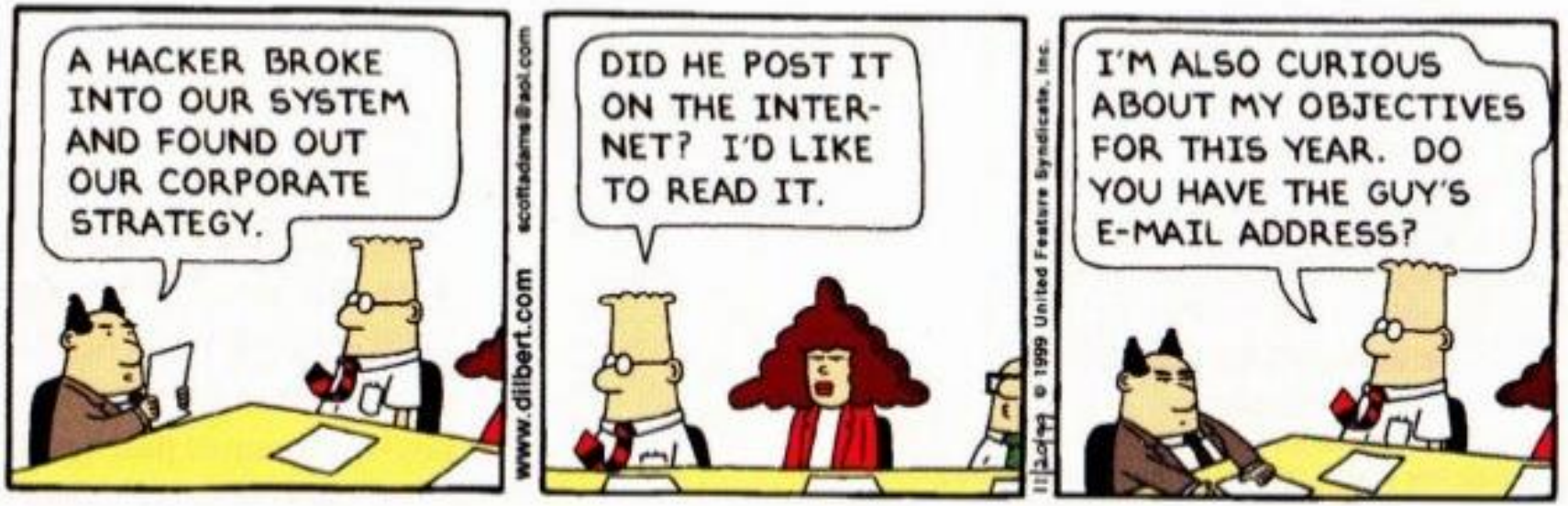
Disclaimer

The views expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense, or the US Government. Distribution A: Approved for Public Release, Distribution Unlimited.

Agenda

1. Introduction
2. Cybersecurity Basics and the Triad
3. 10 Principles of Cybersecurity and Controls
4. Cybersecurity Risk Assessment Framework
5. Conclusion
6. Key Takeaways
7. Resources

Introduction



When Dilbert Jokes About It, It is Mainstream

Source: https://dilbert.com/search_results?terms=hacker

“If you spend more on coffee than on IT security, you will be hacked. What’s more, you deserve to be hacked.”

Richard Clarke, the former National Coordinator for Security, Infrastructure Protection, and Counterterrorism for the United States

Poll Question 1:

Has your organization been hacked?

a. Yes
b. No

Poll Question 1 Results: (Placeholder)

IBM's 2021 Cost of a Data Breach Report

- Average Cost of Breach - $4.24 Million US (+10% over 2020)
- Average Time to Identify and Contain – 287 Days
- Costliest Country – US. Average $5.82 Million
- Costliest Industry – Healthcare

Source: https://www.ibm.com/security/data-breach

Data Breach Costs According to IBM

- Detection and escalation
- Notification
- Lost business
- Post breach response
- And don’t forget reputation

The Gartner Group – 2021 Trends

- Calls for Engaged Boards
- Calls for Vendor Consolidation
- Calls for Attack Simulation
- Follow Consolidation Strategy
- Privacy Enhancing Computing
- Predicts By 2025 Hacks Cause Deaths

Verizon's 2021 Data Breach Investigations Report

- Ransomware Increasing
- People Cause 85% of Breaches
- Errors as Cause Dropped (21% to 17%)
- Web Apps are Targets
- Cloud Targets Increased

Source: https://www.verizon.com/business/resources/reports/2021/2021-dbir-executive-brief.pdf

Ransomware Attack May 2021

Colonial Pipeline

- Risk - 5,500 Mile East Coast USA Fuel Pipeline
- Ransomware Attack - Threatened to Release Company Data
- Cost - Paid $4 Million US (75 bitcoin)
- Group - DarkSide
- Significance – Infrastructure Attack

Ransomware Attack March 2021

- Hackers Encrypted Data on 15,000 Computers
- Compromised SSN and Health Benefit Data
- Cost - $40 Million US Ransomware Attack
- Group - **Evil Corp**
- **Significance – Financial**

CNA Financial

Ransomware Attack May 2021

- Shutdown Entire US beef Processing Operation
- Servers Supporting JBS's IT systems in North America and Australia
- Cost - $11 Million US
- Group – Revil
- Significance – Food Chain Attack

Russian Ransomware Attacks (TDB)

"Russian Ransomware Hackers Pledge Support to Putin and Immediately Have Secret Chats Exposed by Ukrainian Leaker"
(Source: Currently from AT&T)

- Group - Conti Ransomware Gang (2020)
- Ransomware-as-a-service
- Inception to Date "Revenue" $30 Million

Poll Question 2:

Has your organization been victim of a ransomware attack?

a. Yes
b. No

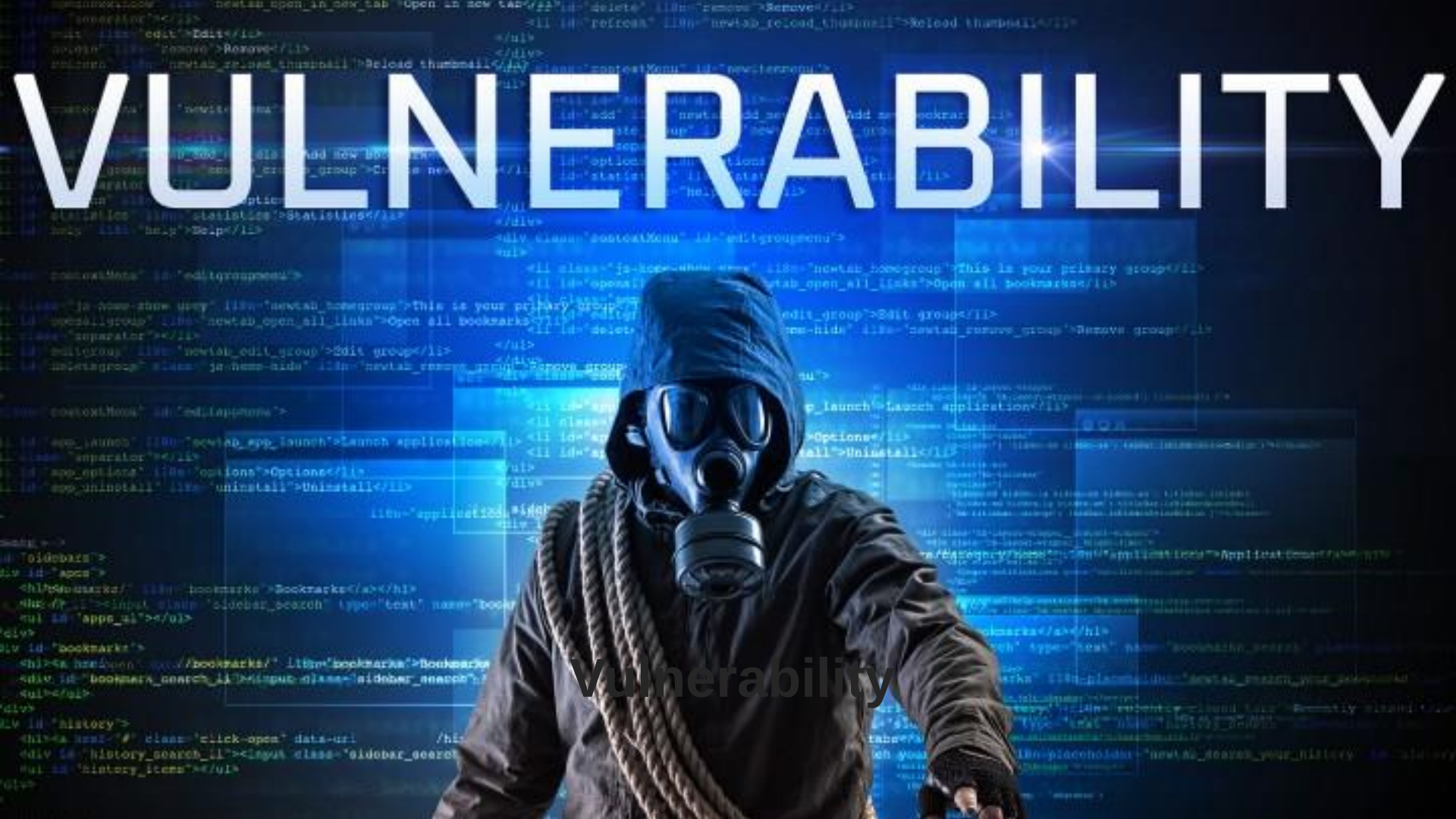
Poll Question 2 Results: (Placeholder)

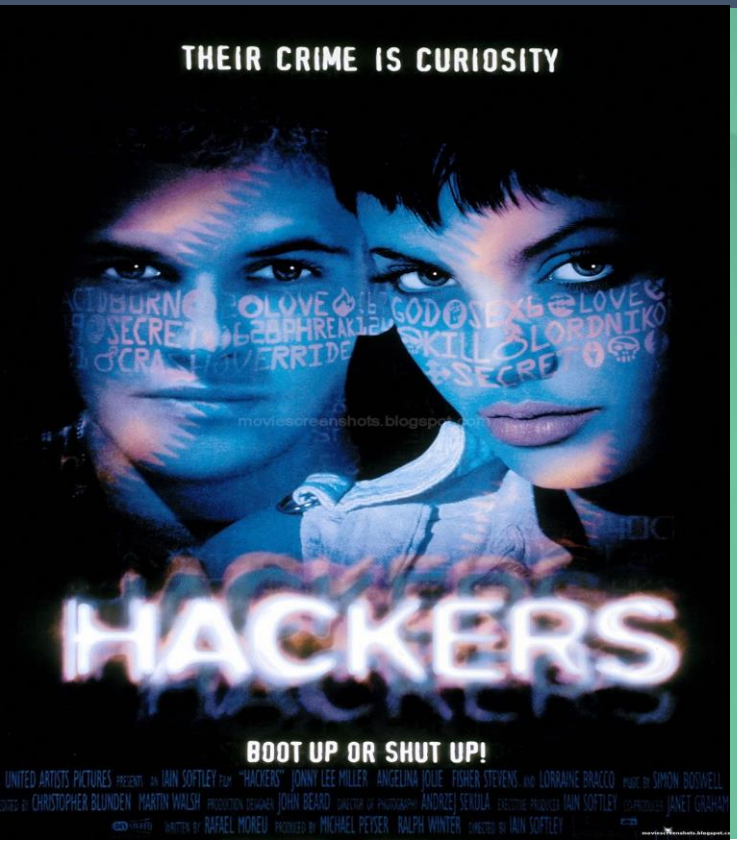
Cybersecurity Basics

cy·ber·se·cur·i·ty
noun

the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this

Source: Oxford Dictionary


VULNERABILITY
Vulnerability

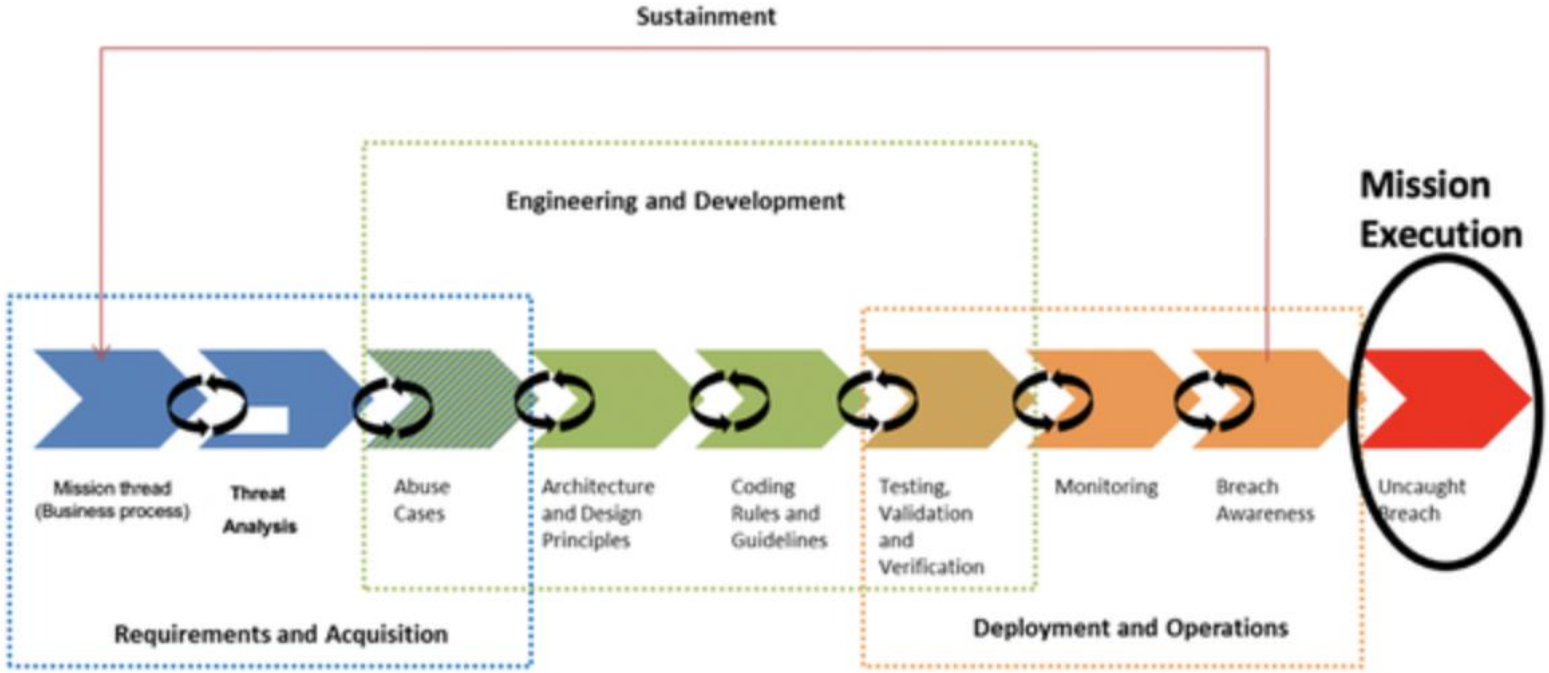


Hacker Manifesto

This is our world now... the world of the electron and the switch [...] We exist without skin color, without nationality, without religious bias... and you call us criminals. [...] Yes, I am a criminal. My crime is that of curiosity."

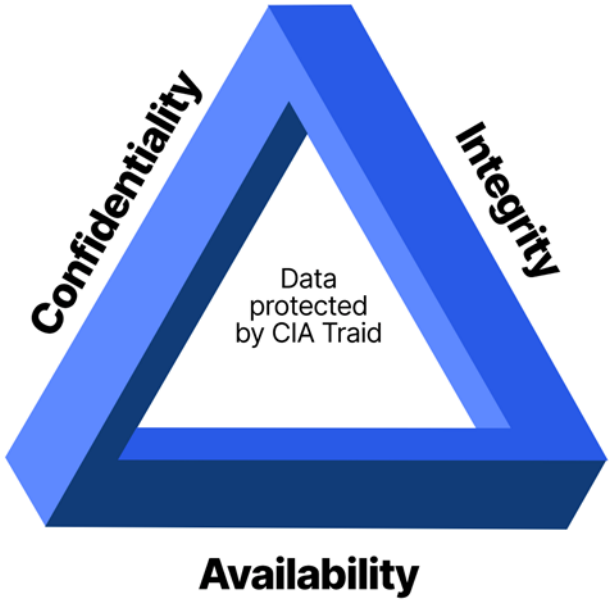
Source: The Mentor (born Loyd Blankenship

Cybersecurity is a Lifecycle Challenge



https://insights.sei.cmu.edu

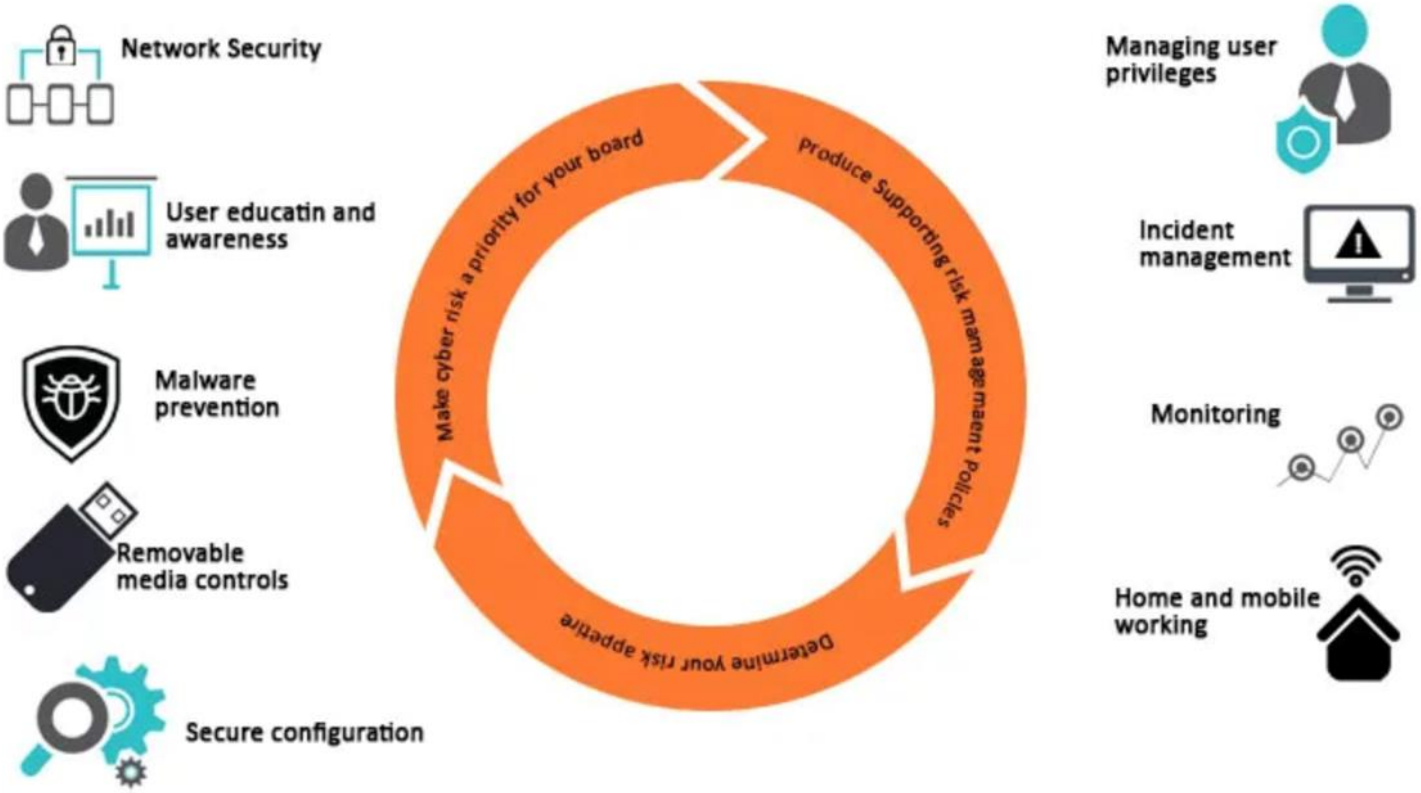
Cybersecurity Triad



Source: https://www.imperva.com/

10 Principles of Cybersecurity

10 Steps to Cyber Security



1. Education and Awareness

- Focus on Cybersecurity Training and Awareness
- 95% of Attacks are Caused by Human Error

Implement Cybersecurity Training

- Computer system orientation
- Educate and remind employees about threats
- Encourage incident reporting

Poll Question 3:

Does your organization hold periodic cybersecurity training?

a. Yes
b. No

Poll Question 3 Results: (Placeholder)

2. Removable Media and Personal Devices

- Establish Strong Defense - Source of Cybersecurity Breaches like Malware, Viruses, and Vulnerabilities

Removable Media Controls

- Issue Company Removable Devices
- Establish Removable Device Policies
- Install Malware Scanning Software
- Minimize Need for Removable Media

Employees – Cybersecurity Achilles Tendon

Source: www.dreamstime.com

3. Mobile and Work at Home

- Establish Security and Network Policies

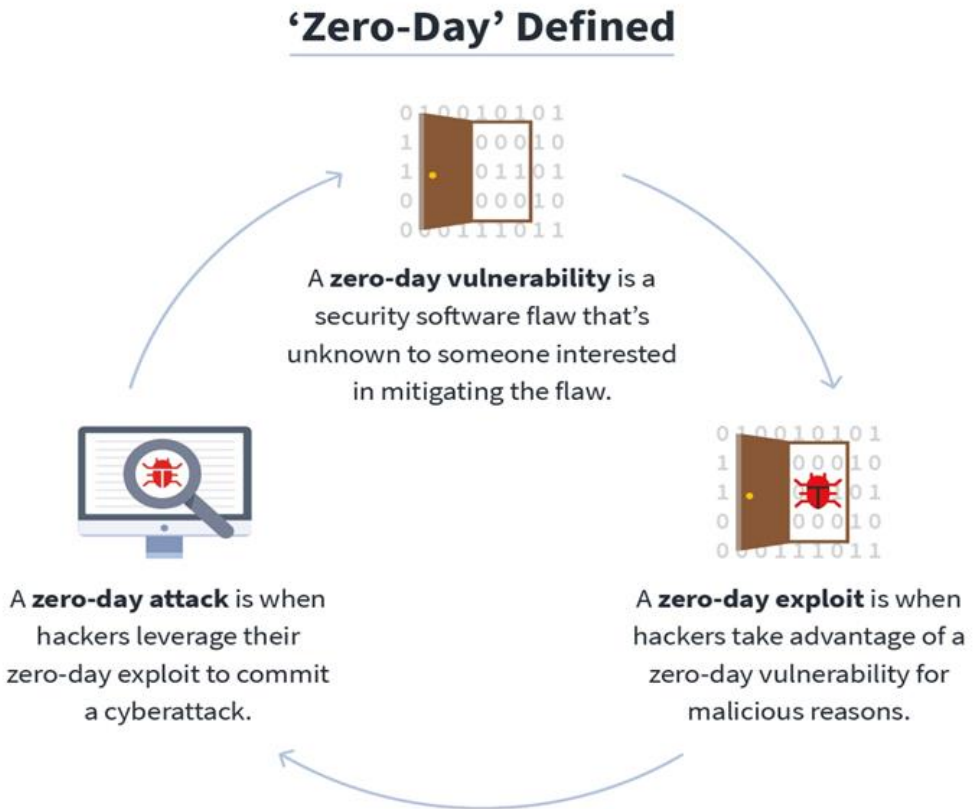
Mobile and Work at Home Controls

- Risk Assessment
- Establish Secure Configuration
- Safeguard Data – Encryption
- Hardware/Software Policies
- Training and Education
- Issue Organization Owned Hardware

4. Malware Prevention

- Malware is Malicious Software – Viruses, Worms, Adware, Spyware Ransomware
- Sources – Emails, System Vulnerability, Web Pages, Portable Devices

‘Zero-Day Attack



Norton Zero Day Attack

Malware Controls

- Use Reliable Software
- Detection and Prevention is Key Defense
- Test Software
- Open Attachments from Reliable Sources
- Be Wary of Websites
- Invest in Virus Detectors

5. Network Security

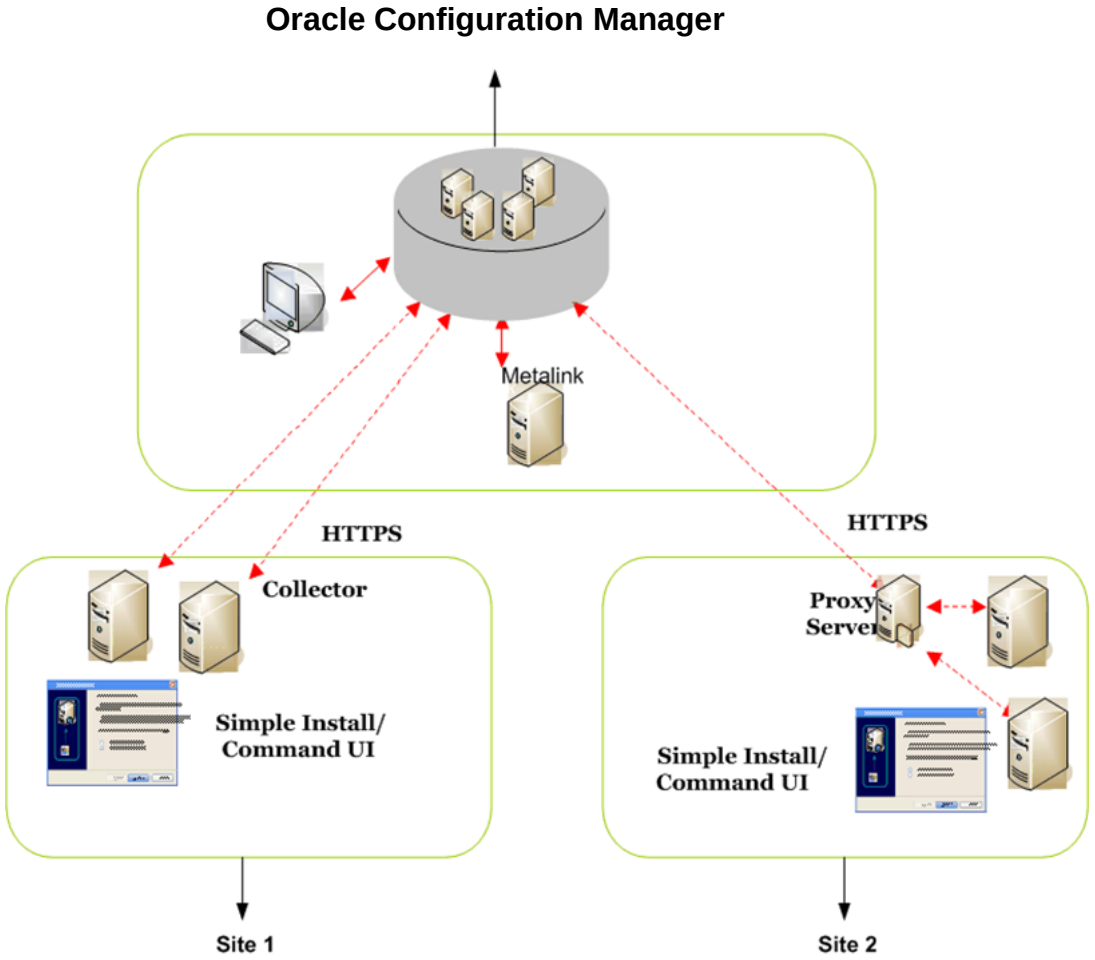
- Ensure Network Can Detect and Withstand Attacks

Network Security Defense

- Zero Trust Approach
- Firewalls
- Safeguard *Internal* Network
- Malware Prevention and Detection
- Subsystems
- Test
- Monitor

6. Secure Configuration

- Secure the Perimeter and Plug Loopholes



Secure Configuration Strategies

- Weak Foundation is House of Cards
- Embed Controls
- Retrofitting the System is NOT the Solution
- Patch Vulnerabilities
- Enlist Experts
- Consider Cloud Solution

Poll Question 4:

Please rate the quality of cybersecurity training in your organization.

a. Excellent
b. Good
c. Fair
d. Poor
e. N/A

Poll Question 4 Results: (Placeholder)

7. User Privileges

- Limit Access to a Need to Access Basis

User Privileges Controls

Source: www.tenor.com

- Limit Access
- Periodic Privilege Review
- Set-up Multi-factor Authentication
- Limit High Security Access
- Discipline Violators
- Strong Password Policies
- Maintain Audit Log

8. Incident Management

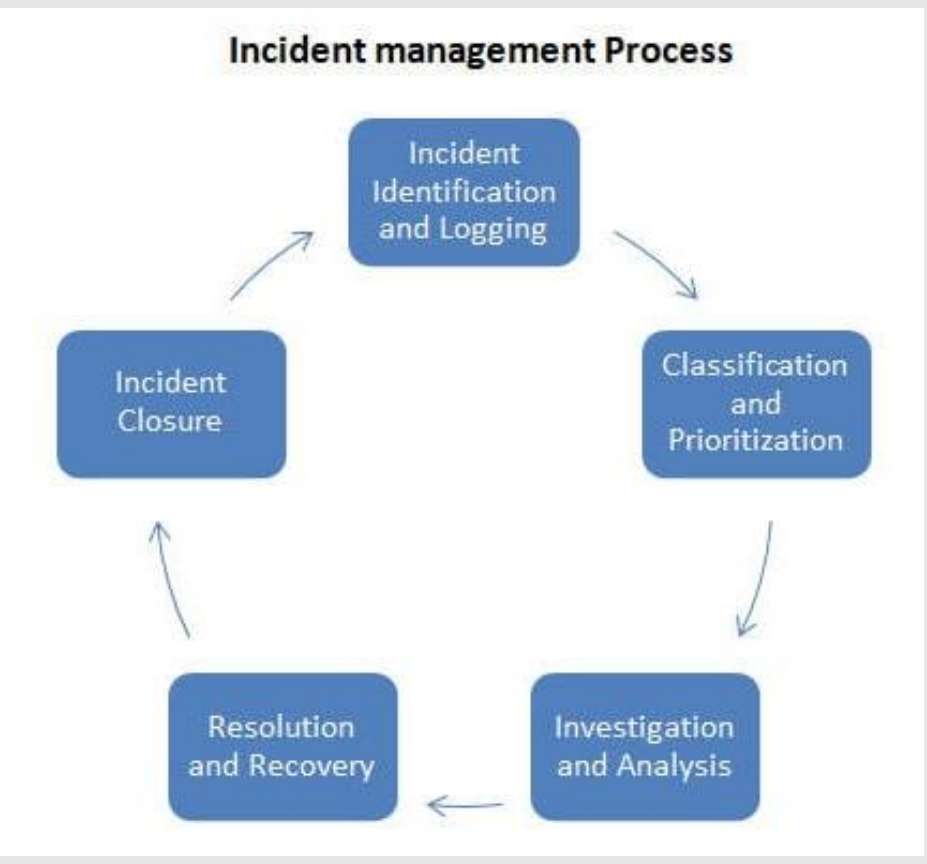
- Manage High-Risk Situations

Equifax 2017 Data Breach

- Failed to Disclose for 5 months
- Cause – Security Vulnerability Patch Not Applied
- Affected 144 Million
- Compromised Names, Social Security numbers, Birth Dates
- Paid $700 Million in Fines

“How does this happen when so much is at stake? I don’t think we can pass a law that, excuse me for saying this, fixes stupid. I can’t fix stupid.”

Representative Greg Walden (R.-Ore.)



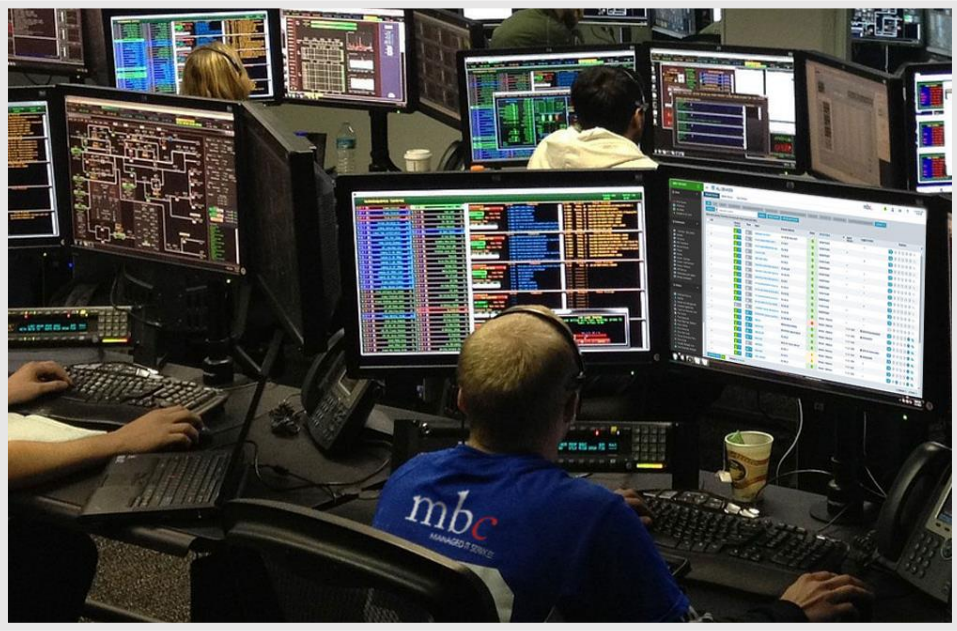
Incident Management Controls

- Set-up Monitoring System
- Establish Detailed Policies, Procedures, and Resources
- Ensure Backups are Reliable
- Run Drills

Source: www.softwaretesting.com

9. Monitoring

- Continuously Monitor Threats and Attacks



Monitoring Controls

- Invest in monitoring systems
- Ban prohibited behavior
- Establish policies
- Display a dashboard
- Be prepared to shutdown

10. Update Software

- Apply Software Patches Promptly

Update Software Controls

- Apply Promptly
- Apply Patch Sets (Service Packs)
- THOROUGHLY TEST

Poll Question 5:

Who develops and implements your organization's cybersecurity policies and procedures?

a. Information Technology Department
b. Outside Cybersecurity Consultant
c. Accounting and Finance Function
d. I don't know

Poll Question 5 Results: (Placeholder)

Cybersecurity Frameworks

Cybersecurity Risk Management

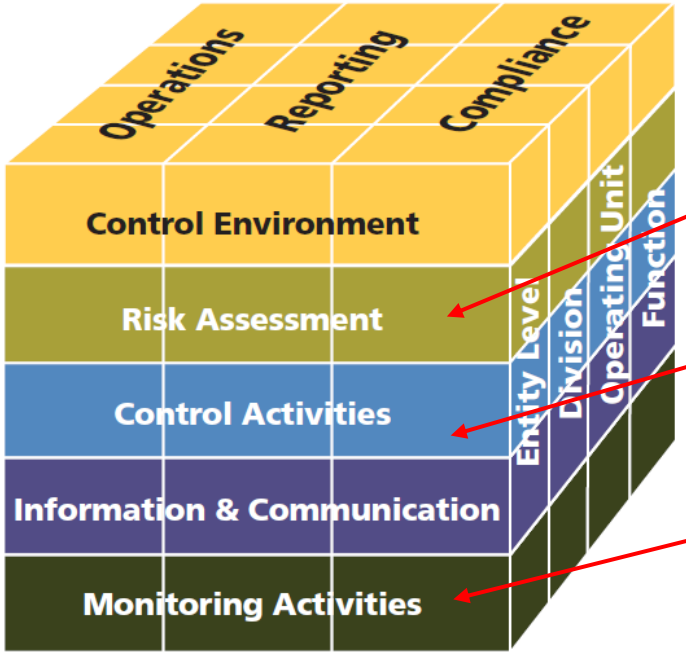
Make Cybersecurity an Organization Priority

Develop, Implement, and Enforce Cybersecurity Controls

Determine Cybersecurity Risk Appetite

Make Cybersecurity a Priority (Or You Will Be Sorry)

Develop, Implement, and Enforce Cybersecurity Controls



Risk Assessment – COSO ERM

Control Activities

Monitoring Activities

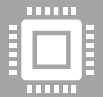
Cybersecurity Risk Assessment

Determine Cybersecurity Risk Appetite

Source: www.safesystems.com

International Organization for Standardization (ISO) 27000 Series

The ISO 27000 series of standards are designed to ***address information security issues***.



ISO 27000 series, particularly ISO 27001 and ISO 27002, have become the **most recognized and generally accepted** sets of information security framework and guidelines.

The main objective of the ISO 27000 series is to **provide a model** for *establishing, implementing, operating, monitoring, maintaining, and improving* an Information Security Management System (ISMS).

U.S. Department of Commerce's National Institute of Standards and Technology Cybersecurity Framework

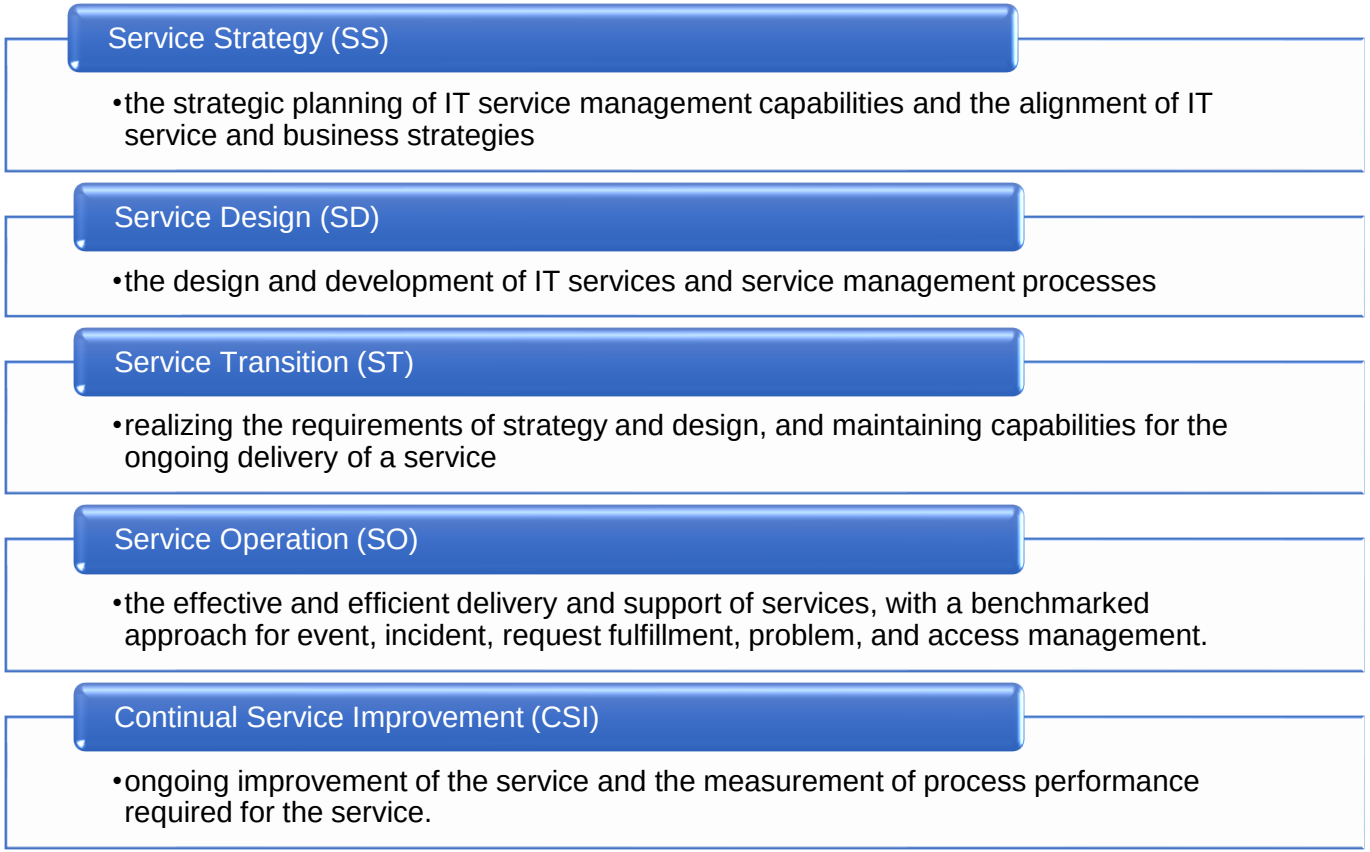
Information Technology Infrastructure Library (ITIL)

A ***de facto* standard in Europe** for the best practices in IT infrastructure management and service delivery.

ITIL's **value proposition** centers on providing IT service with an understanding the business objectives and priorities, and the role that IT services has in achieving the objectives.

ITIL adopts a **lifecycle approach** to IT services and organizes IT service management into five high-level categories.

Information Technology Infrastructure Library (ITIL)



NIST Small Business Corner

SMALL BUSINESS CYBERSECURITY CORNER

- Cybersecurity Basics +
- Planning Guides +
- Guidance by Topic +
- Responding to a Cyber Incident
- Training
- Videos

Your resource for keeping your small business secure.

Get cybersecurity basics, guidance, solutions, and training to protect your information and manage your cybersecurity risks.

Credit: Wendy Szwerc

Key Takeaways

Survival Tips for Management Accountants

Raise Organization's Awareness
Perform a Risk Assessment
Create Cybersecurity Policies and Training
Document Internal Controls
Prepare and Practice a Contingency Plan
Buy Cybersecurity Insurance
Invest in Cybersecurity Detection Tools
Think Smart Using Computer Resources
Education, Education, Education
Look Over Your Cyber Shoulder

Summary and Conclusion

Cybersecurity Resources

- Brands, K. (2021). Cybersecurity From Within. *Strategic Finance*, *102 (8),* 60–61.
- Brands, K. (2020). Creating Cybersecurity Awareness. *Strategic Finance*, *101 (7),* 60–61.
- Brands, K. (2019). Get Smart About Cybersecurity attacks: The time to act on cybersecurity prevention and response planning is right now. *Strategic Finance*, *101(6)*, 60–61.
- ISO 27001 Standard

  ISO 27001
- Security in Computing Fifth Edition Prentice-Hall (Pfleeger, C., Pfleeger, S., and Margulies, J.) 2015
- Small Business Cybersecurity Corner Small Business Cyber Center
- U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF version 1.1)
  NIST Cybersecurity Framework and Small Business Corner

Questions and Answers

Kristine Brands, CMA
Assistant Professor
United States Air Force Academy

Brad Hamilton, CMA, CPA
Co-Owner
Hamilton Accounting Services LLC
Member
IMA Technology Solutions & Practices Committee

Thank You to Our Featured Presenter!

Kristine Brands, CMA

Assistant Professor

United States Air Force Academy

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE


ima22 Accounting & Finance Conference
REIMAGINE
June 12-15, 2022 • JW Marriott, Austin, TX
Registration opens March 8

Final Reminders

- **Complete the Evaluation poll** – 2 options
  - On your screen
  - Evaluation Survey icon at the bottom of your console
- **Access to your CPE Certificate** – 2 options
  - Click the “CPE” icon at the bottom of your console

    or
  - Click the link in your post-event e-mail
- Please print a copy of the CPE certificate for your records.
- Your CPE credit will be automatically recorded in your transcript.

Thank you!

Oracle NetSuite

www.NetSuite.com

ima®

The Association of Accountants and Financial Professionals in Business

ORACLE® NETSUITE