What Management Accountants Need to Know about Ransomware Attacks – *Tech-Talk Mondays*

Kristine Brands, CMA

May 8, 2023

The Association of Accountants and Financial Professionals in Business

ORACLE NETSUITE

Tech-Talk Mondays Title Sponsor

ORACLE®

NETSUITE

www.netsuite.com

Featured Presenter

Kristine Brands, CMA

Assistant Professor

United States Air Force Academy

ima®

The Association of Accountants and Financial Professionals in Business

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.

Learning Objectives

1. Define a ransomware attack and its impact on an organization.
2. Describe ransomware attack risks and trends.
3. Discuss how to develop a plan to prevent a ransomware attack.
4. Identify how to respond to a ransomware attack.

Agenda

1. Introduction
2. Ransomware and How it Attacks
3. Ransomware Risks and Trends
4. Ransomware Attack Examples
5. Ransomware Defense/Best Practices
6. Ransomware Response
7. Conclusion
8. Resources
9. Questions

Introduction

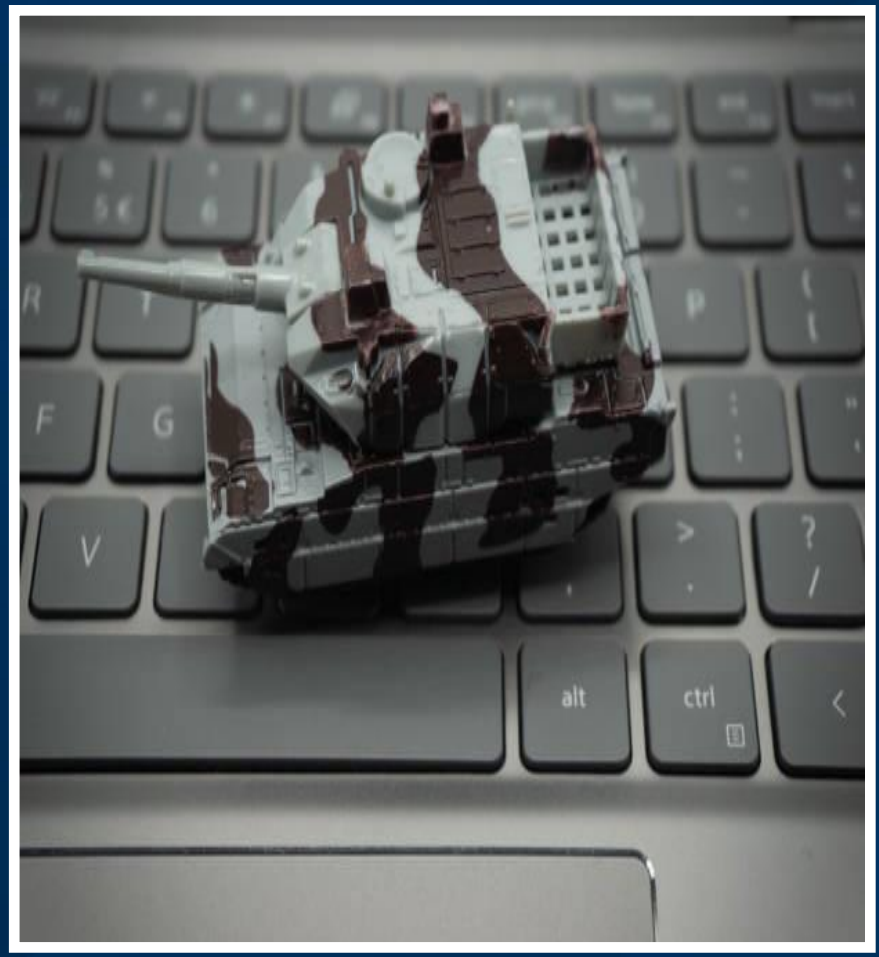
Poll Question 1:

Has your organization been exposed to a Ransomware attack?

a. Yes
b. No

Poll Question 1 Results: (Placeholder)

Calling All Management Accountants to Join the War Against Ransomware Attacks



Ransomware and How it Attacks

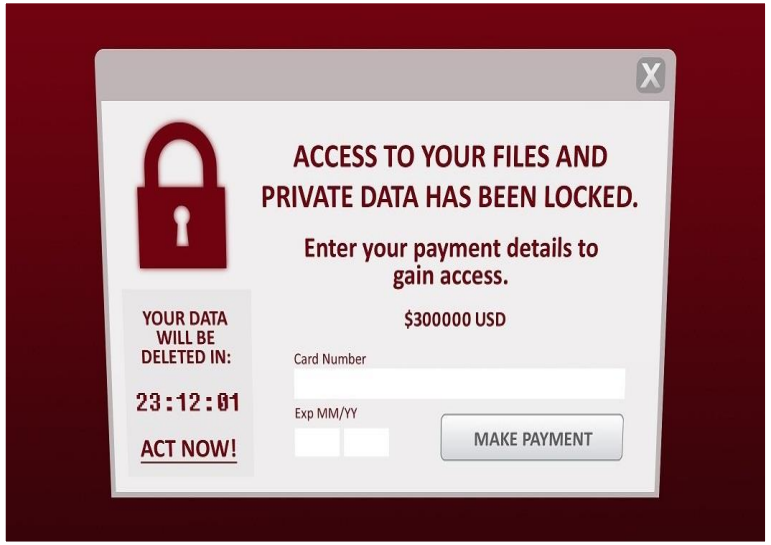
"Ransomware is a type of malicious software, or malware, preventing you from accessing your computer files, systems, or networks *and* demands you pay a ransom for their return.

Ransomware attacks can cause *costly disruptions to operations* and the *loss of critical information and data*."

Source: The US Federal Bureau of Investigation

How Does Ransomware Infect?

- **System is Hacked**
  - User Clicks on Phishing Email Deploying Malware *OR*
  - Credentials are Compromised
- **Frequently "Zero Day Vulnerability"**
- **Ransomware Encrypts and Locks Files**
- **Ransomware $$$ Demand Made**



Poll Question 2:

Does your company have internal controls/procedures to safeguard against Ransomware attacks?

a. Yes
b. No
c. N/A

Poll Question 2 Results: (Placeholder)

Ransomware Entry Points

- **Login Credentials:** Weak passwords, etc.
- **Phishing:** Opening suspect emails and/or links
- **Exploitable Vulnerabilities:** Lack of data encryption or gaps in authorization requirements
- **Botnets:** Network of computers infected with malicious software as a result of outdated operating systems

Lifecycle of a Ransomware Attack

Attack

Negotiation

Post-Event

Discovery

Settlement

Source: www.experian.com

Terminal Lifecycle Risk - Bankruptcy

60% of small businesses suffering a ransomware attack go out of business

- **Code Spaces**
- **The Heritage Company**
- **Wood Ranch Medical**
- **United Structures of America, Inc**

Ransomware Risks and Trends

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

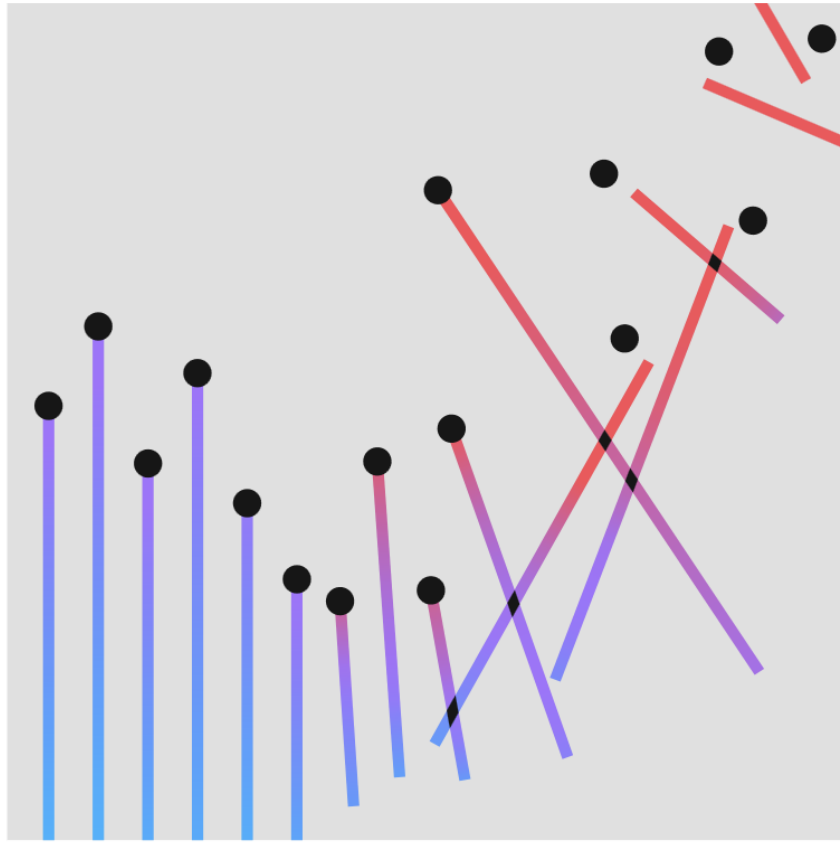
Richard Clarke, the former National
Coordinator for Security, Infrastructure Protection, and Counterterrorism for the United States

IBM's 2022 Cost of a Data Breach Report

- **Average Cost of Breach - $9.4 Million US (2 Times Global)**
- **Average Time to Identify and Contain – 277 Days**
- **Average Cost or Ransomware Attack– US. Average $4.54 Million**
- **Costliest Industry – Healthcare**

Source:IBM Cost of a Data Breach Report 2022

Cost of a Data Breach Report 2022



IBM

Data Breach Costs According to IBM

- **Detection and Escalation**
- **Notification**
- **Lost Business**
- **Post Breach Response**
- **And Don’t Forget Reputation**

Verizon's 2022 Data Breach Investigations Report

- Ransomware Increased 13%
- People Cause 85% of Breaches
- Errors as Cause Dropped (21% to 17%)
- Supply Chain Compromises are Major Risk

Source: https://www.verizon.com/business/resources/reports/2022/2022-dbir-executive-brief.pdf

The Gartner Group – 2023 Trends

- **Attack Surface Growing**
- **Identity System Defense**
- **Digital Supply Chain Risk**
- **Increased Vendor Consolidation**
- **Cybersecurity Mesh**
- **Distributed Decisions**
- **Beyond Awareness**

Source: Gartner Group Top Trends 2023

Ransomware Attack Colonial Pipeline May

- 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 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**

Ransomware Attack - August 2019

- Shutdown Jesuit University in Denver, CO at Semester Start
- Backup Data Compromised
- Paid Ransomware (Problems Continued After Ransomware Payment)

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

Russian Ransomware Attacks

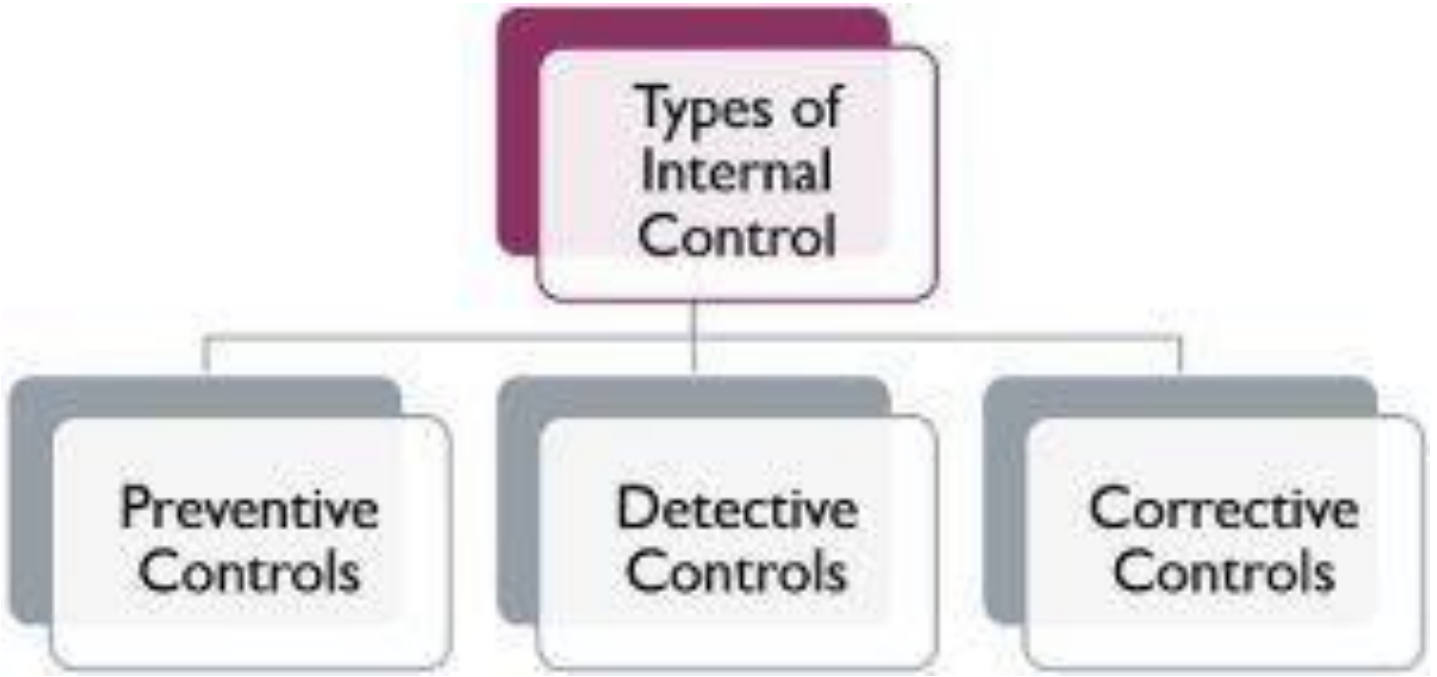
“Russian Ransomware Hackers Pledge Support to Putin and Immediately Have Secret Chats Exposed by Ukrainian Leaker” (Source: Currently from AT&T)

- **Group - Conti Ransomware Gang (2020)**
- **Ransomware-as-a-service**
- **Inception to Date “Revenue” $180 Million**
- **Disbanded 2022**

Ransomware Defense Best Practices

Source: https://info.mooredm.com

Internal Control Triad



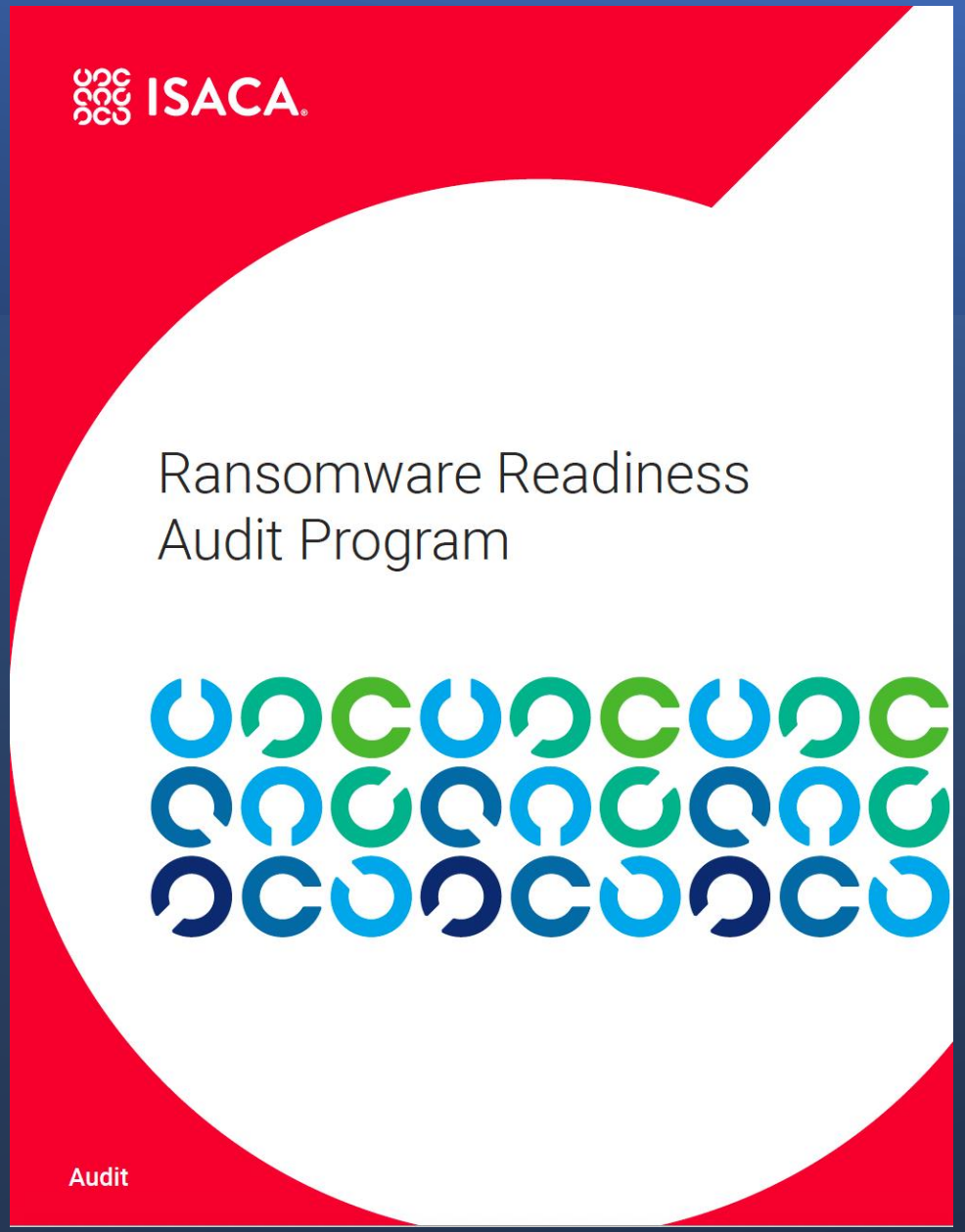
$ $$$$ $$$$$$

Network Security Defense

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

Zero Trust

A security model based on the premise that no one is blindly trusted and allowed to access company assets until they have been validated as legitimate and authorized



ISACA Ransomware Readiness Audit Program

Ransomware Readiness Audit Program

Sections: Governance, Information Protection, Technical Safeguards, Human Safeguards

Process Sub-Area	Reference Risk	Control Objectives	Controls	Control Type	Control Classifica-tion	Control Frequency	Testing Step	COBIT 2019	Other frameworks/ standards	Reference Workpaper	Pass/ Fail	Comments

Ransomware Readiness Audit Program
Section/Objectives

Governance

- Ransomware Strategy/Policy
- Risk Assessment

Information Protection

- Asset Inventory and Management
- Data Inventory and Management
- Operational Processes

Poll Question 3:

Please evaluate your company's training for Ransomware attacks?

a. None
b. Fair
c. Good
d. Excellent
e. N/A

Poll Question 3 Results: (Placeholder)

Ransomware Readiness Audit Program Section/Objectives

Technical Safeguards

- Device Security
- Patch Management
- Intrusion Detection/ Prevention System
- Forensic Capabilities
- Architecture and Configuration

Human Safeguards

- User Awareness and Training
- Group Responsibilities
- Individual Roles/Responsibilities

Implement Ransomware Policy

- **Keep operating systems, software, and applications up to date**
- **Apply all patches promptly**
- **Automatically update anti-virus and anti-malware solutions software and run programs**
- **Back up data regularly and be sure backups completed**
- **Secure backups and store apart from system backed up**
- **Create a continuity and response plan and run a drill**
- **Create and implement cybersecurity and ransomware internal controls**

Monitor Intrusion Metrics

Poll Question 4:

Does your company have a plan to recover from a Ransomware attack?

a. Yes
b. No
c. Don’t Know
d. N/A

Poll Question 4 Results: (Placeholder)

Implement Ransomware Policy

- **Configure JavaScript, Windows Script, and HTML to Open to Notepad**
- **Disable ISO File Extensions in Microsoft Windows Explorer**
- **Restrict Remote Desktop Protocol Directly to the Internet (for Unneeded Services)**
- **Disable Macros in Downloaded Files**
- **Implement Zero Trust Security Model**
- **Perform Ransomware Readiness Program**

Continuous Monitoring

Automate

Train Cybersecurity Staff

Ransomware Attack Response


KEEP
CALM
AND
PULL THE
PLUG

Two-Prong Response Strategy

Source: Microsoft Ransomware Response Playbook

Containment and Investigation

Containment

- Assess Scope
  - Where Did it Originate
  - What was Affected
- Protect and Preserve Systems
  - Disconnect Backups
  - Freeze Access
  - Reset all Access (Passwords)
- Prevent Spread

Investigation

- Assess Situation
  - How Did You Find Out?
  - Identify Date/Time
    - What was Attacked?
    - What Programs Were Running?
  - Is Attacker in System?
- Identify Ransomware Process
- Identify Compromised Credentials?
- What Programs/Apps Disabled?

Eradication and Recovery

Eradication

- Verify Backups
- Block Attackers
- Reset Compromised Users
- Isolate Attacker Control Points
- Remove Malware

Recovery

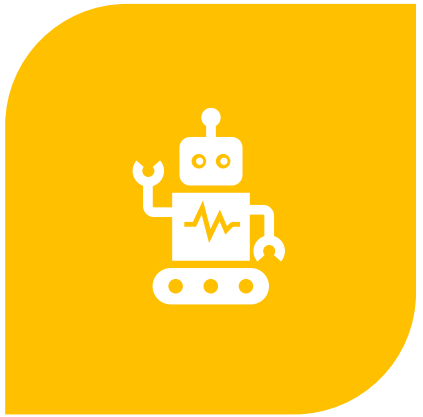
- Recover Files on Clean Device
- Recover Deleted Email

Conclusion and Homework

Pillars of Cybersecurity

INTEGRATION

CONTEXT



AUTOMATION

Remember…

- Don’t Pay Ransomware
- Automate Malware Detection
- Develop Cybersecurity Talent
- Implement Cybersecurity and Ransomware Policies
- Engage a Consultant
- Be Vigilant

Share Experiences

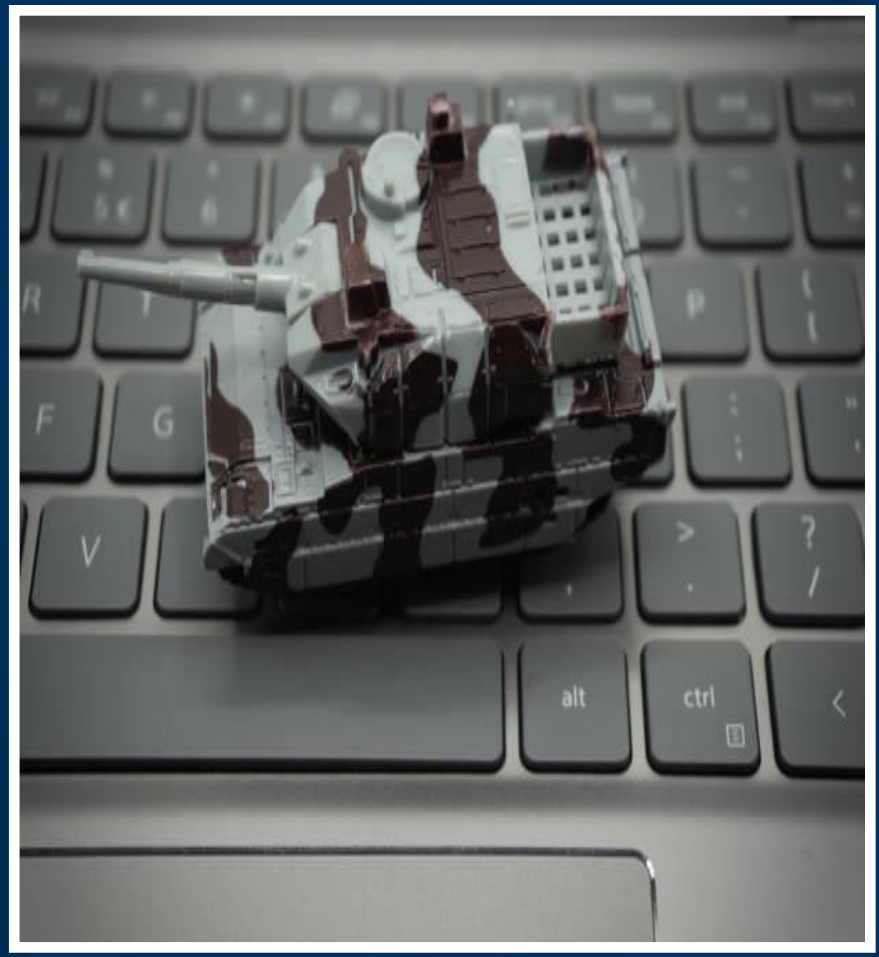
"Even five years ago, an organization that was attacked wouldn't tell anybody. There was the idea that you can't publish what has happened to you because it shows you're vulnerable. It's become so prevalent that if you don't band together, you're going to have a real tough time combating this."

Shari Plantz-Masters, Dean of Anderson College of Business and Computing

“There’s No Silver Bullet for Cybersecurity”

Thomas P. Vartanian
Harvard Business Review
April 23,2023

Calling All Management Accountants to Join the War Against Ransomware Attacks



Resources

Resources

- Cybrary - LTC Brad Rhodes, Army Reserve Cyberwarfare
- FBI - How We Can Help You
- ISACA Ransomware Readiness Audit Program
- Stop Ransomware (CISA)
- Washington Post Cybersecurity 202 Newsletter
- US Cybersecurity & Infrastructure Security Agency

ISACA

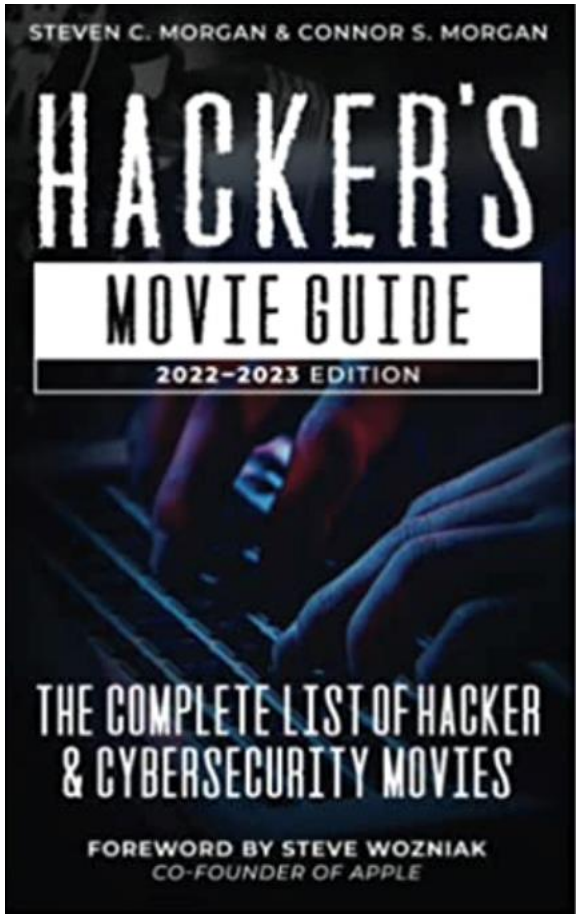
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

STOP RANSOMWARE

Strategic Finance

- Blockchain Implementation and Cybersecurity
  - Smith, Sean Stein, Mar2023
- Creating Cybersecurity Awareness
  - Brands, Kristine, Jan2020
- Get Smart About Cybersecurity Attacks
  - Brands, Kristine, Dec2019
- Implementing Cybersecurity
  - Murphy, Glenn, Jul2021
- Security Breaches: Are You Ready?
  - Hare, Sean, Apr2019
- Strategic Management of Cybersecurity Risks
  - Frigo, Mark l.; Guccione, Darren, Jan2022

Watch Sci Fi and Hacking Movies



- Source: [Cybercrime Magazine]

Questions

Thank you!

Oracle NetSuite

www.netsuite.com

The Association of
Accountants and
Financial Professionals
in Business

ORACLE®
NETSUITE