# Information Assurance

# Capraro Technologies, Inc. (CTI)

**Based on a DoD Briefing & Modified and Maintained by Capraro Technologies, Inc.**


capraro technologies inc.

CRI CYBER RESEARCH INSTITUTE

# Topics

- Information Assurance (IA) – General Overview
- Information Assurance – more detail
- Hacking tools and techniques
- Social Media
- Questions

# Information Assurance (IA) General Overview

# Basic Elements for IA

- Risk Assessment
- Policy and Procedures
- Education
- Backup and Disaster Recovery
- Emergency Mode Operation

# Risk Assessment-1

- **1. Identify information assets.** e.g., Social Security numbers, payment card numbers, patient records, designs, human resources data -- make a priority list of what needs to be protected
- **2. Locate information assets** list where assets reside e.g., file servers, workstations, laptops, removable media (e.g. thumb drives, CDs), smartphones, databases, file cabinets, etc.

# Risk Assessment-2

- **3. Classify information assets.** Consider a 1-5 scale, with the following categories:
- *1* - Public information e.g., marketing campaigns
- *2* - Internal, but not secret, information e.g., phone lists, organizational charts, office policies, etc.)
- *3* - Sensitive internal information (e.g., business plans, strategic initiatives, items subject to nondisclosure agreements, etc.)
- *4* - Compartmentalized internal information (e.g., compensation information, layoff plans, etc.)
- *5* - Regulated information (e.g., patient data, classified information, client sensitive data, credit card data, etc.)

# Risk Assessment-3

- **4. Conduct a threat modeling exercise.** Rate the threats that top-rated information assets face e.g.
  - **STRIDE:** **S**poofing of Identity
    **T**ampering with Data
    **R**epudiation of Transactions
    **I**nformation Disclosure
    **D**enial of Service
    **E**levation of Privilege
- **5. Finalize data and start planning.** Multiply all the cells in each of the worksheets by the classification rating assigned to the asset in Step 3. The result is a rational and comprehensive ranking of threats to the organization.

# Policy and Procedures

- Emphasize the Importance of Cyber Security
- Teach Effective Password Management
- Detect Phishing and Other Scams
- Apply Updates and Patches
- Protect Sensitive Information
- Lock Computers and Devices
- Secure Portable Media
- Report Lost or Stolen Devices
- Take Active Role
- Apply Privacy Settings

# Education

- The first “Firewall” of any organization is the individual Therefore they need to be smart in many areas: e.g.
  - Opening unsolicited email attachments without verifying source and content
  - Executing games, screen savers, or programs from un-trusted sources
  - Failing to install patches, especially for Microsoft
  - Leaving default passwords on or near your computer
  - Visiting unknown web sites
  - Downloading tool bars
  - Downloading Apps from unknown developers
  - Not securing computer systems

# Backup and Disaster Recovery Systems

- Backup files to hard drives – take off site nightly
- Backup files to the Cloud
- Create virtual machines (VM) and backup to the Cloud
- Backup gas or diesel generators
- Multiple fiber Internet connections
- Use of Storage Area Network (SAN) devices with replications made locally and in the Cloud

# Emergency Mode Operation

- Building is not accessible – how long can you go without your computers, applications and files?
  - Where will you go with your staff?
  - Are all your machines virtualized and accessible in the Cloud?
  - Do all your staff have computers and Internet connections from their homes?
  - Can you reroute faxes and telephone calls to another operable location?
  - Do you have a plan – possibly with another organization across town to share resources in case of an emergency?

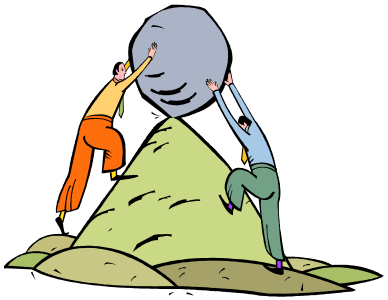
# Summary

- Risk Assessment
- Policy and Procedures
- Education
- Backup and Disaster Recovery
- Emergency Mode Operation

# Information Assurance (IA)

# Three Basic Facts

- Our jobs rely on accurate, accessible information
- Need to identify information correctly and safeguard appropriately
- Need to balance the accessibility of information with the need to adequately safeguard information



capraro technologies inc.

CRI CYBER RESEARCH INSTITUTE

# What is IA?

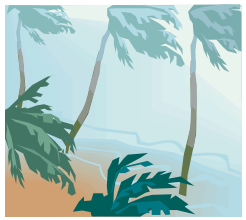
- Measures that protect and defend information and information systems
- IA is really just a collection of methods to provide a risk management approach

# Risk Management

- Risk management means
  - Identifying assets
  - Identifying threats and vulnerabilities
  - Identifying impact
  - Providing risk mitigation

# Threats to IA

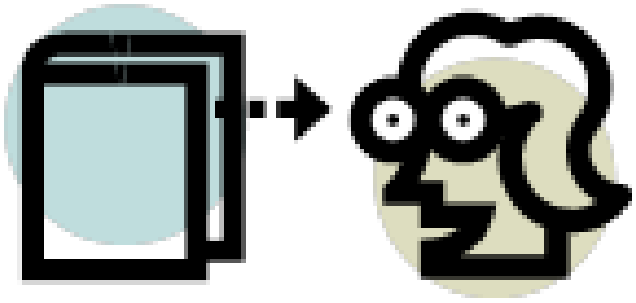
- Threat Categories
  - Natural Threat
    - Natural Events – Fire, hurricane, flood
    - System Environment – Faulty wiring, insufficient HVAC



  - Human Threat
    - Internal – Disgruntled employees
    - External – Spies, hackers

# Information Protection

- Information protection such as security classification, Company Proprietary, Privacy Act, etc.
- Data accuracy, quality, and currency
- Authoritative source
- User training
- User authentication
- Roles and permissions
- Need-to-know



# System Protection

- Password protected
- Biometrics
- Email policy
- Regular back-ups

- Software Information Assurance Vulnerability Alerts (IAVAs)
- Virus Protection
- Firewalls

# Passwords

- **The longer the password, the harder it is to crack.** Consider a 12-character password or longer.
- **Avoid names, places, and dictionary words.**
- **Mix it up.** Use variations on capitalization, spelling, numbers, and punctuation.
- **Include special characters** such as (,&,%,[,}, etc
- **Substitute special characters for letters** e.g. 3 for e, 0 for O, 1 for l, etc.

# One Technique for Generating Passwords

- [PlpiUpMoToOs@ThGrSt] = Please pick up more Toasty O's at the grocery store.  “Toasty O’s”\
- (NoIfY0BaL3Y0AnYoHaN0P1T0Dw) = Now if your baby leaves you and you have no place to dwell. Heart Break Hotel  “Hotel”
- |HiDiD0ThM0RaUpThC1ThC1Sr0n| = Hickory dickory dock the mouse ran up the clock the clock struck one – “Mouse”

# Second Technique for Generating Passwords

# Worst Mistakes End-Users Make

- Failing to install or keep anti-virus software up-to-date; failing to apply anti-virus to all files
- Opening unsolicited email attachments without verifying source and content
- Executing games, screen savers, or programs from un-trusted sources
- Failing to install patches, especially for Microsoft
- Not making and checking backups
- Not installing the security features of your computer and/or network
- Leaving default passwords on or near your computer

# Hacking Tools and Techniques

# Keystroke Logging

- A keylogger program does not require physical access to the user's computer.
- It can be downloaded on purpose by someone who wants to monitor activity on a particular computer or

  it can be downloaded unwittingly as spyware and executed as part of a rootkit or remote administration (RAT) Trojan horse.
- A keylogger program typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file (which does all the recording) and an executable file (.EXE) that installs the DLL file and triggers it to work.
- The keylogger program records each keystroke the user types and uploads the information over the Internet periodically to whoever installed the program.

# Social Engineering

- Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information (e.g. your mail box is full please click here for a fix or call this number for help)
- It is the act of tricking another person into providing information by posing as an individual or agency that is authorized to receive that information or authorized to perform some task
- Techniques may be human or electronic
- Spoofing caller IDs and Short Msg Service (SMS) numbers e.g. https://www.spooftel.com/

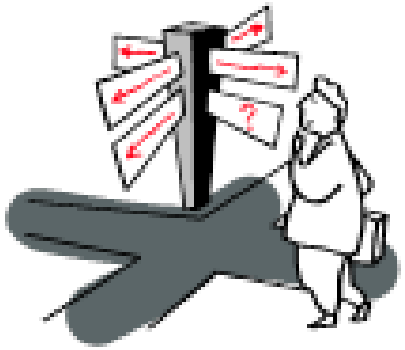
# Phishing

- Phishing
  - Via email or personal interaction
  - Phishing emails not only attempt to trick you into giving out sensitive information, but also can include malicious software
  - A hacker may attempt to gain system information from an employee by posing as a service technician or system administrator with an urgent access problem
- Spear Phishing (Business Email Compromise (BED*)) is a highly targeted phishing attempt
  - The attacker selectively chooses the recipient (target – i.e. YOU) and usually has a thorough understanding of the target's command or organization
  - The email may appear very genuine
    - Address the recipient by name
    - Use lingo/jargon of the organization
    - Reference actual procedures or company policy and Instructions

*Austria $50M

# Pharming

- Pharming
  - A hacker's attack aiming to redirect a website's traffic to another, bogus website
  - Pharming can be conducted either by changing the host's file on a victim's computer or by exploitation of Domain Name Service (DNS) server software
    - DNS servers are computers responsible for resolving Internet domain names into their real addresses
  - Both pharming and phishing have been used for online identity theft information



# Worms

- Worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code.
- Worms utilize networks to send copies of the original code to other computers, causing harm by
  - consuming bandwidth
  - deleting files
  - sending documents via email
  - install backdoors on computers
- The Morris worm caused hundreds of thousands, if not millions, of dollars in damage, and its creator was convicted under the Computer Fraud and Abuse Act.
- Common modes of connected transport include attachments, file sharing networks and links to infected websites.

# Virus

- Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation
- A computer virus might
  - corrupt or delete data on your computer,
  - use your email program to spread itself to other computers,
  - erase everything on your hard disk.
- Spread by attachments in email or instant messaging messages.
- Disguised as attachments of funny images, greeting cards, or audio and video files or via downloads from the Internet or hidden in software (a form of steganography)

# Adware & Spyware

- Adware is any type of program that downloads or displays unwanted banner advertisements in the software being used.
- Adware is often bundled with software: to recover development costs, or to be able to provide the product for free or at a discounted price.
- Adware can be designed to collect data on which sites the user visits, send this data back to the company and deliver advertising based on the information. (e.g. early pregnancy – shopping card)
- Adware can also contain or be classified as spyware, a type of malware that can steal a user's information or corrupt the user's system files.
- Because of privacy concerns and the prospect of malicious adware, most antivirus software detects and removes both adware and spyware.

# Malicious Mobile Code

- Malicious mobile code is a way to get malware installed on a computer.
- It is malware (any malicious code e.g. spyware, virus, etc.) that is obtained from remote servers, transferred across a network, and then downloaded on to your computer.
- Can be transmitted through interactive Web applications using vulnerabilities within ActiveX controls, Flash animation, or JavaScript
- Must keep your system upgraded with security patches to control damage to your systems

# Ransom Ware $$$$$

- Software that takes control of your computer until a ransom is paid
- Gains control via phishing emails, un patched programs, compromised websites, “’poisoned” online advertising and free software downloads
- Encrypts files on a workstation then it may travel across your network and encrypt any files located on both mapped and unmapped network drives bringing to a halt a total organization (acts as a virus)
- Most ransoms start at $300-$500 area, and once the deadline has passed it will likely increase to over $1000
- http://sanfrancisco.cbslocal.com/2016/02/18/california-hospital-ransomware-attack-hackers/ $17K
- Ransomware called WannaCry shut down 65 hospitals in the United Kingdom, and affected not just computers but storage refrigerators and MRI machines (May 2017).

# Not So High Tech

- Dumpster Diving
  - As the name implies
  - Someone goes through the dumpster or trash looking for personal information
    - Credit card receipts, check stubs, billing information

# Ways to Protect Yourself

- When in doubt, check it out
- If you receive an email or offer that seems too good to be true, it probably is
  - Foreign dignitary offering you millions to temporarily hold in your bank account, if you send account information
- Don’t know the sender?  Don’t open it until you check via another method (e.g., phone) or delete it
- Email from your bank asking for account verification? Not likely. Reputable businesses will not ask you for personal information in an email
- Change passwords often and make them long and hard

# Social Media/Social Networking Sites

# Social Media

- Web-based services
- Communities of people who share common interests
- Web interfaces that encompass one or more means of communication
- A shift in how people discover, read, and share news, information and content; transforming monologues (one-to-many) into dialogues (many-to-many)




# Why is Social Media so Popular?

- Virtually anyone can join
- Accounts can be created quickly (5 min or less)
- Most are free and don't bind user to a contract
- Convenient interface for users to add or update content on their profile
- Users can share as much or as little as desired
- Easy to connect with friends and family
- "Privacy settings" available on most sites

# Social Media: Security Concerns

- Impersonation of a friend or colleague can be used to trick users into providing private information or downloading malicious third party applications
- Users can share a variety of multimedia content, from images to video clips to documents. This content has the potential to contain malicious code, which under the right circumstances may cause the user's browser to download malware or perform unintended actions
- Much information might be available through a professional profile such as LinkedIn
- Participation in online discussion groups or blogs might help foreign intelligence services or competitors to single out disgruntled employees who could be recruited or blackmailed

capraro technologies inc.

CRI CYBER RESEARCH INSTITUTE

# Social Media: a Related Concern

- Social Networking Sites' Data Use Policies
  - "What they know about you and who they share it with"
  - Privacy policies
  - Dossiers of on-line activities
  - Your account information is stored on servers in the internet "cloud" so the company owns that information, not you
    - Can be retrieved by a subpoena
- Most successful internet companies have been those that collect information about users and use that information to sell things
- For every User ID, Facebook keeps a log of the IP address that accessed the account, the date and time, and what exactly the user did – clicking on an ad, looking at someone else's profile, posting a photo, sending a message, etc.

Source: Washington Post, Where web sites see all – and tell all, too, May 29, 2010

# Some Social Media Protections

- Consider restricting access to your profile
  - Don't allow strangers to learn everything they can about you
- Keep your private information private
  - Never post your full name, SSN, address, phone number, financial information, or schedule (e.g. Its beautiful here check out the sunset over the Pacific)
  - These will make you vulnerable to identity thieves, scams, burglars, or worse
- Choose a screen name that is different from your real name
  - Avoid using any personal information that would help someone identify or locate you offline
- Think twice before posting your photo
  - Photos can be used to identify you offline
  - They can also be altered or shared without your knowledge

- Don't post information that makes you vulnerable to a physical attack
  - Revealing where you plan to meet your friends, your schedule, or your street address is almost an open invitation for someone to find you

# Some Social Mitigations – Technical

- Keep your Operating System and web browser up-to-date with latest patches
- Keep virus scanners up-to-date with latest definitions and patches, and scan often
- Refrain from browsing the Internet from privileged accounts (e.g., Administrator, root)
- Click the Logout/Logoff button instead of closing your browser session (XSS, session hijacking)


- Consider clearing your web cache and cookies after browser sessions (XSS)
- Beware of URL shorteners (malicious links)

bit.ly

TinyURL.com

**OneDrive**

Goo.gl

capraro technologies inc.

CRI CYBER RESEARCH INSTITUTE

# Some Social Mitigations – Behavioral

- Perform a risk assessment before posting information about you or your organization
- Confirm connection requests either verbally or face-to-face
- Be selective of third-party applications to add to profile
- Be suspicious of emails from social networking sites

# Remember 1:

- Use your common sense
  - If you are contacted by a stranger on-line, find out if any of your established friends know the person, or run an on-line search on them
  - If something seems too good to be true, it probably is
- Trust your instincts
  - If you feel threatened or uncomfortable during an on-line interaction, don't continue
  - Report any offensive or suspicious behavior to the appropriate persons or agencies
- Be suspicious
  - Don't take any information you receive from a new on-line contact at face value
  - The Internet makes it easy for people to say or do things they would never say or do in public or face-to-face interactions

***Protecting yourself is the smart thing to do!***

capraro technologies inc.

CRI CYBER RESEARCH INSTITUTE

# Remember 2:

- Nothing posted on social media can be completely deleted.
- Using social media while on public Wi-Fi hotspots allows for it to be accessed by anyone utilizing that hub.
- Profile information creates a goldmine of info for hackers, the kind of data that helps them personalize phishing scams.
- Everything you place in your profile – personal preferences, political opinions, social commentary and more – is exposed even if you control the privacy settings.

# Remember 3 Cover up your camera

- 17 UK hackers - arrested for using malware to capture nude pictures of Miss Teen USA using her webcam.
- The hackers allegedly used a remote access tool (RAT) called Blackshades Remote Access Tool
- Blackshades RAT sends a seemingly innocent link via a social media and when the victim clicks on the link, their computer downloads malware that initiates a keylogger, grants the hacker access to stored documents and activates the webcam.
- Some use the victim's images as ransom, threatening to release the pictures to the world unless they are paid (usually in Bitcoin).

# Shodan an IoT Search Engine

- Looks for servers, webcams, printers, routers and any device connected to the Internet
- Searchers have found control systems for a water park, a gas station, a hotel wine cooler, a crematorium command and control systems for nuclear power plants, and a particle-accelerating cyclotron
- A quick search for "default password" reveals countless printers, servers and system control devices that use "admin" as their user name and "1234" as their password (e.g. http://www.defaultpassword.com/). Some systems require no credentials at all -- all you need is a Web browser to connect to them.

# No One Is Immune From Being Hacked in US

- Total Records Breached: 1,073,490,127 records from 7,730 Data Breaches made public since 2005 (General)
- MED Records Breached: 48,073,014 records from,3,798 Breaches
- EDU Records Breached: 15,933,122 records from 798 Breaches
- GOV Records Breached: 189,320,445 records from 763 Breaches*
- https://www.privacyrights.org/

* I was one of them

# QUESTIONS?

**Remember the first line of protection is you, the human firewall!**

capraro technologies inc.

CRI CYBER RESEARCH INSTITUTE