
CAUTION
You are NOT allowed to do ANYTHING that begins with the words, "Hey y'all, watch this!"
CAUTION
Danger Area
Proceed With Care And Knowledge
[PROCESSING]
//HACK ATTEMPT FAILED
CONNECTED
USER SAFE
//SCAN
12.123.8234

32nd Annual Carolinas Payroll Conference

Welcome

Roger Swanson
Executive Account Manager

AT-NET Services

AT-NET Services

Application Development | Collaboration | Data Center Virtualization | Infrastructure & Security | Managed Services | Network Infrastructure | Unified Facilities

CYBER SECURITY FOR NON-TECHNICAL EXECUTIVES AND DECISION MAKERS

32nd Annual Carolinas Payroll Conference

Welcome

Roger Swanson
Executive Account Manager

AT-NET Services

Cyber Security for Non-Technical Executives

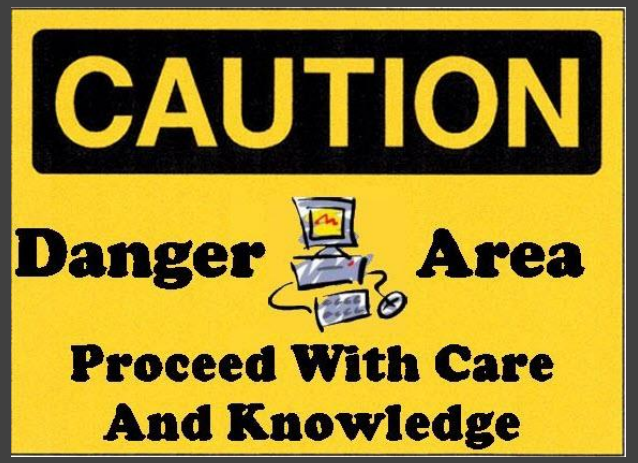
Summary: These slides describe basic overview of Cyber Security

Audience: These slides are intended for an audience who is somewhat familiar with the components and high-level objectives of the Cyber Security.

Learning Objectives: Overview of Cyber Security, review major components of basic Cyber Security topics, Discuss terms, with high level overview of NIST Framework

Cyber Security for Non-Technical Executives

1. Threats, Vulnerabilities, Cyber Risks (CIA-Confidentiality, Integrity, Availability)
2. What steps to take for basic cyber protection, Owner/C-Level responsibilities
3. Training staff, Social Engineering and attacks on your staff
4. Business Continuity planning, are you able to sustain a companywide incident
5. Frameworks for your security policy/plan
6. Risk Analysis, Business Impact Analysis, how RA/BIA interact with Disaster Planning
7. Backing up your information, HOSTING Services and security management
8. Actions to protect yourself and business from being scammed

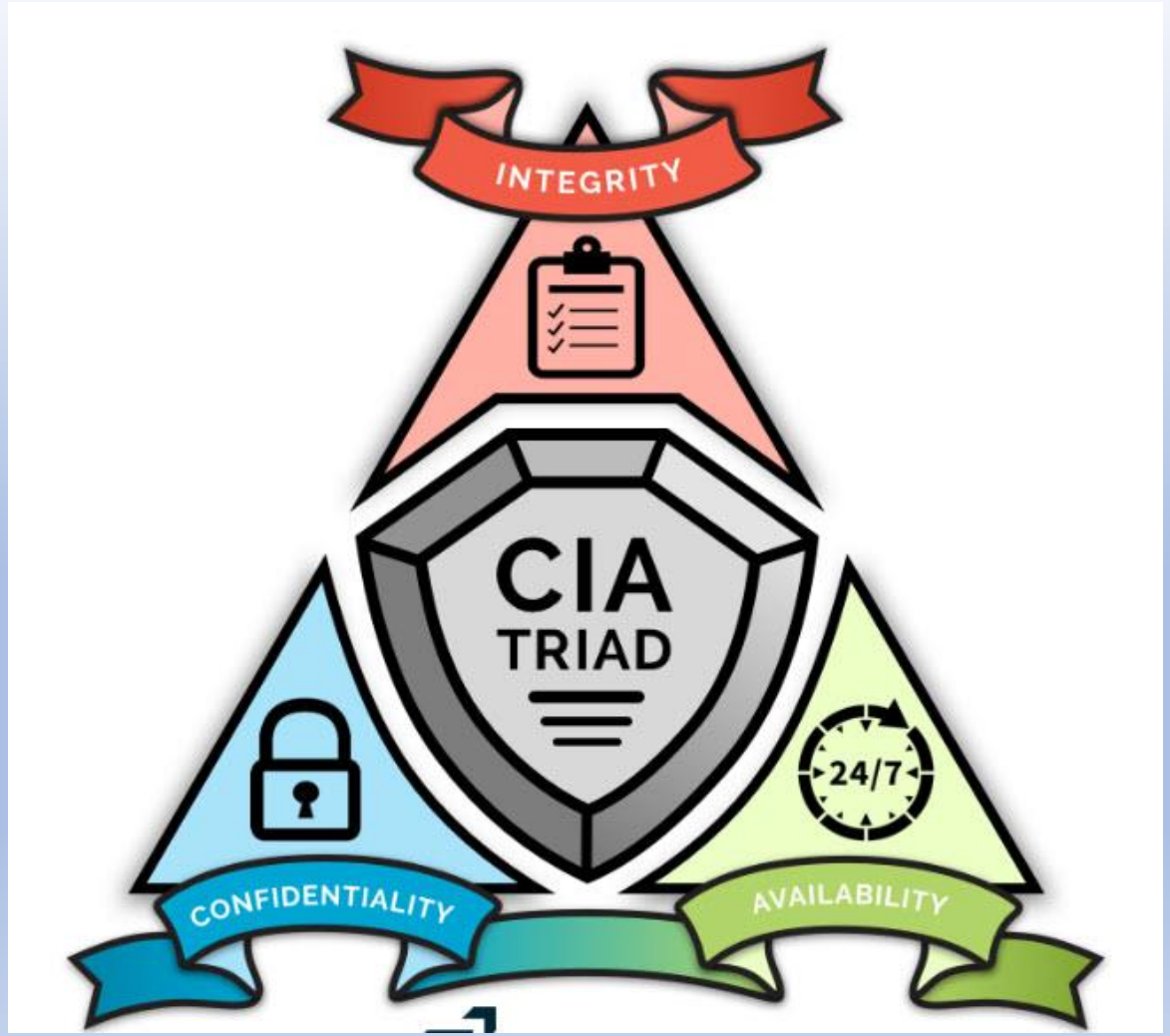

CAUTION
Danger Area
Proceed With Care
And Knowledge

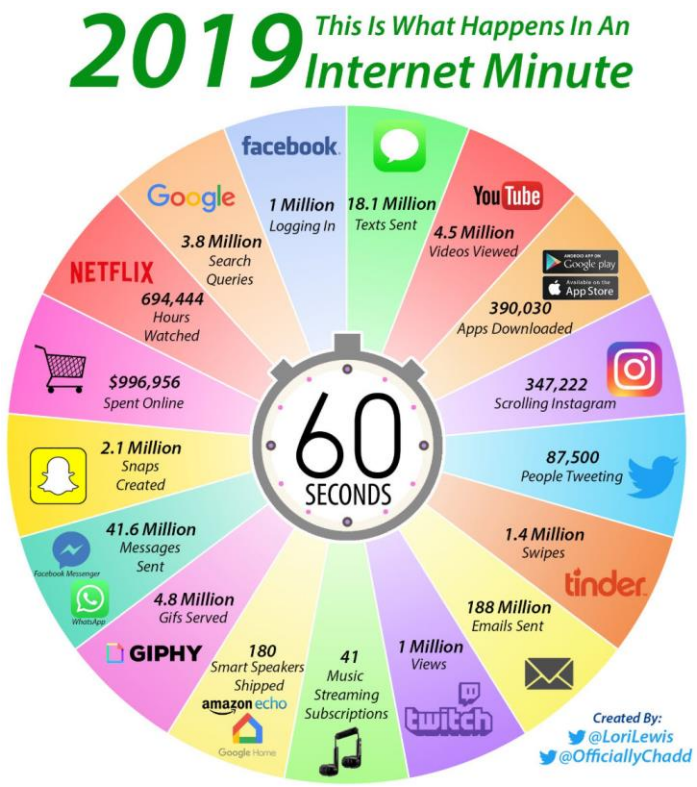

System Protected


Data Breach
Cyber Attack

Objectives for Presentation:

1. Threats, Vulnerabilities, Cyber Risks (CIA-Confidentiality, Integrity, Availability)

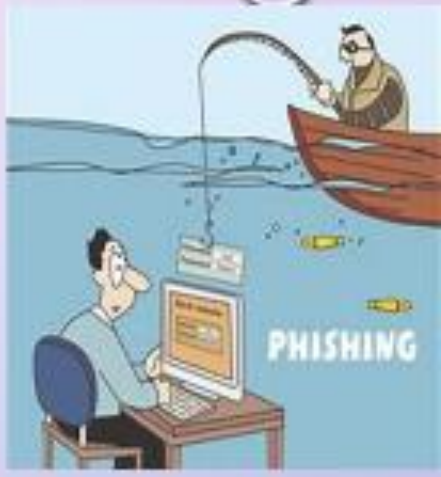




One Internet Minute 2017-2019

How do criminals get my information?

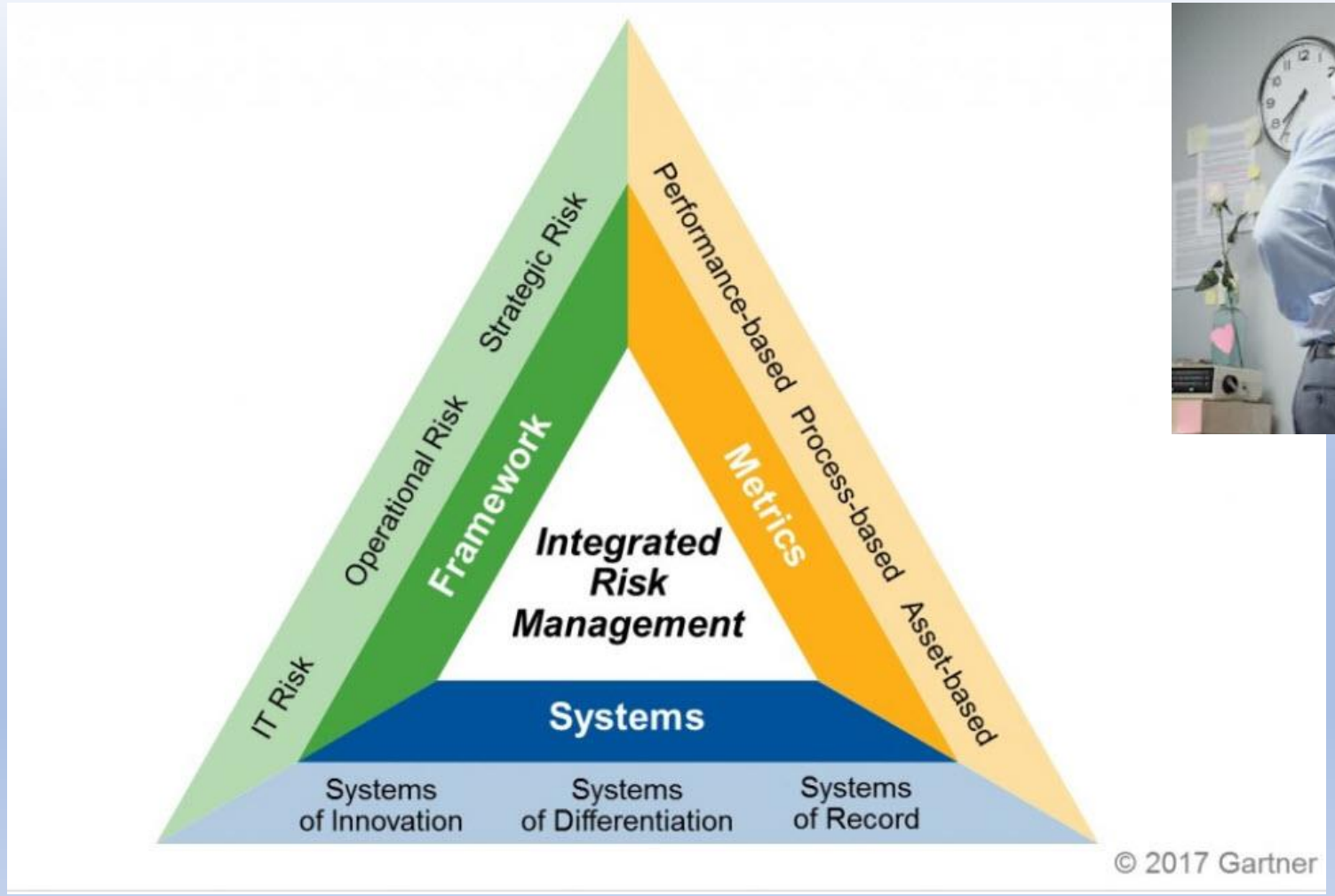
- Change-of-address forms
- Mailbox
- Garbage
- Online purchases using your debit card/credit card and providing security code
- Home health aid workers
- Insurance & beneficiary information
- Impersonation
- Tax information
- Affinity
- Shoulder surfing
- Social engineering
- Phishing, Vishing, & Smishing
- Purchase of personally identifying information from various online & Dark Web sites

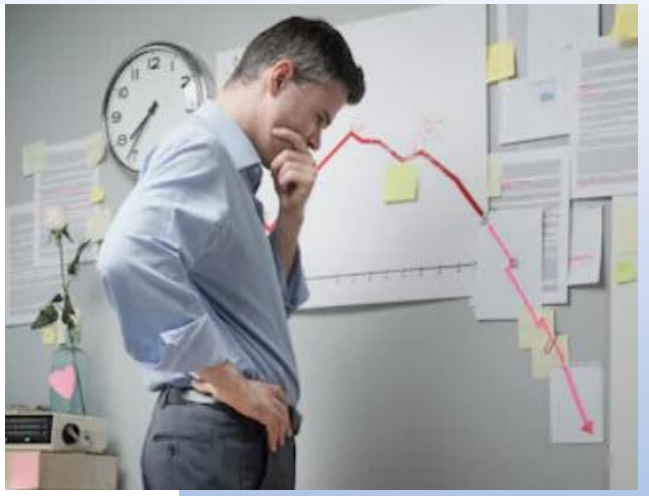


Thought: Who has access to my PII and how can I protect it?

Objectives for Presentation:

2. What steps to take for basic cyber protection, Owner/C-Level responsibilities



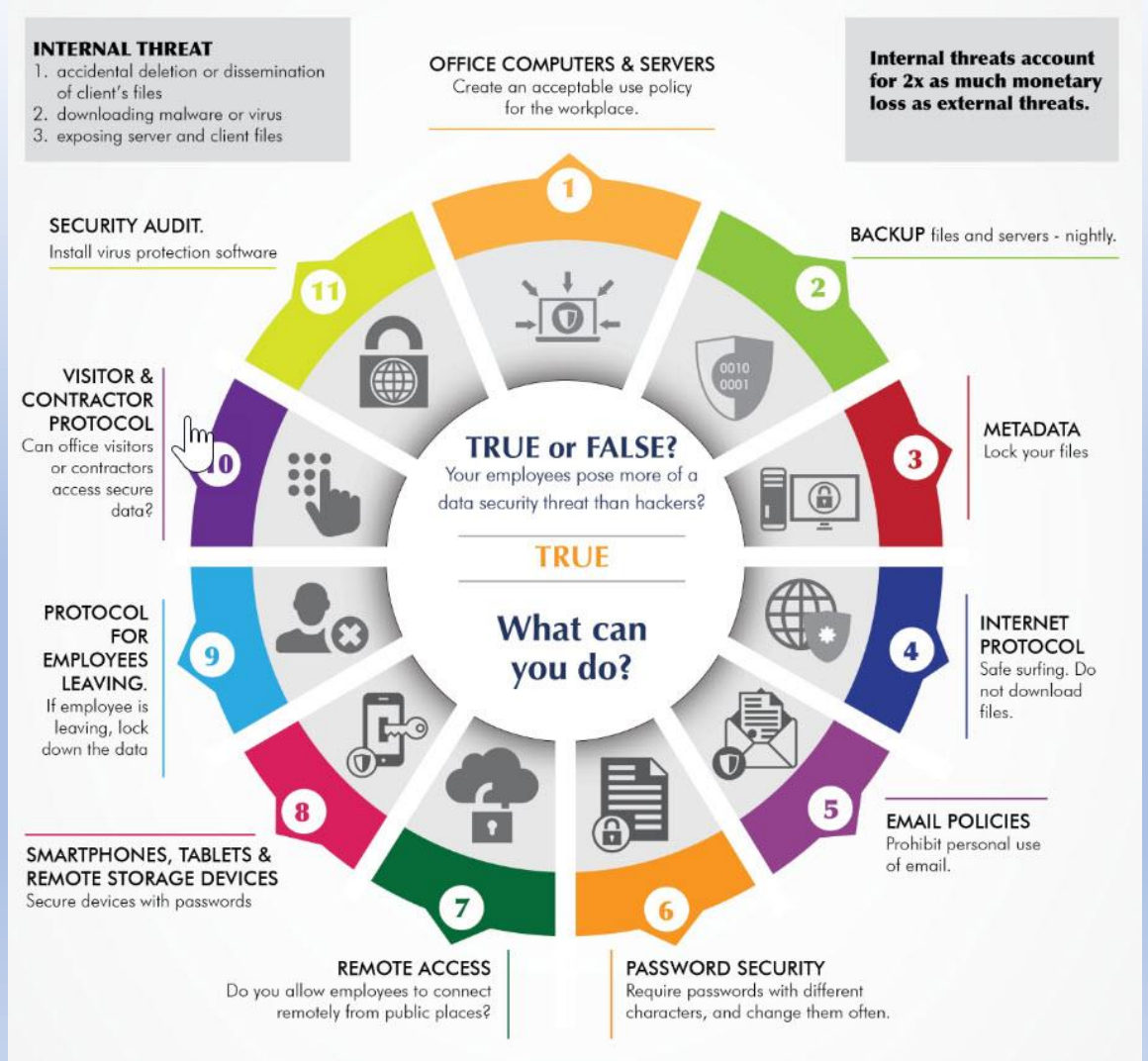


Objectives for Presentation:

3. Training staff, Social Engineering and attacks on your staff

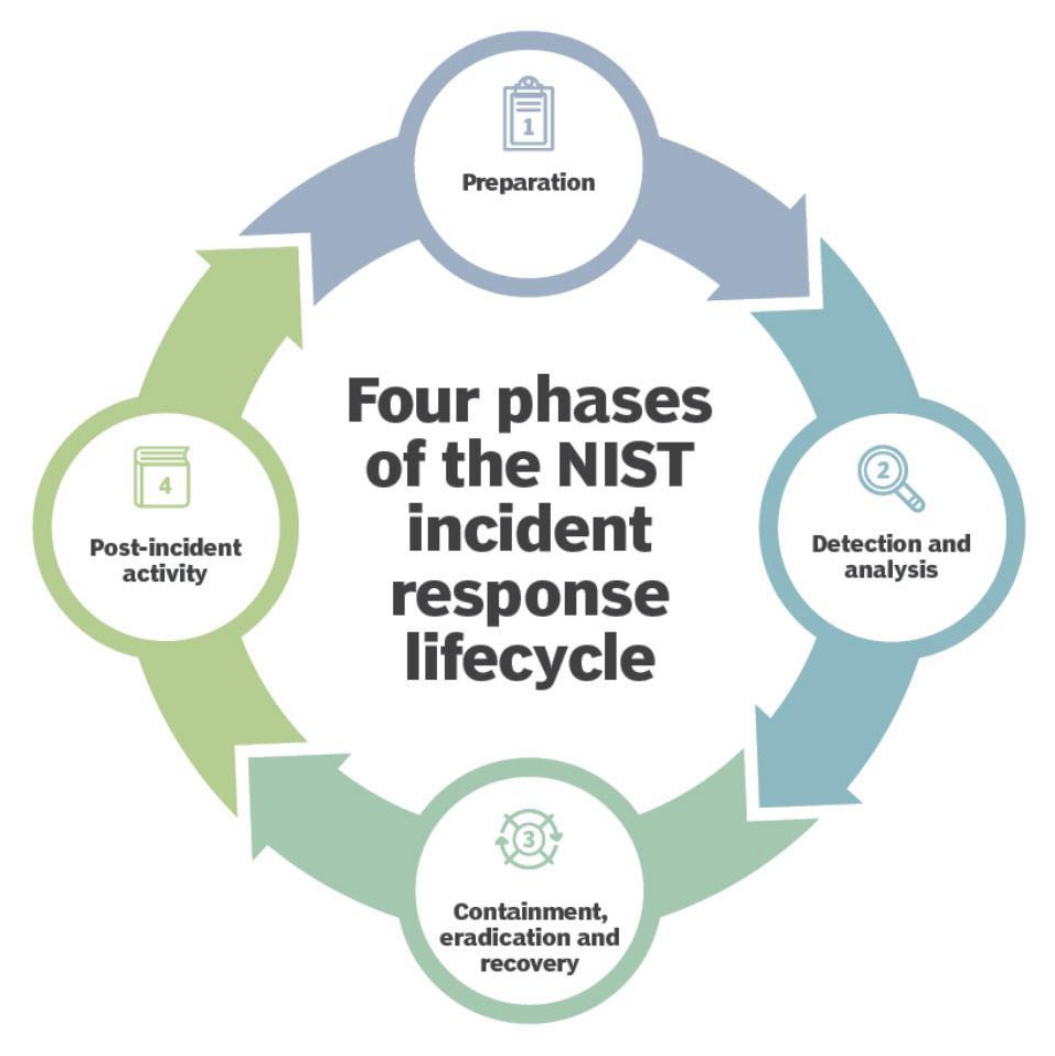
Objectives for Presentation:

3. Training staff, Social Engineering and attacks on your staff



Objectives for Presentation:

4. Business Continuity planning, are you able to sustain a companywide incident

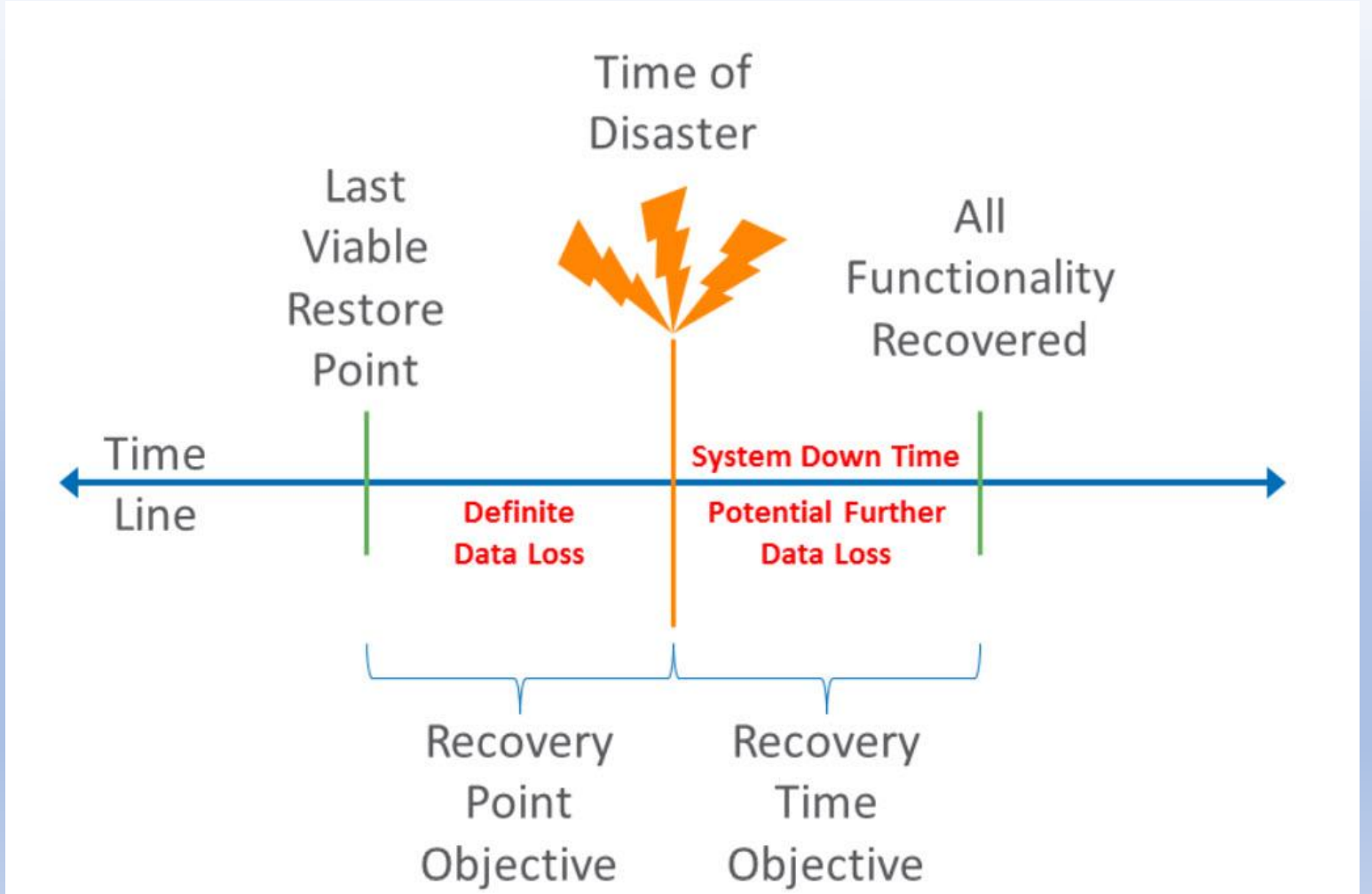


Objectives for Presentation:

4. Business Continuity planning, are you able to sustain a companywide incident

Objectives for Presentation:

4. Business Continuity planning, are you able to sustain a companywide incident



Objectives for Presentation:

5. Frameworks for your security policy/plan.

FRAMEWORK - A layered structure indicating what kind of programs can or should be built and how they would interrelate.

NIST (National Institute of Standards in Technology)

The Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk.

In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

The Five Functions

- Highest level of abstraction in the core
- Represent five key pillars of a successful and wholistic cybersecurity program
- Aid organizations in expressing their management of cybersecurity risk at a high level

The Identify Function

•The Identify Function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities

Example Outcomes:

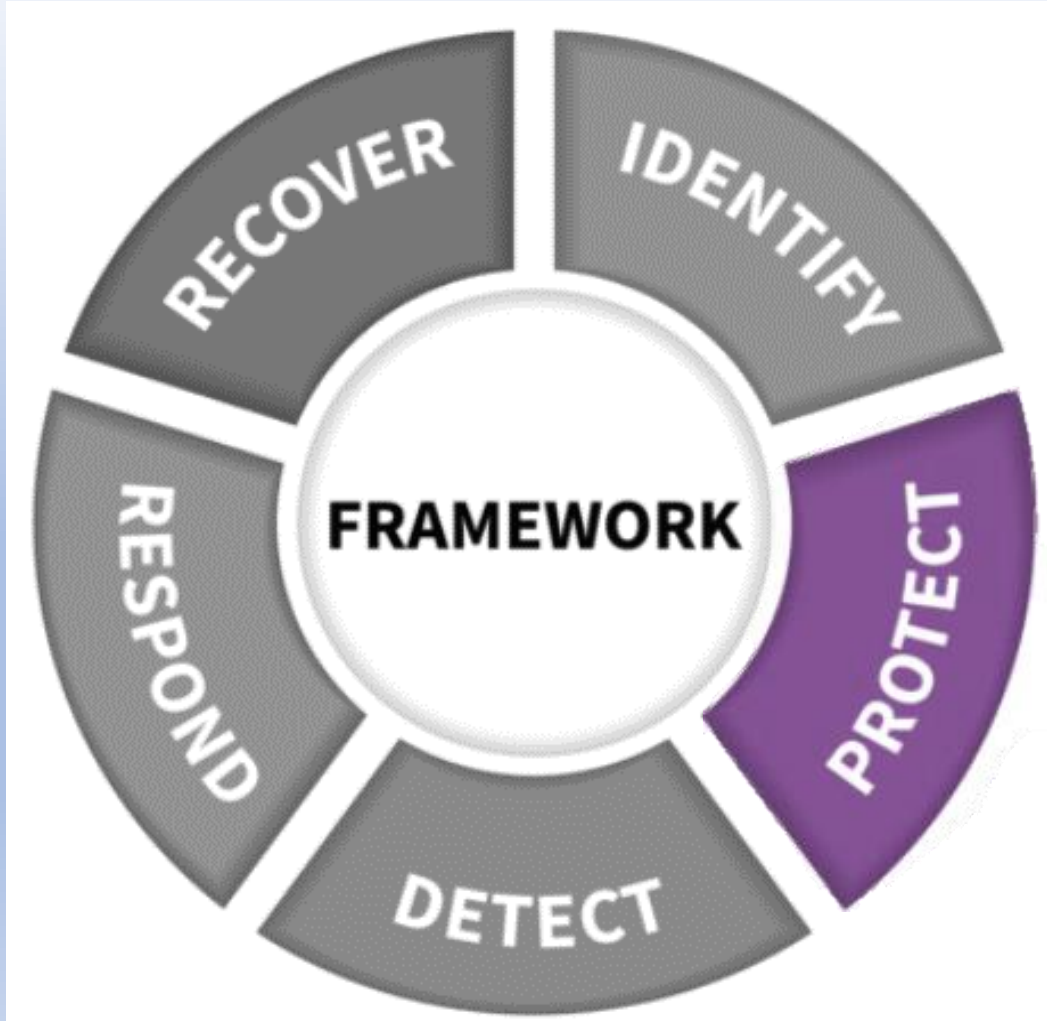
- Identifying physical and software assets to establish an Asset Management program
- Identifying cybersecurity policies to define a Governance program
- Identifying a Risk Management Strategy for the organization

The Protect Function

•The Protect Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services

Example Outcomes:

- Establishing Data Security protection to protect the confidentiality, integrity, and availability
- Managing Protective Technology to ensure the security and resilience of systems and assists
- Empowering staff within the organization through Awareness and Training



The Detect Function

•The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner

Example Outcomes:

- Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events
- Ensuring Anomalies and Events are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures

The Respond Function

•The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact

Example Outcomes:

- Ensuring Response Planning processes are executed during and after an incident
- Managing Communications during and after an event
- Analyzing effectiveness of response activities

The Recover Function

•The Recover Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

Example Outcomes:

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities

Resources

Where to Learn More and Stay Current

Framework for Improving Critical Infrastructure Cybersecurity and related news, information:

www.nist.gov/cyberframework

Additional cybersecurity resources:
http://csrc.nist.gov/

Questions, comments, ideas:
cyberframework@nist.gov

National Institute of Standards and Technology
U.S. Department of Commerce

Objectives for Presentation:

6. Risk Analysis, Business Impact Analysis, Continuity & Disaster Planning

Objectives for Presentation:

6. Risk Analysis, Business Impact Analysis, Continuity & Disaster Planning

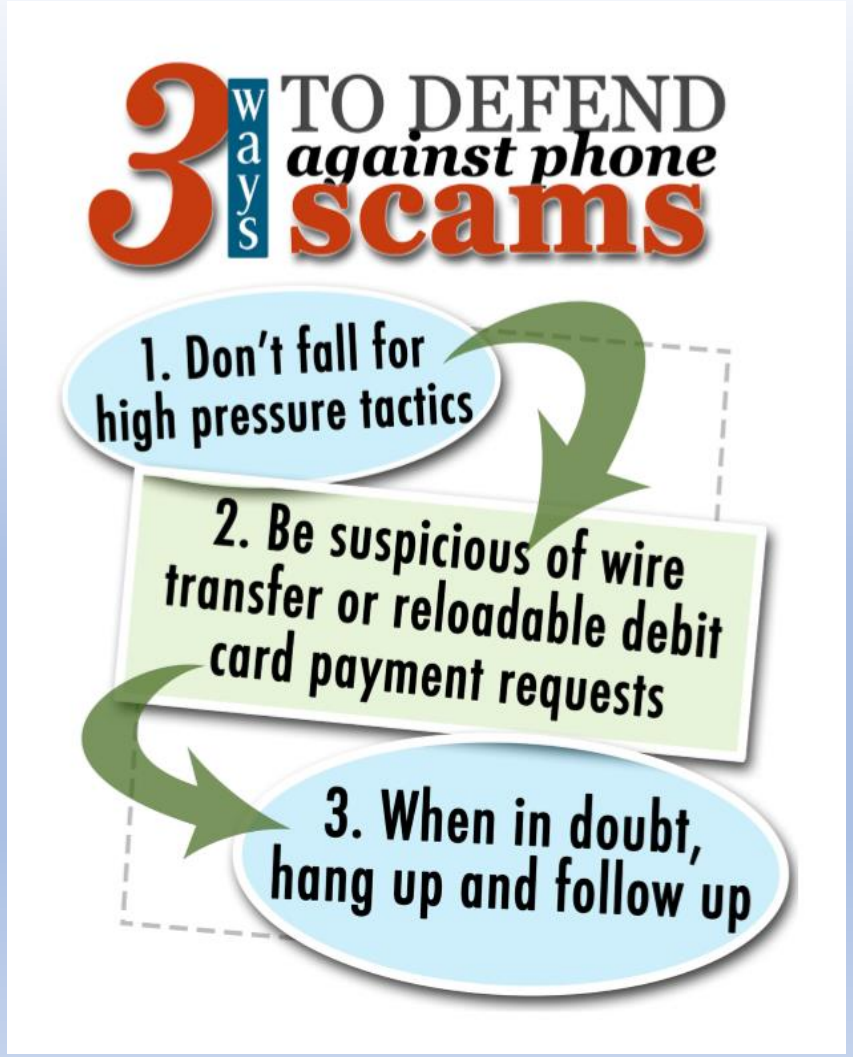
Objectives for Presentation:

6. Risk Analysis, Business Impact Analysis, Continuity & Disaster Planning

Likelihood (What's the chance the of the risk occurring?)	Consequence: How severe could the outcomes be if the risk event occurred? →	1 Insignificant	2 Minor	3 Significant	4 Major	5 Severe
	5 Almost Certain	5 Medium	10 High	15 Very high	20 Extreme	25 Extreme
	4 Likely	4 Medium	8 Medium	12 High	16 Very high	20 Extreme
	3 Moderate	3 Low	6 Medium	9 Medium	12 High	15 Very high
	2 Unlikely	2 Very low	4 Low	6 Medium	8 Medium	10 High
	1 Rare	1 Very low	2 Very low	3 Low	4 Medium	5 Medium

Objectives for Presentation:

7. Actions to protect yourself and business from being scammed



Statistics:

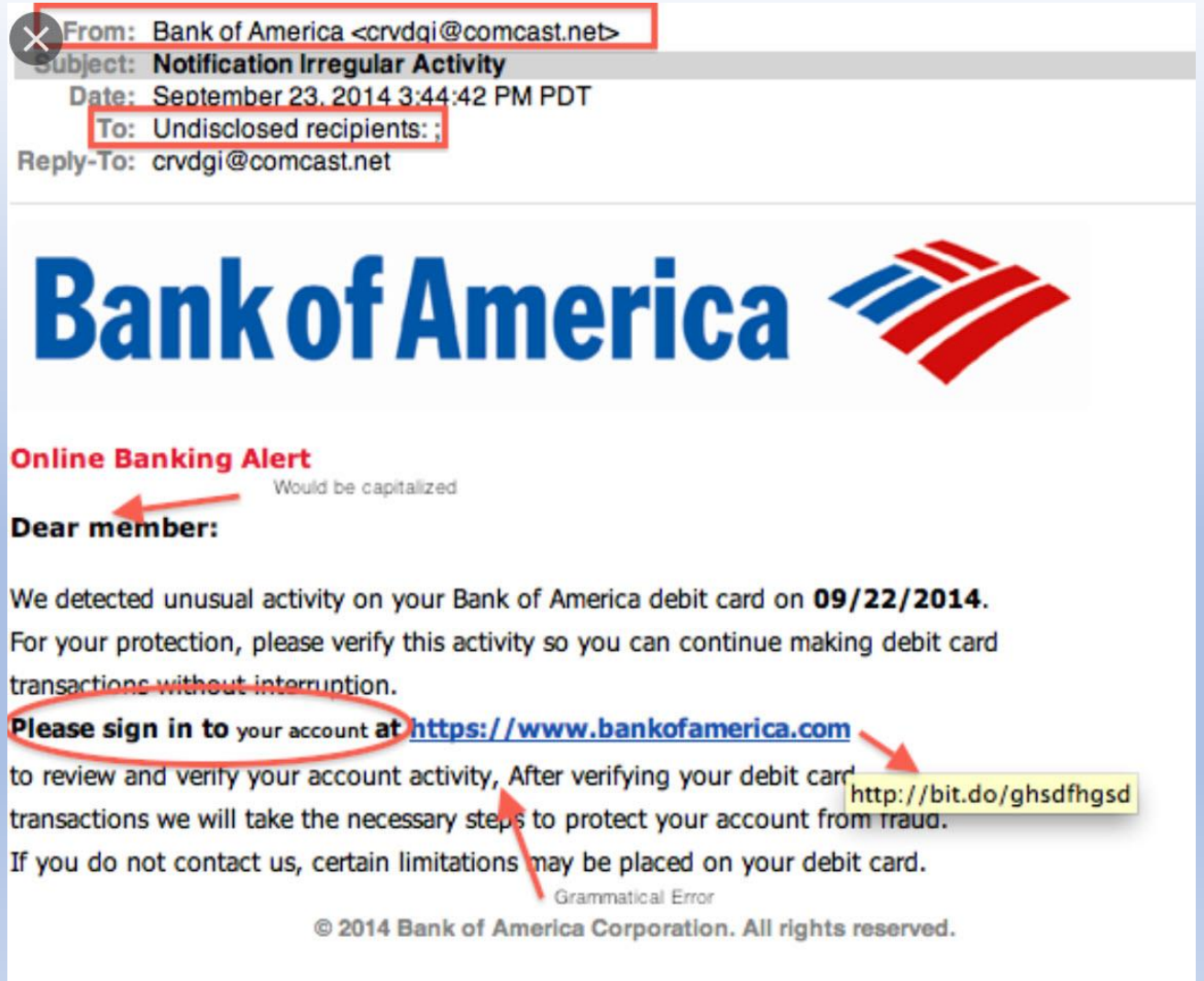
- Consumer Financial Protection Board
- Financial Crimes Enforcement Network
(Feb 27, 2019)

- Study revealed key facts, trends, and patterns from 2013 to 2017 by analyzing 180,000 elder financial exploitation suspicious reports
  - Filed by FI, Banks, Casinos, and Money Service Businesses

- Findings:
  - Financial Institutions have seen the numbers of elder victimizations quadruple
  - 58% increase in money wires (2017)
  - On average, older adults aged 70 to 79, lost on average $43,300; When the older adult knew the suspect, the average loss was larger – about $50,000

Objectives for Presentation:

7. Actions to protect yourself and business from being scammed



SWEEPSTAKES & COMPUTER REPAIR SCAM

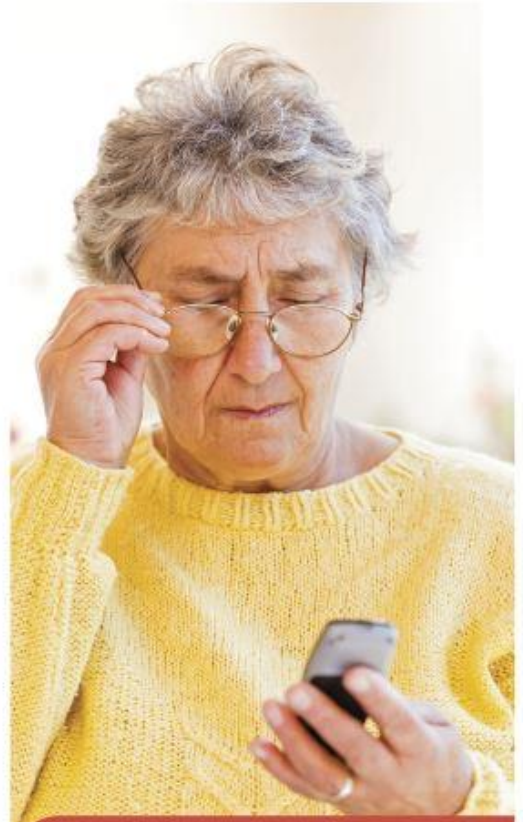
1. Understand what you care about, and why
2. Think about situations in which you could be compromised

Protecting Older Americans Against Fraud

Sweepstakes Scams / Jamaican Lottery Scams

Fraud Case #7:

"Lisa" from New Mexico reported that criminals stole $300,000 from her mother-in-law. This began as a sweepstakes scam when a man called to tell her she had won a lottery. It evolved into a romance scam, and the caller began asking for money to help pay various expenses. The man eventually had the locks on her house changed, and her phone replaced remotely in order to cut her off from her concerned children. A Fraud Hotline investigator filed a report with the FTC and referred Lisa to state agencies and legal directories. The investigator also sent Lisa additional information on the sweepstakes and romance scams to share with her mother-in-law.



Fraud Case #9:

"Arlene" from California reported that she was targeted by a computer scam. She clicked on a pop-up advertising IT support services for one year for $300. She paid and thought she had subscribed to the service. After five months, she received a series of calls offering her a refund because, the caller said, she had not used the service. However, they required her to give her private bank information in order to receive the refund. She gave them some of the information before she realized this was a scam. She eventually realized that her computer had been taken over remotely and infected with malware. She contacted her bank to protect her account and had her computer cleaned by the retailer. A Fraud Hotline investigator reported this to the FTC and the FBI's Internet Crime Complaint Center.

MEDICAL & ROMANCE SCAM's

1. Understand what you care about, and why
2. Think about situations in which you could be compromised
3. Be aware of the strengths and weaknesses of risk management techniques
4. Keep an eye out for cyber security myths
5. Balance cyber risks against other types of risk

Fraud Case #18:

"James" from North Carolina called the Fraud Hotline to report that his mother passed away in January 2016. Since June of that year, someone has been using her identity on credit cards and car loans. James was not made aware of this until the credit company contacted him in 2017. The Fraud Hotline investigator sent him the identitytheft.gov link and a Fraud Book for more information. The investigator also encouraged him to work with the credit card company and credit reporting agencies.

Fraud Case #14:

"Gail" from Tennessee called the Fraud Hotline to report that she was the victim of a romance scam. A man contacted her via the online game, "Words with Friends," and they developed a romantic relationship. The man told her that he has $12 million in gold and works on an oil rig in Nigeria, but needed her help to access it. Gail had sent the man $500,000 and depleted her retirement account before she realized that this was a scam. A Fraud Hotline investigator filed a report with the FTC and IC3 on her behalf, and also sent her a copy of the Fraud Book to help her understand how else she may be targeted by him.

POLL THE AUDIENCE

- Do you have a Cyber Awareness program?
- What are your main concerns about using the Internet?
- Have you ever implemented a Cyber Security program?
- What is your biggest technology challenge today?

Thank You!

Today's focus:

Basic Steps for Non-Technical Executives and Decision Makers

Roger Swanson
Executive Account Manager

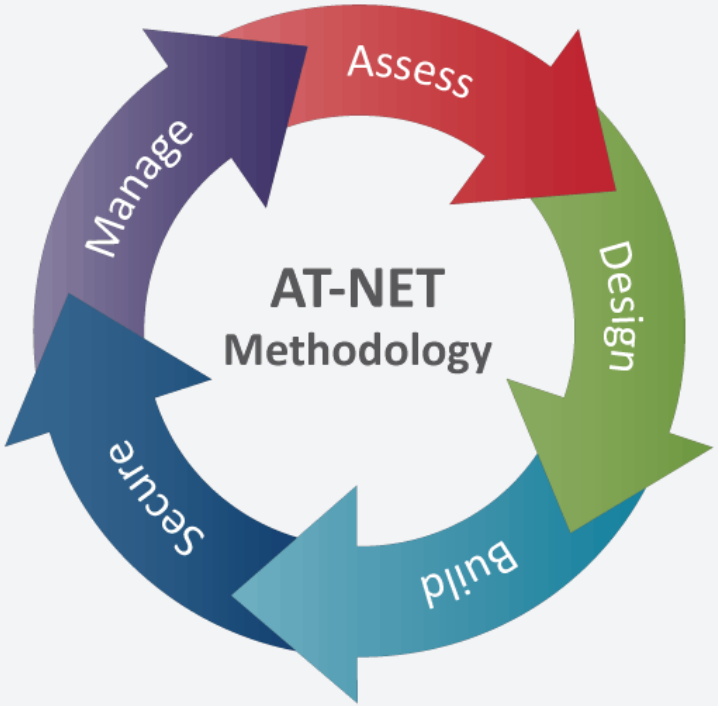
ATNET Services, Inc. - Charleston Division
843-576-3773 / Roger.Swanson@at-net.net
www.RogerSwanson.com

AT-NET Services

Application Development | Collaboration | Data Center Virtualization | Infrastructure & Security | Managed Services | Network Infrastructure | Unified Facilities

Methodology

Our Solutions are designed to protect every aspect of your IT infrastructure. Our cyclical approach allows us to assist at any point in your company's security process.



- Assess - Discover Strengths & Vulnerabilities
- Design - Create & Plan Strategies
- Build - Construct Intuitive Solutions
- Secure - Protect Valuable Assets
- Manage - Complete Systems Support

Technology Solutions that Drive Productivity | www.at-net.net | Toll-Free: 866.708.0886

AT-NET Services

Application Development | Collaboration | Data Center Virtualization | Infrastructure & Security | Managed Services | Network Infrastructure | Unified Facilities

Locations:

Corporate Charlotte Office
3401 Vardell Lane, Suite D
Charlotte, NC 28217
Phone: 704.831.2500
Email: sales@at-net.net

Atlanta, GA Office
Phone: 866.275.4734

Charleston, SC Office
Phone: 843.576.3773

Columbia, SC Office
Phone: 803.929.5372

Greenville, SC Office
Phone: 864.679.0006

Knoxville, TN Office
Phone: 866.708.0886

Washington, DC Office
Phone: 877.734.4364

Partners:


CITRIX
Microsoft
GOLD CERTIFIED
Partner
NetApp
CISCO
PARTNER
Premier
Certified
Liebert
hp
RedCondor
WEBSENSE
SECURING PRODUCTIVITY
vmware
RSA
The Security Division of EMC
LifeSize
EMC²
where information lives

AT-NET Services

Application Development | Collaboration | Data Center Virtualization | Infrastructure & Security | Managed Services | Network Infrastructure | Unified Facilities

Thank you for you time today.