



What Technology Managers Really Need to Know About Security

One Size Does Not Fit All

AGENDA

- **Introduction**
- **Basic Security Concepts Reviewed**
- **Six Security Discussion Areas**
 - From three size perspectives
- **What's a Manager to do?**
- **Checklists & Closing**

Introduction

- **Michael Esolda, CGCIO**
 - CIO for Woodbridge Township and Schools
- **John Hitchcock**
 - Systems Administrator for the Township of Branchburg
- **Bernadette Kucharczuk, CGCIO**
 - Director of Data Processing (Info Tech/MIS) for the City of Atlantic City
- **Todd Costello**
 - Director of MIS for the Township of Middletown

Introduction

- **Audience Tech Knowledge Poll**
- **Audience Muni-Size Poll**
- **Session Description**
- **What is GMIS?**
 - **Tech Manager's Resource**
 - **Don't Reinvent the Wheel**
 - **Find Project Partners**
 - **Shared Services Collaborators**
 - **Experienced Vendors**

Introduction

- **Bottom Line Take-Away Messages**
 - Need strong, solid, professional, advice on technology best practices. Even small organizations are targets and organizational technology management is NOT the same as home technology management.
 - Look for webinar and other technology training offerings throughout the year and send as many staff as possible when they are available. Encourage technology staff to network with other municipalities.

AGENDA

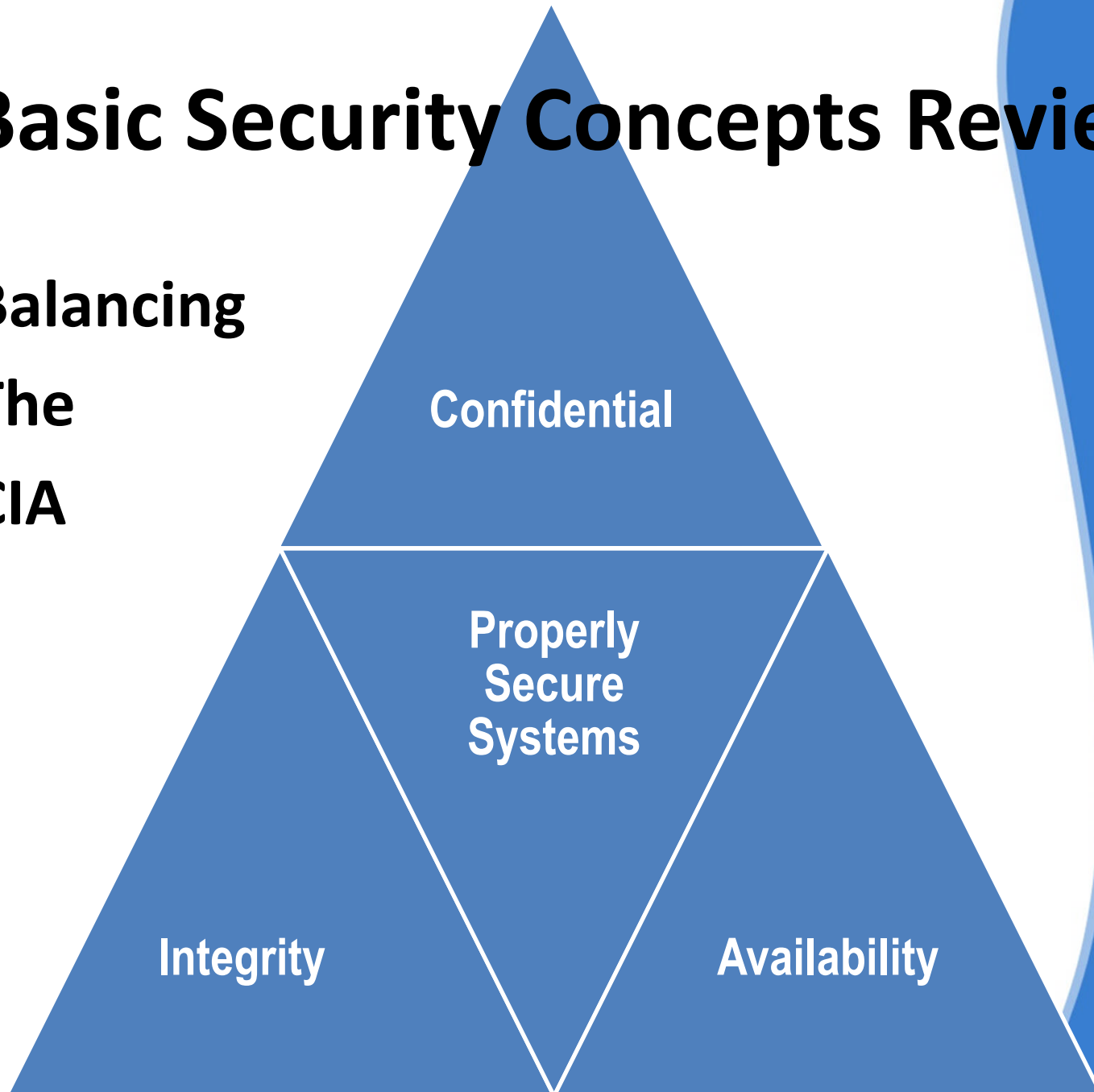
- Introduction
- **Basic Security Concepts Reviewed**
- Six Security Discussion Areas
 - From three size perspectives
- What's a Manager to do?
- Checklists & Closing

Basic Security Concepts Reviewed

- Overall Goal of Security – Balance the CIA
 - Confidentiality: Make sure the data is only available to those who have the proper authority
 - Integrity: Make sure the data is reliable and true so users are confident it has not been changed by unauthorized parties
 - Access: Make sure the data can be reached when needed from the places where the users are (remote access vs. physical access)

Basic Security Concepts Reviewed

Balancing
The
CIA

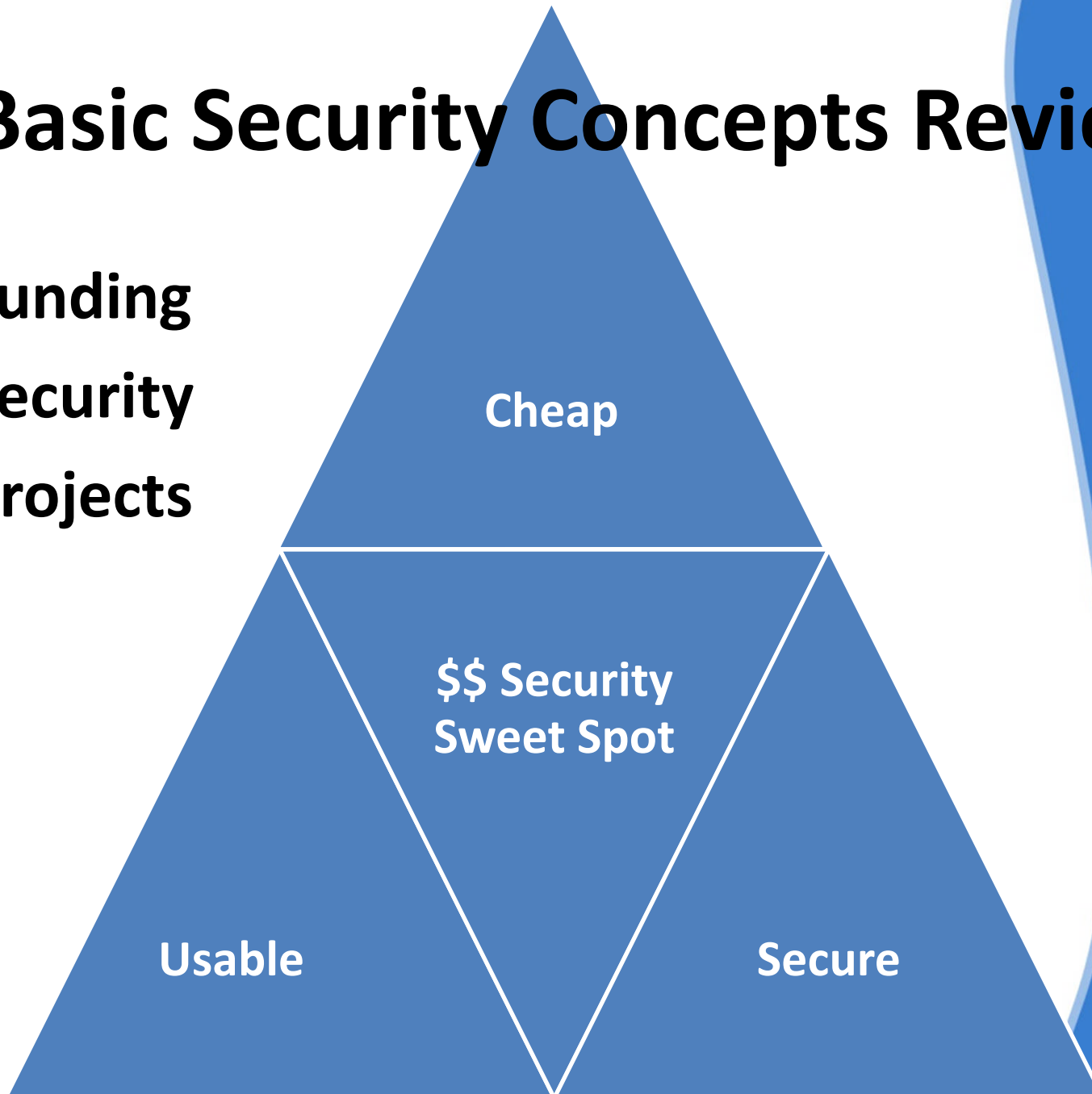


Basic Security Concepts Reviewed

- Dollars and Cents-ible Investment Goals
 - Gartner estimates that 6.3 % of government IT budgets are allocated to security
 - Nationally all organizations spend approximately 6.6% of their IT budget on security
- 31% of Security Costs are Attributed to Personnel

Basic Security Concepts Reviewed

**Funding
Security
Projects**



Basic Security Concepts Reviewed

- Why are there vulnerabilities? Why do we have to provide security?
 - Human Errors? User Desires for Higher Usability? Software manufactures looking to “cut corners”?
 - In the world of bits and bites we inherently trust data and input from non-trusted sources.
- Would you let someone in the front door without verifying who they are first?

Basic Security Concepts Reviewed

- Security is Not Something to Buy. Security is a Process of Skillful Risk Management.
 - Some Equipment
 - Some Policy
 - Lots of User Education
- What can you afford to lose in terms of your organization's finances, equipment and reputation?
 - Do nothing to protect them, you will lose them.

AGENDA

- Introduction
- Basic Security Concepts Reviewed
- **Six Security Discussion Areas**
 - From three size perspectives
- What's a Manager to do?
- Checklists & Closing

Six Security Discussion Areas

- **Threat Assessment**
- **Desktops**
- **Applications**
- **Servers**
- **Network**
- **Internet/Web/Cloud**

Threat Assessment

- External Threats
- Internal Threats
- Combined Threats

Threat Assessment - Small

- Everyone is a target
 - South New Jersey Municipality -- \$600,000 stolen
 - Zeus Trojan -- \$3 million stolen from U.S. Businesses and Municipal entities
 - Security firm McAfee-- Estimates \$1 trillion per yr. in lost/stolen devices, intellectual property & internet attacks

Threat Assessment - Medium

- Network Administrator (full time employee)
 - Set up website for software distribution
 - Illegal copies of software stored on multiple devices (servers and workstations)
 - FBI and High-Tech Crimes Task Force investigation resulted in confiscation of some equipment
 - \$25,000 in restitution ordered by Court to help cover “clean-up” costs

Threat Assessment - Large

- Large Municipalities are Targets.
- Simple things to remove sniper attacks
- Example of targeted attacks via email to specific employees.
- “DON’T ADVERTISE YOUR ADDRESS” – use Forms for Communication- simple and effective
- Remove the threat from the outside in.
“Border security”

Six Security Discussion Areas

- **Threat Assessment**
 - Need Defense in Depth!
- **Desktops**
- **Applications**
- **Servers**
- **Network**
- **Internet/Web/Cloud**

Desktops - Small

- Virus, Spam & Malware protection
 - System scanning
 - Media scanning
 - Web filtering
 - Email filtering
- Data Back-ups
 - Restricting save to location
 - Selecting your data
 - Scheduling Back-ups
 - Offsite back-ups storage

Desktops - Medium

- Desktop Operating System Patch Management
 - a Patch is like a Software “recall”
 - Need to check for them and install them regularly
- End-User Desktop Policies
 - Who can “log-in” and what are they allowed to do
 - Written, but need technology enforcement
- End-User Access Controls to Desktop
 - Log-in user name/password retention
 - Remote Desktop, GoToMyPC, PCAnywhere

Desktops - Large

- KISS Principle. The simple things are the most vulnerable ones.
- Administrator Lockdown
- Disabling the Administrator login
- Disabling USB drives and AutoRun
- Strong Group Policy management – Do as Much as you can at the server not at the workstation
- Local AV/Malware protection Server Pushed

Six Security Discussion Areas

- Threat Assessment
- Desktops
- **Applications**
- Servers
- Network
- Internet/Web/Cloud

Applications - Small

- Password policy
 - Default passwords
 - Strong passwords
 - Treat as confidential
- Defining User access
 - Not all users are Administrators,
 - Only allow users access to what is required of them.

Applications - Medium

- Application Installation Policy and Controls
 - Everybody?
 - Power Users?
 - Administrators
 - Need to Verify software is properly licensed
 - Copyright infringements
 - Concurrent Use
- Out-Side Vendor Access - When and How?
 - Signed Consent Agreement
 - Security/Background on their employees?

Applications - Large

- Client Server Vs Web App
- Larger Municipalities have been trying to get away from using client/server apps. Too many to setup and too many security risks with software installs.
- Some apps need administrative access on directories and hidden file locations
- Web Apps – Easier to deploy and security is handled at easy dynamic level.

Six Security Discussion Areas

- Threat Assessment
- Desktops
- Applications
- Servers
- Network
- Internet/Web/Cloud

Servers - Small

- Spam & Malware control
 - IP reputation analysis
 - Verify sender or origin of an email
 - Intent analysis
 - Rule-based filtering
- Domain configuration
 - Assigning user permissions
 - Password policy
 - Account lockout policy
 - Resource management

Servers - Medium

- When technology really gets sticky....
 - If you don't know a term, use the Wiki
 - www.wikipedia.org
- Active Directory – for Microsoft servers
 - Secure access to this critical core components
- Dynamic Host Configuration Protocol (DHCP)
 - Think about Getting Internet Access at a Hotel
 - Code or password protected – should be at the office
- Print Servers
 - Storing/archiving copies of things printed

Servers - Large

- Strong Password Encryption
- Use Group based file sharing roles
- TEST OUT PATCHES BEFORE DOING UPDATES
- DO NOT DO AUTO UPDATE!
- Only allow Remote Admin via internal or VPN not NAT
- Disk Encryption with SAN – Remote Storage
- VMWARE – Better Physical and Virtual Security easier to manage.

Six Security Discussion Areas

- Threat Assessment
- Desktops
- Applications
- Servers
- **Network**
- Internet/Web/Cloud

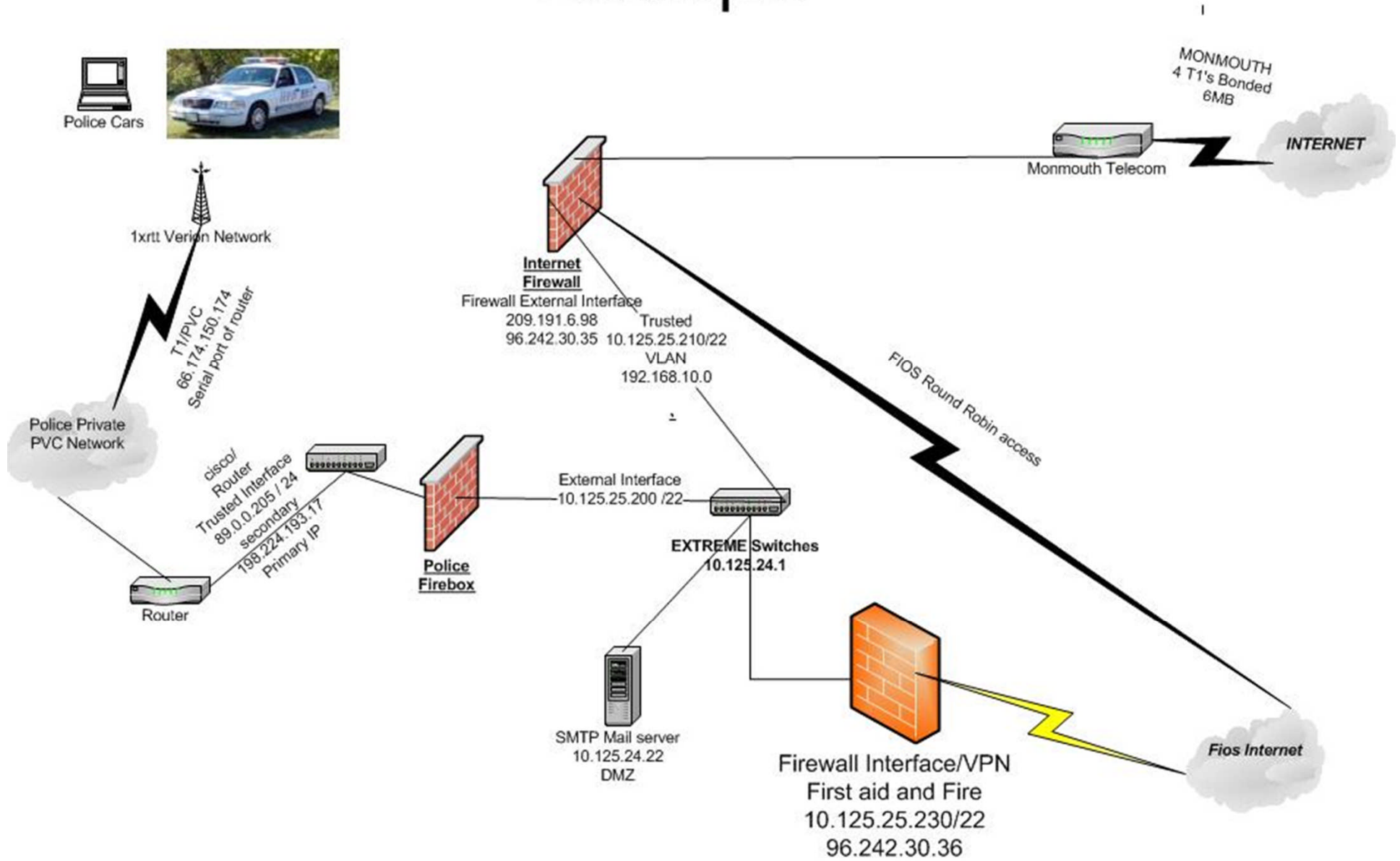
Network - Small

- Understand your network
- Define Core Security Policy
 - Planning
 - Prevention
 - Response
- Protect your systems
 - Firewalls
 - Traffic Monitoring

Network - Medium

- Wide Area Network (WAN)
 - Tie multiple buildings across the municipality together to share resources – TeleComm Highway
- Gateway, Routers and Switches
 - Slide notes have Wiki definitions
 - Physical and Logical Security Concerns
 - Unlocked Broom Closet = Wide-Open on Ramp
 - Poor Logical Design = No Tolls and No Express Lanes
 - Need Secure VLAN for most critical components
 - Change all Default Passwords!!
 - If you open box, turn on & it works, it is NOT secure

Network Diagram Example



Network - Large

- Physical security Very Important (Where is your Gear Stored) Who has access?
- Packet Encryption on VPN/Police Networks (Separate LAN) Civilian vs Non Civilian
- Layer 2/Layer 3 Switches – Software vs. Hardware manageable
- Firewalls – How many is Enough? Manageable? Easily updated?
- Email – Spam, Virus, Malware scanning - Stopping a broadcast

Network – Large (cont)

- Protect against internal broadcast messages.
- “BANDWIDTH HOGS” ie Video and BOT attacks
- Simple steps – DHCP Protection/DNS
 - Don’t allow DNS To be handed out automatically
 - Restricting MAC Address DHCP – Lots of Work but effective
 - VLAN Your Networks – VOICE (VOIP), DATA, Management of Systems - Will reduce risk of catastrophic outage.

Six Security Discussion Areas

- Threat Assessment
- Desktops
- Applications
- Servers
- Network
- Internet/Web/Cloud

Internet/Web/Cloud - Small

- Internet and web usage policies
 - No organization is too small.
 - Restrict Internet access to key personnel and systems.
- Web and Email filtering
 - Enforcing usage policies
 - Minimizes threat exposure
- Network Address Translation (NAT)
 - Technique to hide an IP network

Internet/Web/Cloud - Medium

- Cloud Services
 - Where is the Cloud?
 - Internal Clouds Vs. External Clouds
 - The ultimate in outsourcing?
 - Great Plans for getting your data to them, but how do you get your data back if you change your mind or want to change providers?
 - Just “Trust Us” mantra – if we show you how we are securing your data, then it won’t be as secure as if we keep it a secret.
 - Managing the Risks

Internet/Web/Cloud – Large

- Protect at the Border
- Firewalls – DMZ – Email Servers
 - Group Based Internet Access (Active Directory) SSO
 - Limited Internet access to non essential personal
 - Content or Site Specific Filtering – i.e. Facebook, My space, Twitter – How much is too much?
 - Port Blocking – additional good practice Blocking IM Traffic.

Internet/Web/Cloud – Large cont.

- Cloud – Are you the host of your own Cloud or are you part of another Cloud Environment
 - Hosting a cloud –Lots of security to handle – Shared Services for multiple towns. Direction of Police and Non Police Systems. i.e. County 911 services.
 - Email Clouds – i.e. Google, Yahoo, or even a hosted Exchange. “YOU HAVE NO CONTROL” Especially physically – AG Guidelines, DARM
- Biggest question – Where is my DATA?

AGENDA

- Introduction
- Basic Security Concepts Reviewed
- Six Security Discussion Areas
 - From three size perspectives
- **What's a Manager to do?**
- Checklists & Closing

What's a Manager to Do?

- Understand the needs and goals of your Organization.
 - Know your network infrastructure.
 - Maintain your systems.
 - Understand your upgrade options.
 - Maintain strong & proactive security policies.
 - Maintain operational worthiness.

What's a Manager to Do?

- Medium Perspective
 - Can't outsource it all, you need some internal technology expertise if only to manage the external out-sourced contracts
 - Need reasonable fiscal resources
 - Too Big to know everyone and their whole family
 - Too Small to pay for the full complex level of security
 - Watch for “Penny-Wise and Pound-Foolish” Decisions
 - Solid Policy, Regular Monitoring and Consistent Enforcement are CRITICAL.

What's a Manager to Do?

- Large Perspective
- Keep to the fundamentals (User is still your biggest Threat)
- Continue to expand on Free and built-in security measures
- Good auditing of network and workstation inventory
- Spot checks of Internet website activity
- Check the logs on Malware / AV Console using centralized report server

AGENDA

- Introduction
- Basic Security Concepts Reviewed
- Six Security Discussion Areas
 - From three size perspectives
- What's a Manager to do?
- Checklists & Closing

Checklist - Small

- **Municipal must haves:**

- Anti-virus
- Back-ups
- Password Policy
- User access Controls
- System and operational recovery plan
- Acceptable Use Policies
- Password Enforcement
- Email filtering (spam, virus, spoofing, phishing, spyware, file blocking)
- Web filtering (URL filtering, file blocking, IP/Port blocking)
- Firewall(s) protecting from both internal and external risks
- Security Policies
- Awareness and Training for your Users

Checklist - Medium

- **All Small Must-Haves PLUS:**
 - Patch Management
 - System for Remote Access by Outside Vendors
 - Application Installation Controls and Policy
 - DHCP and Print Server Controls
 - Active Directory Configuration and Management
 - Switch, Router, and Gateway Security
 - Physical Security Systems
 - Internal or External Cloud Management

Checklist - Large

- **All Small and Medium Must Haves PLUS:**
 - Desktop Lock-downs and Device Lock-outs
 - Single Sign-on Security Management
 - In-house Development Security and Policy
 - Archival Security and Management
 - System Configuration Change Management
 - Black-list Prevention and Monitoring
 - Network Security “Sniffer” and Intrusion Detection
 - Website Security and Content Policy
 - Social Networking and IM Policies

Closing

- **Bottom Line Take-Away Messages**
 - Need strong, solid, professional, advice on technology best practices. Even small organizations are targets and organizational technology management is NOT the same as home technology management.
 - Look for webinar and other technology training offerings throughout the year and send as many staff as possible when they are available. Encourage technology staff to network with other municipalities.
- **NJGMIS can help.... Encourage your tech folks to join! www.njgmis.org**



What Technology Managers Really Need to Know About Security

One Size Does Not Fit All

2010-2012 NJ-GMIS

Executive Board Members

- **Justin Heyman, President - Township of Franklin**
- **Robert McQueen, Vice President – Township of Princeton**
- **Chris Payne, Secretary - City of Plainfield**
- **John Hitchcock, Treasurer - Township of Branchburg**
- **Mitchell Darer, Executive Director - NJIT / CIAT**

Section Representatives

- State Agencies: Marc Pfeiffer, NJ Div. of Local Gov Services
- County Government: Khalid Anjum, Middlesex County
- Municipal Government: Dave Miller, Twp. of Parsippany/Troy Hills
- Public Schools: Michael Dean, Lawrence Township Public Schools
Michael Schwarz, Hillside Public School

FOUR QUESTIONS- OUTRO

- Do you the know the names of your IT counterparts in:
 - 1) Your neighboring school district(s)?
 - 2) Your County/Community College?
 - 3) Your neighboring municipal government(s)?
 - 4) Your county government?

What Do Members Get From GMIS International?

- Network with Peers
 - Annual Conferences
 - Education Sessions and Local Meetings
- Website Access
 - Sample RFPs, Policies, Contracts, etc.
- GEM – GMIS Educational Materials
- Eligibility for Annual Awards and CGCIO discount
- Value – Dues for Small only \$75 per year, Medium \$150 or \$300, Large \$400

GMIS New Jersey

– Where We've Been...

- New Jersey Digital Government Summit
- School Board Association & NJ TechSpo
- League of Municipalities (2005- to present)
 - 2010 League Workshop: Tuesday, Nov. 16 – 3:45pm – What Tech Managers Really Need To Know About Security – Room 404
 - 2010 League Workshop: Wed, Nov. 17 – 9:00 am3:45 – What Elected Officials Need To Know About Technology – Room 415

GMIS New Jersey

– What We Have

- New Jersey GMIS Listserv
 - Local List Serve to help members talk to other local NJ members :
 - Notify members of meetings and events
 - Special interest groups to exchange ideas and discuss issues
 - Exchanging of ideas relating to various technologies & vendors (hardware, software, applications, etc)
 - Sharing of contracts, rfp's, best practices
- NJGMIS Technology Education Conference

NJGMIS – TEC 2011

Technology Education Conference

- SAVE THE DATE: WED. APRIL 6, 2011
- The Palace at Somerset Park Somerset, NJ
- REGISTER NOW –
www.njgmis.org/conference.html
- Keynote Speaker confirmed Dr. Alan R. Shark,
Executive Director/CEO of the Public
Technology Institute (PTI) and Assistant
Professor at Rutgers University School for
Public Affairs and Administration

NEW JERSEY GMIS CONTACT

NJ GMIS

PO Box 34 East Orange, NJ 07019

732-602-6017

www.njgmis.org