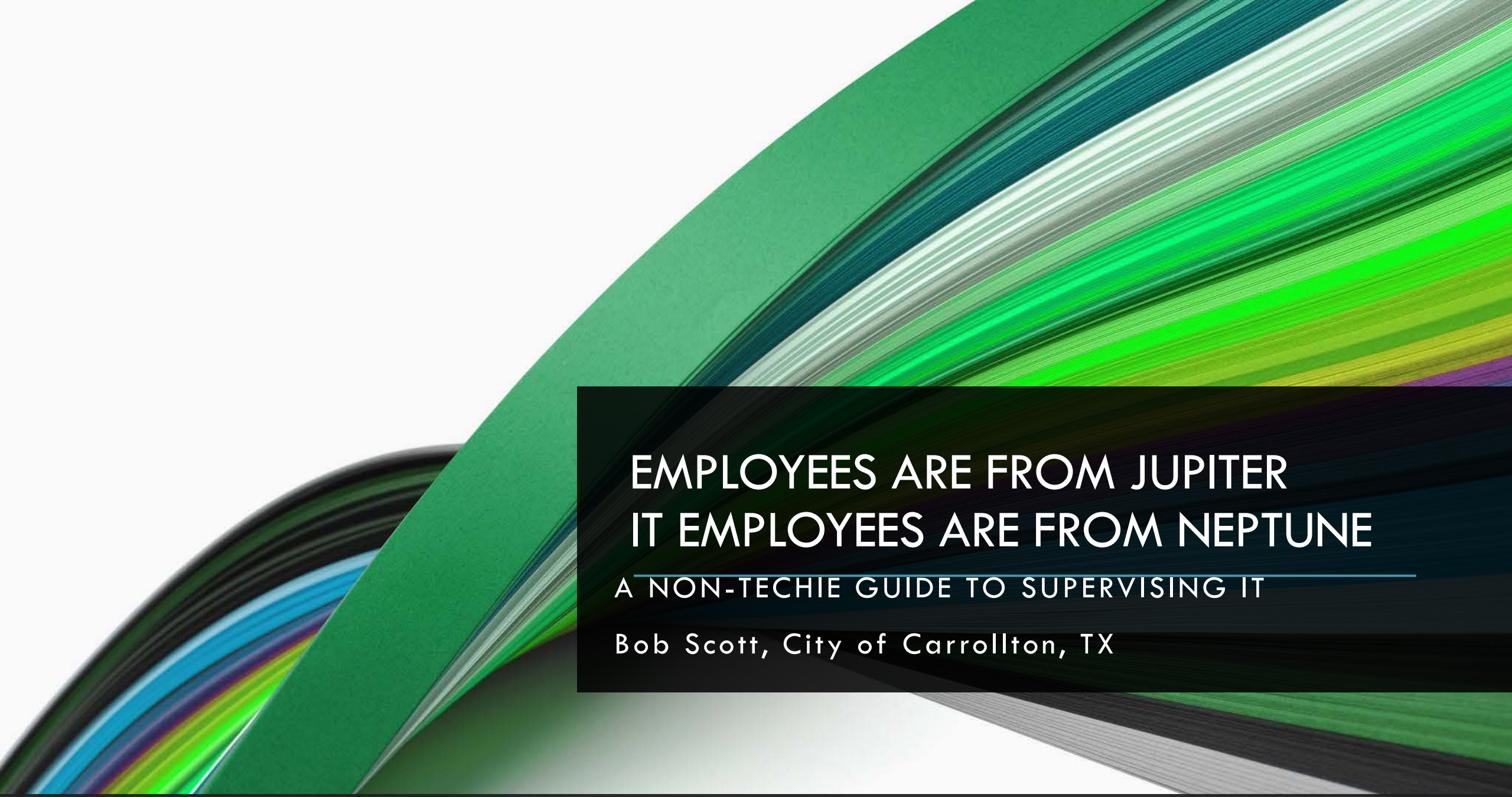


EMPLOYEES ARE FROM JUPITER IT EMPLOYEES ARE FROM NEPTUNE

A NON-TECHIE GUIDE TO SUPERVISING IT

Bob Scott, City of Carrollton, TX

Session Objectives

In just a few short years, IT has become omnipresent in every aspect of an organization's operations and strategic vision and yet executive's understanding and supervision of IT has not always kept pace. Accordingly, this session will:

- De-geek a highly technical topic through cliches and humor
- Create a small number of basic principles for effective IT supervision by focusing on Personnel, Architecture/Applications and Threats
- Provide practical explanations, examples and tools for each in order to obtain an efficient, effective and secure IT operation.

Personnel

Overriding Cliches for Personnel

Know What You Don't Know

Know What Your IT Staff Doesn't Know

Know What You Don't Know

Supervising IT is unique due to:

- Highly Technical Nature
- Extreme complexity and integration throughout the entire organization
- Constant and rapid evolution
- Vulnerability to and consequences of failure

A unique operation requires both unique approaches and expansions of proven supervisory techniques

Not spending the time to learn what you don't know is a frequent mistake

Sub-Cliches to KWYDK

If you understand the basics and big picture, the details will fall in place

You can't learn a foreign language without ever speaking it

Trust but verify

Understanding the Basics…

For computers and networks to be able to communicate with each other, common languages and protocols have been developed. Although some of the common players Microsoft and Cisco are trying to standardize the playing field; there are still as many variations of architecture as there are organizations. Useful terms to know:

- Network-the catch-all phrase for the servers, data storage, memory, switches and routers run on an operating system and connected using wired or wireless to run applications, serve the end users and connect them to each other and to the internet
- Servers-computers that process information, run tasks of both a utility and application nature including the saving and retrieving of information as needed. Servers can be on premise, remote or cloud based and physical or virtual
- Switches-hardware used to network multiple **computers** together with Ethernet ports.
- Routers-a networking device that forwards data packets between **computer** networks.

Understanding the Basics…

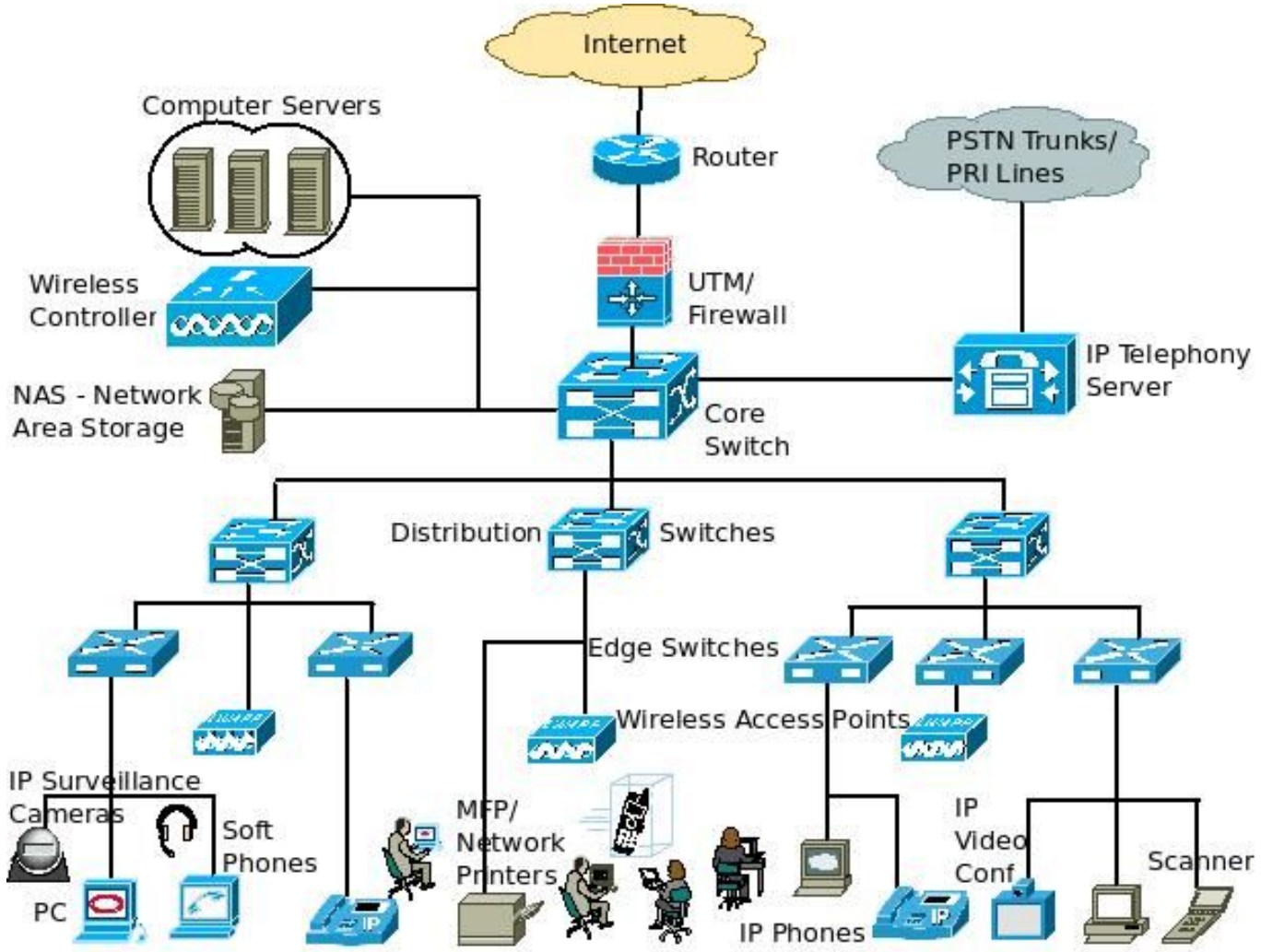
- Server Message Block (SMB)-the name given to the packets of information that are sent between devices
- EIGRP (Enhanced Interior Gateway Routing Protocol)-Cisco product for routing information within the network
- BGP (Border Gateway Protocol)-Microsoft protocol enabling computers to communicate between networks.
- SCCM (System Center Configuration Manager) Microsoft tool for automating updating and patching of devices.
- Ports-entry point to a network. Like a house with multiple doors and windows, a typical network will have many entry points to the network that the average user will not even be aware of but hackers are.
- Firewall-device that filters and logs all data entering a network
- Architecture-The design and framework of a network, including the characteristics of individual hardware, software, and transmission system components and how they interact
- Configuration-process of determining network settings, policies, flows and controls either on individual hardware or virtually.
- Segmentation- the process of dividing the network into "subnets" primarily for security. CJIS requires police systems be segmented from the remaining network
- Domain- Logical sub-grouping of computers but typically at a different level than a subnet and primarily for administrative purposes.

Understanding the Basics…

Active Directory and Active Directory Domain Services (AD DS)-part of windows operating systems is a directory of all authorized users. AD DS manages users, computers and allows system administrators to organize data into logical hierarchies. Also provides security certificates, single sign on.

- Organization → Group → Role → User
- Levels of Authorization
  - Enterprise Administrator (EA)-Highest level of administrative privileges. EA privileges is the grand prize for a hacker. EA access should be limited and not used for daily system administration.
  - Domain Administrator (DA)- Lower level of administration than EA but still quite powerful.
  - System Administrator (SA or sysadmin)-Typically for individual applications and often performed by the departmental owner as well as IT.

Typical Network



You can't learn a foreign language…

Don't allow yourself to be acronym-ed to death, ask for definitions; remember IT's complexity make acronyms a necessity.

Slow down the conversation or ask for plain English explanations, or better yet, have them draw it out. Ask to start with the big picture first, then the specifics of the issue

If you still don't understand, do some independent research and then ask again

Trust but Verify

The stakes are way too high to not independently verify:

- Follow up on red flags or problem areas described in this presentation
- Ask for a copy of the cyber-insurance application-was maximum coverage allowed
- Ask to meet with consultants and ask questions and review their reports
- IT by its nature is extremely data driven so numerous reports should exist, if they don't, that is a huge red flag
  - Aging of open help desk tickets
  - Logging reports
  - System scans and monitoring dashboards
- Ask open ended questions and pretend you're from Missouri

KWYISDK

The half life of knowledge is extremely short in the IT world with complexity and rapid evolution driving significant specialization. Implications include:

- Knowledge gaps can be costly and should be quickly identified
- Understanding that egos, embarrassment or a "shooting the messenger" management style can lead to bluffing when employees don't know or aren't sure.
- IT staff need to know that it is far better (and safe) to admit they don't know how rather than bluff. Create a safe environment for bad news and problem solving.
- Significant commitment to training and certifications need to be business as usual
- Unwillingness to openly communicate and collaborate across IT's functional areas adds to the knowledge voids (yes, silos can exist within IT, too). Teamwork is essential
- Outsourcing those skills not available in-house while recognizing some things should never be outsourced

Sub-Cliches to KWYISDK

Unicorns are hard to find and harder to catch

You can pay me now or you can pay me later (but later is more)

Pounding square pegs into round holes rarely works

Give them the skills to leave but make them want to stay

Unicorns are Hard to Find and…

An ideal IT Director/CIO will have:

- "Grown up" in one IT area: Administration, Network, Security, Project Management, or Operations/Customer Support but must understand and know how to be effective in all of them
- Vertical dexterity, aka being able to understand the 30,000 foot view but just as able to zoom down to the weeds to understand a technical issue or if a subordinate is bluffing
- Translation and presentation ability to put IT speak into plain English and sell the vision
- People and management skills to be able to manage and motivate IT employees
  - Willing to hire people who are smarter than they are
  - More concerned about team success than individual recognition

Since most won't meet all the criteria, you must decide which is the most important and how to compensate for missing qualities

You can pay me now…

Sticker shock and IT salaries are often synonymous terms but hiring unqualified employees can cost you even more so consider:

- Developing a separate IT pay plan
- What is vital to keep in-house and use outsourcing for the rest
- Know exactly the skill sets and indicators of those skills (i.e. certifications) that you are looking for because the last thing you want is to pay an exorbitant salary and get a dud

Square pegs

IT has become so complex and rapidly evolving that specialization is a necessity so know that:

- Learning on the job without an experienced mentor in that specialty can be disastrous
- Even a new employee with the right skills can struggle without good documentation to guide them
- Due to its highly technical nature, certifications **matter more** in IT than in other parts of the organization, but the **right** certification matters the most
- As important as technical skills are, don't forget organizational fit and if hiring from the private sector making it clear how government is different both good and bad

Give Them the Skills to Leave but…

Turnover is inevitable and common in IT due to:

- High demand for IT skills
- Easy cross-over between government and private sector IT
- Intense salary competition fostered by greater flexibility in the private sector

In addition:

- New technology and new vendors require constant training and development
- These new skills will make them extremely marketable elsewhere

Therefore:

- Develop a reputation for training and development
- Focus on quality-of-life and work/life balance issues
- Work to create comradery and teamwork within the department
- Foster the relationships with and between IT Director and staff. Your IT staff can be your best recruiting tool

Architecture and Applications

Overriding Cliches for Architecture and Applications

Complexity Demands Precision, Uniformity and Redundancy

Expediency is the # 1 Enemy of Excellent IT

What You Are Asking For May Not Be what You Want

Sub-Cliches for Architecture and APPs…

You can’t manage what you don’t measure , and you can't measure what you are not logging.

Not knowing what to expect multiplies the surprises

High SPF’s are only good in sunblock

Refreshment is more than just replacement

“But it works” is a scary thing to say in IT

Buy Once, Use Many

You can’t learn to swim by watching someone else get in the water

Complexity Demands Precision…

Even a relatively small network will contain thousands of components (switches, routers, servers, pc's, printers, etc,) running hundreds of applications, using specified configurations and protocols and transmitting millions of instructions and data packets daily. A lot can go wrong!

Precision and uniformity will not happen without:

- Strong policies backed by management buy-in
- Centralizing most software and hardware through IT-just say no to rogue devices and software
- Strong protocols for pushing software updates and patches
- Trained IT staff that follow and enforce the chosen protocols and configurations
- Routine scanning to ensure all assets are captured
- Robust monitoring of the system

Complexity Demands Precision…

Even with discipline, complete uniformity may not be possible:

- Applications that will only work on a certain version of a certain browser
- Applications that will only work with certain versions of adobe or other products
- Outdated hardware that prevents updating to the latest version

Signs to look out for:

- Large number of single user failures or helpdesk requests
- Patches that cause problems with some users but not others
- IT not able to provide a comprehensive list of assets and software in the network including how many versions of the same software are being run or how many versions of the same device exist or how many devices have already reached end of life by year.

You Can't Manage What You Don't Measure and You Can't Measure…

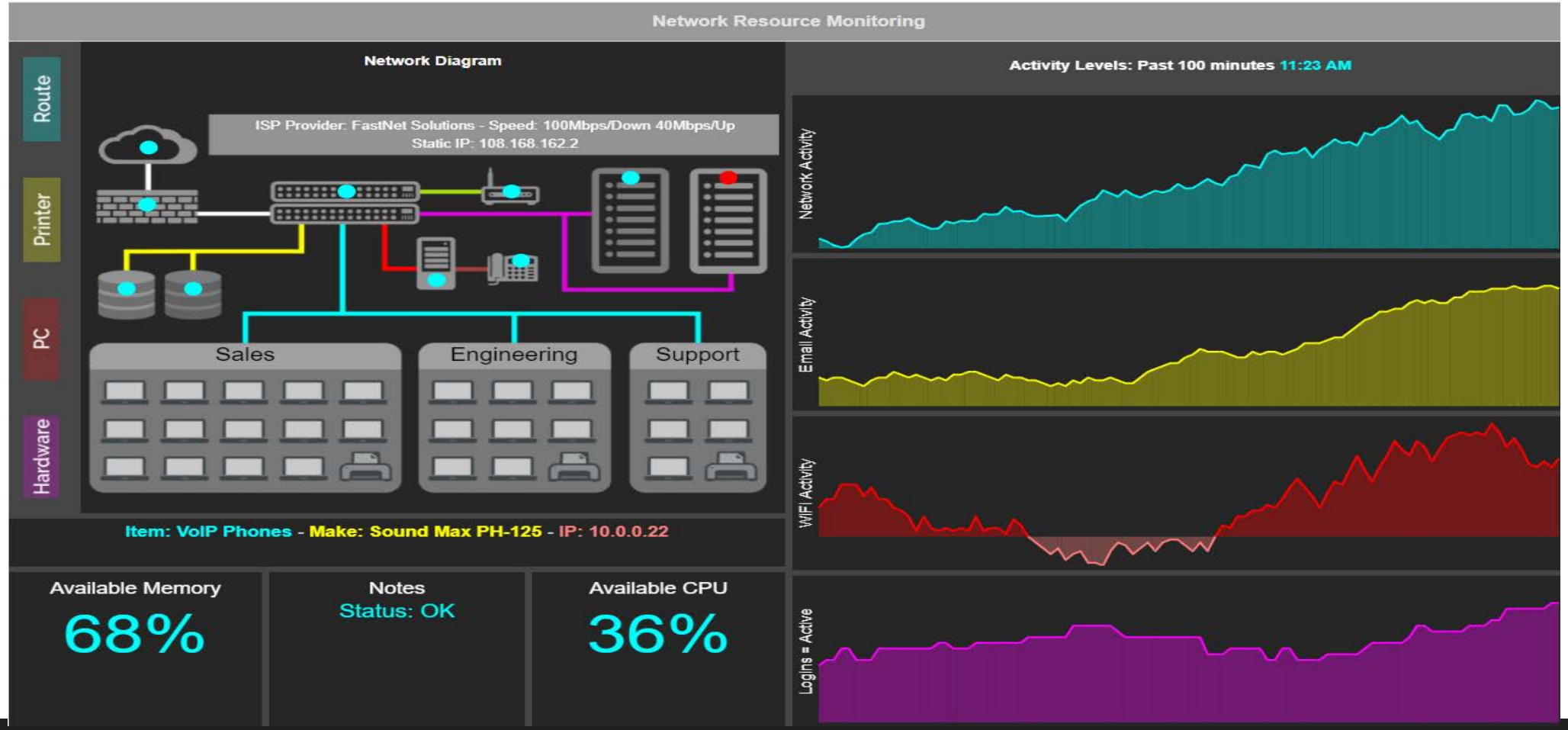
Many IT Departments are data rich but information poor

Some however, are not as data rich as they easily could be because they don't utilize logging software appropriately

Data aggregation software can take the millions of bits of data and aggregate it into meaningful measurements. Key factors:

- Knowing what to measure
- Knowing how to interpret what you're measuring
  - High priority Red Flags
  - Lower priority trend or issue to monitor
- Having the time, knowledge and resources to follow up on what you learn

Monitoring Dashboard-System



Monitoring Dashboard-Security

Not Knowing What to Expect…

Patches, routine updates or other changes often break something due to:

- Improper configuration, setup, and/or operations
- Lack of review and testing before pushing out an update
- Inconsistent setup or configurations of devices (i.e. some break and others don't)
- Not having all devices on the same version of software
- Poor or incomplete documentation of existing systems

Since no one wants to break things, needed updates are postponed which only compounds the problems making it even more difficult to maintain and secure the system

Expediency is the # 1 Enemy of IT

An amazing number of IT transgressions occur due to expediency:

- Shared Passwords
- Patching what should be replaced
- Improper or lack of labelling of cabling or ports
- Incomplete or missing documentation
- Too many employees with administrative privileges
- Installing new equipment or software without reading the instructions (Women, I know what you're thinking)
- No routine review of change logs (I mean-what could possibly happen)
- Poor IT Hygiene-remember the jobs not done until you clean up afterwards
- Sloppy procurement practices including:
  - Not completely analyzing business needs in advance resulting in poor or incomplete specifications
  - Not leveraging readily available research on products from Gartner, Forrester etc.

Remember-faster is not necessarily efficient or better

High SPF's Are only Good in Sunblock

A robust, resilient network has redundancies and the ability built into many systems to seamlessly switchover following a failure of the primary.

When systems go down frequently (even for good reasons) it could be indicative of a single point of failure (SPF)

Cost/Benefit may be the reason given but even for lower priority systems, advancing technology and virtualization has made eliminating SPF's more achievable

Refreshment is More Than Replacement

Every asset in the network has a useful life and should be scheduled for replacement the day it is installed, typically called a technology refresh cycle

- 5 Years for Infrastructure
- 3 Years for end points (computers, laptops, building cameras, desk phones)
- 2 Years for Ipas, iPhone, etc.

Often the old is simply replaced with the new without utilizing new capabilities or considering if the existing configuration is optimal

- This could be a sign of lack of knowledge, training, time or resources resulting in a staff who stays with the “known” out of fear that they may break something.
- It is also another form of expediency

"But it Works" Is a Scary Thing to Say in IT

Electrical fires are the result of wiring that "worked" for a while until it didn't

Just because an application is "*working*" does not mean that it is working right or that a disaster is not imminent. IT employees must:

- Ensure that the configurations chosen have not created security vulnerabilities
- Back ups are being done on schedule and produce usable data for restoral
- Hardware is being refreshed on schedule
- Software is being patched and updated and has a useful life left (i.e. continues to be supported)

What You Are Asking For May Not…

IT has become so integrated into every department's business processes that it has become impossible to function without it.

Imagine an organization that decided all supervision of employees would be performed by HR

As dysfunctional and inefficient as that sounds, we often try to do the same with IT by seeking turnkey IT solutions with only minimal departmental involvement or understanding

The result is both predictable and avoidable if from the director down, the time is invested to know the tradeoffs of the various solutions and the department is closely involved in every step.

Buy Once, Use Many

The diversity and many lines of business in a general government often result in numerous applications. Carrollton:

- Has 10 computer applications that record revenue for the city
- Thirty- four separate, significant department applications supported by three application support personnel in IT
- At any given time is in the process of acquiring and implementing three to four independent applications

With increasing functionality and flexibility of computer applications, the potential cost savings of utilizing one application for multiple purposes and multiple departments is huge.

You Can't Learn to Swim by Watching

Departments often expect IT to have all the knowledge of not only the application itself but of the department's operations, how they use the application and what reports they need.

The reality is that the application is a tool to make their operation more efficient and the department will only fully utilize the tool if they understand it from various perspectives

Consider requiring departments to have at least one technically oriented position in the department, build it into the job description and interview for it. Include IT in the interview panel.

Threats

Overriding Cliches for Threats

We Have Met The Enemy And They Are Us

Cybersecurity Is a Cat and Mouse Game of One Upmanship

That's Why We Play the Games

Sub-Cliches for Threats

The shoemaker's kids always go barefoot

Vulnerabilities, we control, Threats not so much

IT General Controls are not just an IT thing

Security is everyone's job

What you don't know will hurt you

We Have Met the Enemy…

Recent headlines have conditioned us to think of threats as being external

- Many bad outcomes are strictly internal
- Even when the threat is external, internal issues are often the reason for the threat's degree of success

Areas creating a soft target or a failure waiting to happen include:

- Inadequate training
- Obsolete hardware or software
- Inadequate staffing
- No monitoring or incomplete monitoring
- Poor architecture or segmentation
- Not applying updates in a timely manner
- No review of change logs
- Insufficient back ups and restoral procedures
- Poor IT hygiene

The Shoemaker's Kids Always…

Bonus Cliché: Do what I say, not what I do.

Let's face it, this is basic human nature and not isolated to IT but in IT the consequences can be huge. Examples include:

- Sharing the same system administrator passwords between staff
- Never replacing certain IT passwords for years at a time
- Keeping the default password that came with the hardware
- Abusing access privileges for inappropriate reasons

Cybersecurity is a Cat and Mouse Game

When asked why he robbed banks, the robber replied "*because that's where the money is*":

- Hacking has become a big-time business and like any good businessmen hackers are constantly analyzing return on investment and response rates
- When revenues drop below desired levels, strategies and tools are changed or adapted
- In addition, technology's rapid evolution provides ample opportunity to exploit unknown weaknesses contained in new versions, new connectivity or new functionality

As a result, the job is never done, and organizations must remain constantly vigilant in maintaining current versions of software and having a nimble and robust incident response plan in place.

Vulnerabilities we control, Threats…

Vulnerabilities are known weaknesses in software, hardware or system configurations that a hacker can exploit

- Software is available that can track and report vulnerabilities
- What that software monitors and what it doesn't depends on how it is installed and configured
- New vulnerabilities are constantly being discovered so don't be surprise by spikes
- Vulnerabilities will often be classified by the sophistication needed to exploit it

We don't get to choose which threats and when they will come so reducing vulnerabilities and constant monitoring for early threat detection is the best defense.

Hackers can be divided into four categories:

- White hats-ethical hackers that use their skills to help organizations harden their defenses
- Novice
- Sophisticated
- Nation state

IT General Controls Are Not Just an IT Thing

In 2013, the Committee of Sponsoring Organizations (COSO) updated their Integrated Internal Control Framework adding a principle on general controls over technology:

- General Controls do not relate to any specific application but instead is what happens in the IT department
- The message to finance and top management was clear that IT general controls are no longer just a black box that can be left to IT department
- We are now to the point that the worlds best controls outside of IT and terrible controls inside IT = terrible controls.

Security is Everyone's Job

U.S. Local governments are a favorite hackers target because:

- High visibility and wide-open websites that provide lots of information (aka transparency)
- Perceived easy target
- Perceived wealth and desire to avoid long outages or negative publicity

Most successful hacks come via e-mail making every employee a target

- Every employee should view themselves as an important part of the security effort
- Frequent on-line tutorials explaining new phishing strategies and spotting red flags
- IT led phishing campaigns should be conducted to identify vulnerable employees needing more training
- Standard procedures should be established for identifying suspicious e-mail to IT

That's Why We Play The Games

You can install the best security and monitoring software and diligently reduce vulnerabilities but until tested by a talented White Hat, whether your system is secure is nothing more than speculation

Tips for meaningful penetration testing:

- Hire a company with a reputation for finding things
- Have a complete listing of all assets and IP addresses
- Contract for both internal and external penetration system
- Even if they are being engaged for a specific purpose i.e. HIPPA audit do not limit their scope-let them roam

What You Don't Know Will Hurt You

The recent Solar Winds hack in which malware stayed buried for months without knowledge highlights the danger:

- Malware embedded in application or system software can exist undetected for months or longer
  - This malware may transmit sensitive information and then later be removed to hide the breach
  - It can also serve as a Trojan Horse timed to delay deployment to render recent back ups useless
- Escalation of access privileges for a compromised user can also pose severe threats
- Indirect or sidecar attacks with malware being imbedded in software from trusted vendors is also a threat

While you will never eliminate all risks close monitoring of system changes and outbound transmissions is now a must

Appendices

A-COMMON CERTIFICATIONS

B-GENERAL CONTROLS OVER TECHNOLOGY

C-AVAILABLE SECURITY RESOURCES

Common Certifications

APPENDIX A

Common Certifications

GENERAL

Information Technology Infrastructure Library (ITIL)- Developed by UK government but now separate joint venture, ITIL is a series of IT best practices and checklists that help align the IT function with the needs of the business. Checklists are not industry, technology or business specific so must be considered a high-level guideline. ITIL certifications are available to individuals.

Control Objectives for Information Technology (COBIT)- IT governance framework developed by Information Systems Audit & Control Association (ISACA) offers CRISC (Certified in Risk & Information Control) and CISA (Certified Information Systems Auditor)

Common Certifications

SECURITY

CISSP (Certified Information Systems Professional) offered by the International Information System Security Certification Consortium $(ISC)^2$ This the preeminent certification for security. Any medium IT shop or larger should have at least one.

CISM (Certified Information Security Manager) offered by ISACA.

CompTIA Security+. Basic certification that would benefit any IT employee.

PROJECT MANAGEMENT

PMP (Project Management Professional) offered by Project Management Institute (PMI).

CAPM (Certified Associate in Project Management) offered by PMI.

PMI PBA (PMI Professional in Business Analysis) offered by PMI.

Common Certifications

NETWORKING

CompTIA Network+ -General networking knowledge that is not specific to individual manufacturer.

CCNA (Cisco Certified Network Engineer)- CISCO specific networking certification that is generally considered more difficult to obtain than CompTIA+. CISCO has about 50% market penetration.

SYSTEM ADMINISTRATION/ENGINEERING

MCSA (Microsoft Certified Solutions Associate) Lower level certification for Microsoft operating systems.

MCSE (Microsoft Certified Solutions Expert)-Microsoft cloud computing including Azure MCSA and three years Azure experience are prerequisites

Common Certifications

SYSTEM ADMINISTRATION/ENGINEERING

OCA (Oracle Certified Associate) –Lower level Oracle certification.

OCP (Oracle Certified Professional)- Oracle Linux System Administrator which requires OCA , Linux 5 and Linux 6 certifications as pre-requisites.

RHCE (Red Hat Certified Engineer)-Linux based expertise which requires RHCSA (Red Hat Certified System Administrator) for pre-requisite.

CompTIA-Server+-Not specific to any operating system.

Common Certifications

DATABASE

Oracle Database Administrator- Three levels Oracle Certified Associate (OCA), Oracle Certified Professional (OCP) , or Oracle Certified Master (OCM) but each certification is version specific and not transferrable to other versions.

Microsoft for SQL Servers- Three levels Microsoft Technology Associate MTA-Database, Microsoft Certified Solutions Associate MCSA-Database and Microsoft Certified Solutions Expert MCSE-Database.

General Controls Over Technology

APPENDIX B

Application vs. General Controls

Application controls are simply the automated version of what we have always done:

TRADITONAL	AUTOMATED
Locked filing cabinet	User ID and Password
Physical segregation of duties	Password hierarchies that segregate duties through screen access
Illegible initials on paper invoices	Automated workflow approvals
Manual review, paper forms, footing of inputs	Input controls, automatic population of certain fields, edit checks
Using reports to monitor and control budget	System controls that refuse to process transactions if budget authorization is inadequate.

Application vs. General Controls

General controls represents what happens in the IT department to keep:

- computers connected.
- data bases humming.
- applications running and reliable.
- response times fast.
- information trustworthy.
- hackers at bay.

In addition, when bad things happen, general controls ensure rapid recovery and post-incident analysis and remediation.

Importance of General Controls

COSO 2013 Principle 11 states: **Selects and develops general controls over technology.**

To single out general controls over IT from all other control activities signifies their importance to the entire organization. Expressed another way:

> *"If top management does not know and control what happens in the IT department, then they are deluding themselves regarding the effectiveness of their entire system of internal controls"*

IT General Controls

ADMINISTRATIVE CONTROLS

- Alignment with strategic goals
- Policies
- Risk assessment
- Administer Security program
- Hiring and screening
- User access process (new user, terminations, changes)
- Access authorization
- License Management
- Change Log monitoring and reconciliation
- Contingency planning / business continuation/ data backup
- Budgeting for maintenance, upgrade and replacement aka-sustainability

PHYSICAL CONTROLS

- Facility access controls
- Workstation controls
- Device and media controls
- Facility maintenance
- UPS
- Back up facilities

IT General Controls

TECHNICAL CONTROLS

- Authentication controls (password, etc.)
- Access controls (operating system, application)
- Audit controls (monitoring and testing)
- Encryption controls
- Architecture controls (firewalls, VPN, etc.)
- Configuration controls

VENDOR MANAGEMENT CONTROLS

- Contract language (confidentiality, ownership, regulatory and legal compliance)
- Performance monitoring and enforcement
- Controls audit, SOC/AT-C 801
- Vendor access control
- Vendor copies of confidential information

IT General Controls

SECURITY CONTROLS

- Perform an Information Security Risk Assessment
- Security incident response
- Security awareness & training-every employee who has access to a computer should consider themselves a security team member
- Threat monitoring
- Regularly test or monitor effectiveness of controls
- Have outside party perform penetration testing
- Periodically evaluate and adjust the Information Security Program

Security Resources

APPENDIX C

Leveraging Shared Services

Texas Department of Information Resources (DIR) awarded AT&T a Managed Security Services (MSS) contract:

- Available to all governments in Texas
- Offers a menu of ala carte services within three categories:
  - Security Monitoring and Device Management
  - Incident Response
  - Risk and Compliance
- State agencies are now required to perform a cybersecurity assessment every two years. Local governments would be smart to follow the model.

My Favorite Four Letter Word-**FREE!**

The Department of Homeland Security (www.dhs.gov) offers a variety of free services to state and local government https://www.dhs.gov/sites/default/files/publications/4_stc-dhs-state-offerings.pdf including:

The Cyber Security Evaluation Tool (CSET) cset@dhs.gov and https://ics-cert.us-cert.gov/Assessments

The Cybersecurity Assessment and Risk Management Approach NCSD_CIP-CS@dhs.gov

The SANS Institute is a cooperative research and education organization (www.sans.org) specializing in IT Security. The offer a variety of free resources and for fee courses, conferences and certifications.

Also, inquire of your cyber policy insurance carrier regarding assessment resources or pre-identified consultants that can help