Understanding IT Like An Insider

A NON-TECHIE GUIDE TO UNDERSTANDING AND WORKING WITH IT

BOB SCOTT, DEPUTY TOWN MANAGER PROSPER, TX

GFOAT SPRING PRE-CONFERENCE

GFOAT
Government Finance Officers Association of Texas

Y2K, AI, and Hackers are NOW!

In the late 20th century, Y2K was the widespread fear that computer systems had become so connected within and between entities that a common software flaw (two-digit years) would cause massive computer outages that would cascade around the world. The new millennium arrived without incident.

Fast forward to July 2024, a security sub-contractor for Microsoft named CrowdStrike installed a faulty software update that crashed 8.5 million operating systems world-wide causing global disruption of vital services with media referring to it as Y2K "like". A similar but less impactful incident had occurred from a Microsoft update a few years earlier.

Generative AI has exploded in use and is quickly becoming integrated into IT Systems and user applications. It represents both great potential and great risk. Risks include erroneous results, violating privacy laws, compromising entity security and non-compliance on restrictions on government use.

Plus, hacker related attacks from around the world have multiplied and are a constant threat.

***** KNOWING IT like an Insider can help leaders invest in the right IT Solutions and Controls**

Session Objectives

IT has quickly become omnipresent in every aspect of an organization's operations and strategic vision and yet **executive's understanding (IT Literacy) and resulting supervision of IT has not always kept pace.**

Finance, whether it supervises IT or simply helps executive management with IT budgets and internal controls must have a basic understanding of the IT environment.

This session will:

- De-geek a highly technical topic through clichés and humor
- Create a small number of basic principles for understanding what makes IT effective by focusing on four topics: Big Picture, Personnel, Architecture/Applications and Threats
- Provide practical explanations, examples and tools for each to obtain an efficient, effective and secure IT operation.

Overriding Clichés for Understanding the Big Picture

Know What You Don't Know (KWYDK)

It's Not Until the Tide Goes Out That You Know Who Is Swimming Naked

Sub-Clichés for KWYDK

- If you understand the big picture you can drill down as needed.
- You can only learn a foreign language by practicing.
- Love it or Hate it, Generative AI is the New Normal
- Technology is Amoral

Know What You Don't Know

Understanding IT is unique due to:

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

Most executive management that IT reports to have never worked in IT.

A unique operation requires unique understanding, approaches and rigorous use of proven supervisory techniques

- Ask questions and take the time to learn
- Compare your IT teams against industry standards & frameworks
- Ask about "behind the scenes" tasks and whether they are getting done
- Use experts to perform Operations and security reviews **and** implement recommendations

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

Understanding the Basics…

For computers and networks to be able to communicate with each other, common languages and protocols have been developed. Large vendors like Microsoft, Cisco, Google, Amazon AWS are trying to standardize the playing field; there are still as many variations of architectures.

Useful terms to know:

- Architecture -The design of a network, application, security control or IT infrastructure, including the characteristics of individual hardware, software, and network components and how they interact.
- Network - the catch-all phrase cabling, switches, routers, and internet connections using wired or wireless technologies that serve to connect end users to systems and each other.
- Routers & Switches - hardware used to network multiple **computers** together with Ethernet ports and forward data packets to the right destination.
- Firewall - device that filters and logs all data entering a network
- 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.
- Configuration-process of determining network settings, policies, flows and controls either on individual hardware or virtually.
- Scanning and Mapping software- Tool used understand the configuration and applications running in a network including vulnerabilities.
- Media Access Control (MAC) Address- physical and hardware address for each computer and device on a network including the manufacturer and device type. Can be spoofed.
- Internet Protocol (IP) Address- a logical address assigned to a computer when it joins a network that allows all computers in the network to communicate with each other and to the internet if the network is so connected. **When you get on Wi-Fi at a hotel or Starbucks you are connecting first to a network and then to the internet.** The internet can also be accessed directly through an Internet Service Provider (ISP) or indirectly through a network.

Understanding the Basics…

- Segmentation- the process of dividing the network into "subnets" primarily for security. CJIS requires police systems be segmented from the remaining network. A common method of segmentation is the creation of DMZ's and firewalls. **Mapping and credentials are the kryptonite of segmentation.**
- Servers- computer that process information, run tasks of both a utility and application nature including the saving and retrieving of information as needed. Servers can be physical or virtual and located on premise, in a remote data center or in the cloud.
- Operating System (OS)- primary software on a computer that manages the computer's user interface and resources like memory, hardware, and software applications. For example, Windows, MacOS / iOS, and Linux (many cloud-based applications)
- Domain-Logical sub-grouping of computers but typically at a different level than a subnet and primarily for user administration purposes.
- User Directory- a centralized repository where user profiles (usernames and passwords) are stored.
- Microsoft Tenant-A cloud-based account dedicated to a particular customer. Likewise, an Amazon AWS account.
- Virtual Private Network (VPN)- a secure point to point digital connection protected by encryption and masking of IP addresses enabling safe and secure remote work or an inexpensive way to connect branch offices via the internet to the network. With VPNs often bypassing firewalls and other perimeter protections, MFA should be used for the remote computer.

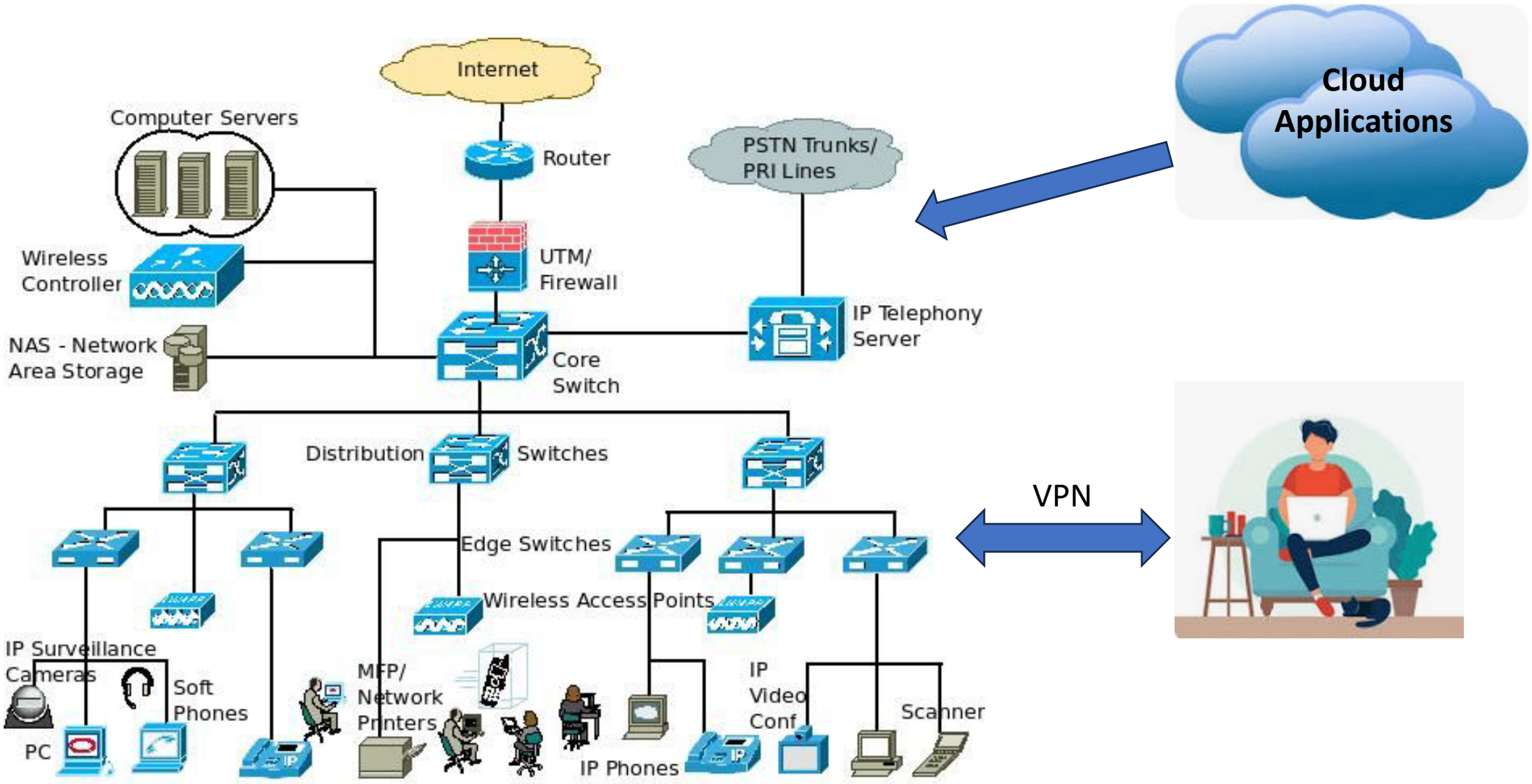
Understanding the Basics…

- Application Programming Interface (API)- programming that coneects and facilitates the transer ofdata and information between separate and specialized applications.
- Single Sign On - Solution that allows users to sign on to various applications using the same password.
- IT Hygiene- broad term for the best practices and procedures used to maintain the efficiency, effectiveness and health of the digital infrastructure. Basically, it's the things you should do but nothing bad happens **immediately** if you don't.

Microsoft Active Directory and Azure AD/Entra – a directory of all authorized users, computers and other resources; allows system administrators to organize data into logical hierarchies. Also provides security certificates and ability for single-sign via integrations.

- Organization → Group → User →Role
- Levels of Authorization
  - Enterprise Administrator (EA)-Highest level of administrative privileges. **EA privileges are 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. **Another big target of hackers.**
  - System Administrator (SA or sysadmin)-Typically for individual applications or databases and often performed by the departmental owner as well as IT.
- Levels of Azure Authorization
  - Global Admin - allows admins full access to all Azure resources using the respective Azure AD tenant. **Another big target for hackers.**

Typical Network



You can only learn a foreign language…

Ask IT for some self-study material –show interest

Don’t allow yourself to be acronymed 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

Generative AI-The New Normal

AI has been around a long-time.

- Apple's Siri is a teenager (14) and MS grammar check is older than that.
- However computing capacity and programming had limited AI to predetermined tasks and questions

The AI world has changed

- The video game industry and their need for super fast processing and life-like "on the fly" animation drove the need for far faster and more flexible GPU's (gaming processing units) vs. traditional CPUs
- Nvidia stepped into the void for the video game world and is now the "darling" of AI chips.
- The capability of Nvidia's chips has made Generative AI that can take existing information including images, audio, and extensive datasets and generate new content including the ability to learn over time.
- Generative AI, however, is only as good and as accurate as the datasets it draws material from with end users seldom knowing the source
- The old adage ***"Garbage In, Garbage Out"*** **still applies but it is now more grammatically correct and polished garbage.**

Generative AI-The New Normal

Specific Risks of AI/Generative AI include:

- Certain AI platforms are legally prohibited for government or individual departments (DeepSeek-all governments, Chat GPT-Criminal Justice applications)
- Harvesting and inclusion in datasets of PHI or PII or other protected information (such as which brand of firewalls you use) by AI applications.
- Incorrect or deceptive information is generated.
- Built in bias in the AI generated analysis
- Violation of copyrights
- Use of AI to defraud the organization.

Government's IT departments must get ahead of AI use quickly by adopting policies that address:

- All AI tools must be approved and obtained with licenses by IT. Personal AI tools are **not** allowed for government and criminal justice applications.
- When use of AI tools is appropriate and when it is not.
- Protecting PII and confidential information.

Generative AI-The New Normal

- Double checking sources and proofing AI generated material.
- Labelling material that is significantly AI generated.
- Prohibition of bias, deceptive use and practical jokes including understanding how AI can be used to defraud the organization-always verify unusual digital request through independent means or in – person.

Describing acceptable and common uses:

- Drafting contracts, job descriptions and policies.
- Wordsmithing and improving flow or tone of a person written document.
- Conversational information retrieval (CIR) including data mining or more complex queries.
- Language learning and practice/Instant translation for non-English speaking citizens.
- Note-taking assistance.
- Researching new topics and receiving executive summaries or synopsis.

Technology is Amoral

Some of Technologies **greatest strengths** and most useful tools also represent some of the **greatest risks/threats** to our organizations. Examples include:

- Internet itself. The ability to instantly connect and exchange information anywhere in the world is synonymous with modern life but also creates a complexity to systems and ability to be attacked from anywhere in the world.
- Encryption. Originally developed to protect data and privacy and used every day in multiple applications, it has now become synonymous with ransomware.
- Flexibility in Configuration of Applications. The ability to perform a task in multiple ways or to customize the application to best work with your specific applications and needs can create vulnerabilities and "back doors" into the network. For example, the ability to set up users on active directory, other operating systems or as stand-alone users means that there are multiple default passwords that all must be changed to avoid unlocked back doors.

Sub-Clichés to "…Swimming Naked"

Every organization is subject to the same type of IT risks, but not all organizations are affected equally:

CrowdStrike July 2024 outage:

- **American Airlines-same day recovery with 51 cancellations**
- **Delta Airlines-five days to recover with 7,000 cancellations.**
- Southwest Airlines scheduling system collapse during December 2022 winter storms is another example.

Sub-Clichés "It's Not Until the Tide Goes Out That…

- "But it Works" is a scary thing to say in IT
- Trust but verify

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

Electrical fires are the result of wiring that "worked" right up until it burned the house down

Just because an application or network hardware 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
- Redundancy is built into critical functions
- Hardware is being refreshed on schedule
- Patch protocols determine when testing is appropriate before installation
- Software is being patched and updated and has a useful life left (i.e. continues to be supported)

Trust but Verify

The stakes are way too high for finance or top management to not independently verify:

- Follow up on red flags or problem areas described in this presentation
- **Review IT's General Controls over Technology** (discussed later)
- **Ask to meet with IT consultants, including Pen Testers and ask questions and review their reports**
  - Consultants should know they are also working for top management not just the IT Director
- 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 and knowledge of baseline activity
- **Does your entity complete CISA's National Cybersecurity Review (NCSR) or similar external document-if no, why not, if yes ask for a copy or other internal Best Practice checklists…**
- Take the time to learn!

Big Picture-Question 1

Cities are typically legally required to segment their systems.

a) True
b) False

Big Picture-Question 2

Which is **not** true regarding Generative AI

a) Its end product is only as good as the data sets it draws from

b) It is regulated by a strict set of Federal rules and regulations that protect privacy and discourage inappropriate use.

c) It is here to stay and will only become more prevalent over time

d) Certain AI programs and platforms are prohibited for specific uses by governments

Big Picture-Question 3

Which would be a red flag for a payroll application that is currently performing well?

a) Monday at 9:00 am, it is running slowly

b) Vendor has provided end of life notification

c) The application is running several updates behind

d) The application generates frequent error/edit messages

e) All of the above

f) Both b) and c)

Big Picture-Question 4

A Tenant can be:

a) Specific applications that are hosted by a network on premises

b) A royal pain if they party too much and don’t pay their rent

c) Various applications that are hosted by one provider in the Cloud

d) The IT name for a sub-module of a larger application.

Overriding Clichés for Personnel

Know What Your IT Staff Doesn't Know

Unicorns Are Hard to Find and Harder To Keep

Sub-Clichés to KWYISDK

- 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

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 such as ultimate responsibility for IT direction and security
- Outsourcing also has its risks as contractors are often under both time and profit pressure and can take shortcuts. Consider requiring SOC reports or RAMP certification.

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 or passing basic skills tests) that you are looking for because the last thing you want is to pay an exorbitant salary and get a dud.
- Consider a simple skills test before the final offer

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

Personnel Question 1

IT Directors are considered Unicorns when:

a) They are willing to work for government pay

b) They understand all aspects of IT even if they only worked in one area

c) They are equally comfortable at the 30,000 foot level and in the weeds

d) Both b) and c)

Personnel-Question 2

To retain highly proficient IT staff, a government can:

a) Create an IT specific pay plan
b) Outsource for the skills that are most difficult to find
c) Grow your own through mentoring, training and certifications
d) Provide flexibility on hours and working remotely
e) All of the Above

Personnel-Question 3

Knowing that you can outsource the task but not the responsibility, which IT tasks should never be completely outsourced?

a) IT Help Desk

b) Applications Support

c) Network Support

d) IT Director

Personnel-Question 4

Certifications are particularly important in IT because:

a) IT tends to have high turnover with employees often switching jobs or industries making certifications an objective, verifiable measure of abilities.

b) IT skills and techniques are constantly morphing

c) Many skill sets are vendor specific and can best be learned from that vendor's own certification program

d) All of the above

Overriding Clichés for Architecture and Applications

Complexity Demands Precision, Uniformity and Redundancy

You Can’t Manage What You Don’t Measure

Expediency is the # 1 Enemy of Excellent IT

What You Are Asking For May Not Be what You Want Or Need

Sub-Clichés for Architecture and APPs…

- Not knowing what to expect multiplies the surprises
- High SPF's are only good in sunblock
- Refreshment is more than just replacement
- 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 …

Bonus Cliché: You can't fix a problem you don't know you have!

Many IT Departments are data rich but information poor

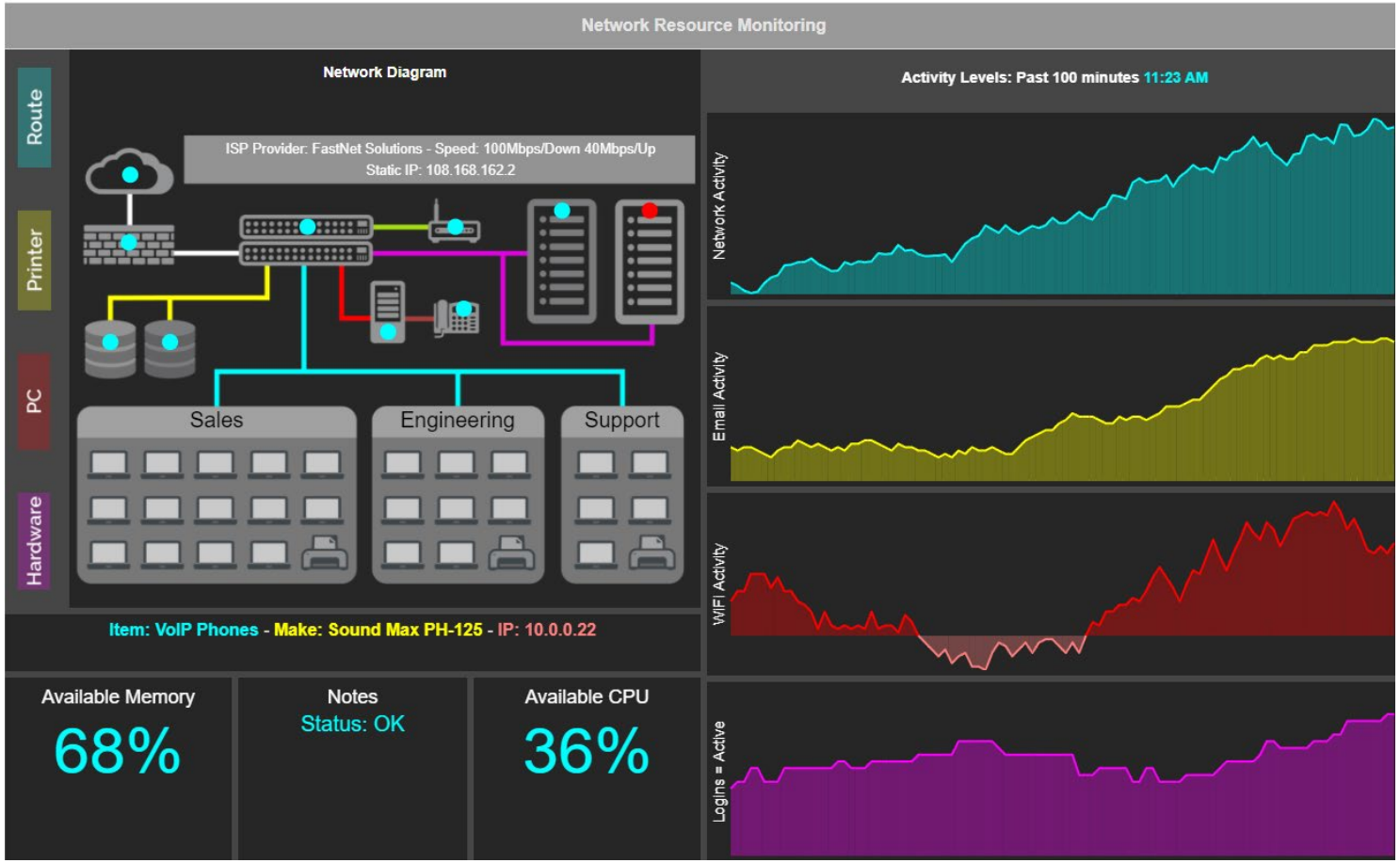
Some, however, are not as data rich as they easily could be because they don't log data appropriately

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

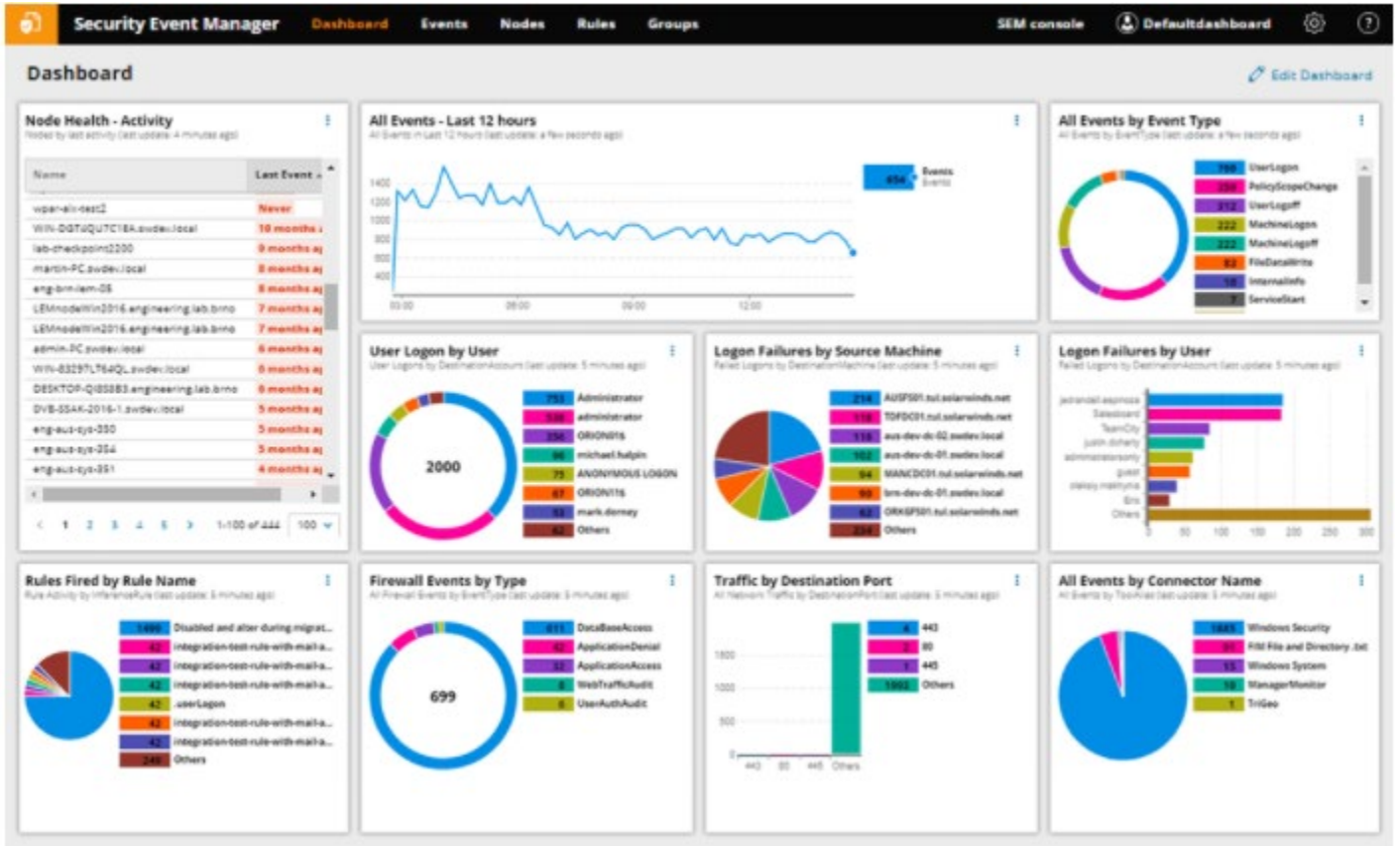
- Knowing what to measure
- Knowing how to interpret what you're measuring
  - Creating Baselines for the system- aka knowing what to expect and know when things aren't normal
  - High priority Red Flags
  - Lower priority trend or issue to monitor
- Having the time, knowledge and resources to follow up on what you learn

Security Information and Event Management (SIEM) is specialized software that evaluates abnormal activity and alerts administrators to possible threats.

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
- Inadequate training and supervision of personnel maintaining the system

Since no one wants to break things, needed updates are often postponed which 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
- Installing software patches before testing
- 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
- 3-4 Years for end points (computers, laptops, building cameras, desk phones)
- 3-4 Years for iPads, 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

Buy Once, Use Many

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

- Had 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.

What You Are Asking For May Not Be What You Want or Need

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.

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.

Architecture and Applications- Question 1

An example of poor IT hygiene is:

a) Deactivating a terminated employee in Active Directory but not deleting their profile

b) Not documenting a configuration change to a network router

c) Getting caught in the hallway by an employee, fixing their problem on the spot but not generating a help desk ticket

d) Not properly bundling and labeling cable runs

e) All of the above

Architecture and Applications- Question 2

A goal of refreshment is:

a) Replacing critical hardware before it fails

b) Taking advantage of new hardware technology to improve efficiency and reliability

c) Take a fresh look at network configurations to make sure they have been optimized

d) All of the above

Architecture and Applications- Question 3

Single Points of Failure can be:

a) Software
b) Hardware
c) Infrastructure (cabling, facilities etc.)
d) People
e) All of the above

Architecture and Applications- Question 4

Which of the following is not a benefit of frequent scans and data aggregation?

a) Increased security

b) More efficient network

c) Available forensic data in the event of a problem

d) Both a) & b)

e) None of the above

Overriding Clichés for Risks & Threats

We Have Met The Enemy And They Are Us

Cybersecurity Is a Cat and Mouse Game of One Upmanship

This is Why We Play the Games

Sub-Clichés for Risks & Threats

- We Have Met the Enemy and They are Us.
  - The shoemaker's kids always go barefoot
  - **Vulnerabilities, we control, Threats not so much**
- Cybersecurity is a Cat and Mouse Game of One Upmanship
  - IT General Controls are not just an IT thing
  - Always keep your cards close to the vest
  - Security is everyone's job
  - What you don't know will hurt you
- This is Why We Play the Games
  - It's not a matter of "if", it's **WHEN!**

Risk and Threats Definitions

Open Source Intelligence (OSINT) Information that an entity places on their website or an individual places on social media that a hacker will use often combined with other information to perform and attack.

Attack Vector- is the method the hacker chooses to attack an entity's network. It may be as simple as mass phishing campaigns employing social engineering or it can be more sophisticated based on research, scanning tools and other means. It can even be walking into a government's offices and plugging a thumb drive or computer into an unsecured network connection.

Deep/Dark Web- any part of the world wide web that is not indexed by a search engine and often use various techniques to hide their presence and secure activity from unwanted eyes. Hackers use the dark web to exchange information about potential victims and to sell stolen data or hacking tools.

Elevation of Privileges (EoP)-when a threat actor successfully penetrates perimeter security and is the network, they will often search for other user id's and passwords and if successful in hacking the passwords search for users that have been mapped to other parts of the network or have administrative privileges allowing them to move laterally through the network and perform more damaging attacks.

User Based Analytics - Software used to identify suspicious activity based on behavior.

Endpoint Detection & Response (EDR)-cybersecurity tool that continually monitors endpoints for suspicious activity and behavior and provides tools for investigation and response.

Defense in Depth (DiD)-cybersecurity concept of multiple layers of security controls to protect systems and data. If one layer fails, other measures are in place to stop or slow the attack until the attack can be detected and countermeasures deployed.

Security Information and Event Management (SIEM)-specialized software that collects, monitors, analyzes and correlates events and diverse data to develop baseline activity and behavioral norms to identify suspicious activity and possible threats.

Security Operations Center (SOC)- except for the largest of entities is a remote 24/7 service that monitors client security for numerous entities. In the event of a cyberattack, the SOC would react immediately with remotely deployed countermeasures while notifying client's IT staff of the issue and proposed response.

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:

- Incompetent staff
- 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
- Staffing levels and workload can be a factor

Be attentive around IT, do they demonstrate a culture and seriousness around security issues, do they have time to think about what they are doing?

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 businessperson, 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.

Five Most Successful Attack Strategies

1. **Compromised/Stolen Credentials**
2. **Phishing, Smishing (SMS texts) and Vishing (Voice and Voicemails)**
3. **Unknown "Zero Day" Vulnerabilities**
4. **Malicious Insider**
5. **Known-Unpatched Vulnerability**

Vulnerabilities We Control, Threats Not So Much

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 surprised by spikes
- Vulnerabilities will often be classified by likelihood and consequences of exploitation

Unfortunately, we don't get to choose how or when we will be attacked so reducing vulnerabilities and constant monitoring for early threat detection is the best defense.

Hackers can be divided into five categories:

- White hats-ethical hackers that use their skills to help organizations harden their defenses
- Hacktivist-someone who hacks or launches digital attacks because of social, environmental or perceived injustices
- Novice (Script kiddies)
- Sophisticated
- Nation state

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 finance and top management does not know and control what happens in the IT department, then they can't possibly know whether their entire system of internal controls is effective or not"

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.

IT General Controls

ADMINISTRATIVE CONTROLS

- Alignment with strategic goals
- Policies
- Risk assessment
- Administer Security program
- Least Privilege
- 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
- RAMP Certification

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
- Evaluation of partial or complete adherence to National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) by completing the National Cybersecurity Review (NCSR)

AICPA Gives COSO 11 a Shout Out

- In October 2021, the Auditing Standards Board of the AICPA issued SAS 145: *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement* effective 12/31/23 and forward (aka Now).
- Key provisions include:
  - Strengthens the requirements for understanding and assessing system of internal controls including the economic, ***technological*** and regulatory environment of the entity
  - Revises requirements to evaluate the design of certain controls within the control activities component, ***including general information technology (IT) controls***, and **to determine whether such controls have been implemented**;
  - Requires new approaches to evaluating inherent and control risk that will likely increase audit procedures
  - Creates a new "stand-back" requirement intended to drive an evaluation of the completeness of the auditor's identification of significant classes of transactions, account balances, and disclosures;

Expected Practices in IT

- All governments with a law enforcement function should require Criminal Justice Information System (CJIS) certification for all IT personnel for flexibility and additional screening.
- All system administrators (not just within IT) should consider having two (regular and administrative) id's to protect segmentation and prevent viruses from traveling like wildfire through the system. The tradeoff is more id's = more license fees and it can be cumbersome.
- Cross training, training, segregation of duties and Theory of Least Privilege should be business as usual
- Every IT department should have basic policies covering user responsibilities, expectations of privacy, security measures, passwords and training
- Complete Inventory and replacement schedule for Network equipment
- Complete List of all IP addresses (remember, each IP address is an entry point to your network and should be secure)

Expected Practices in IT

- Centralized License Management
- Robust Vendor Management Program including verifying that systems were installed as specified and all default passwords have been identified to IT
- Periodic penetration testing that is not subject to scope limitations
- Strong IT hygiene practices including:
  - Removal of terminated users from Active Directory
  - Wiping all devices prior to disposal
  - Periodic cleaning out caches on peripheral and network devices
  - Neat orderly and clearly labeled cable runs and data closets
  - Strong documentation
  - Timely patching and updates following strict protocols

Always Keep Your Cards Close to the Vest

An amazing amount of “hacker” useful information is readily available on-line and have facilitated many cyber attacks. Examples include:

- On-line check registers prepared under the Comptroller’s Transparency Stars program that hackers use in payment diversion frauds.
- Unclaimed property lists that contain so much information, unrelated parties can claim the property.
- Bid awards providing great detail regarding system hardware, firewalls, VPNs and security software used
- IT briefings not conducted in Executive Session.

Good security starts with being deliberate about not revealing too much

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

Historically, most successful hacks came 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

New Strategies such as using a stolen password and user id to VPN into the network are becoming increasingly common.

Passwords

Passwords when entered into a log -in screen are immediately converted into a long numeric hash using a hashing algorithm such as MD5, Bcrypt or SHA 256. These hashes can then be temporarily or permanently stored in caches for various applications.

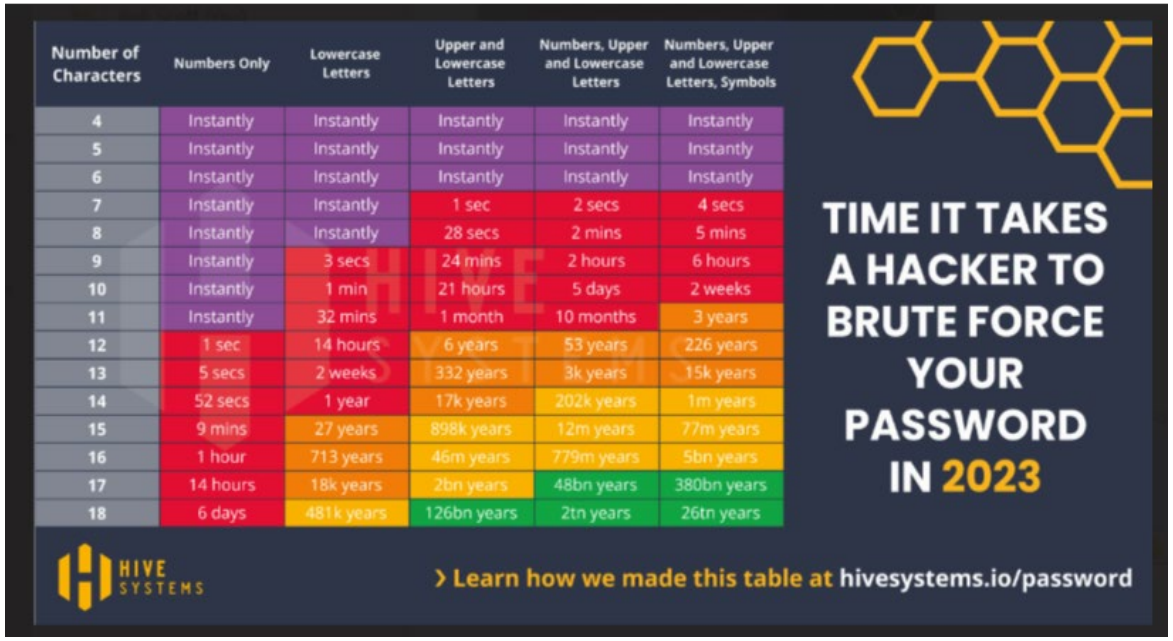
Passwords can be compromised in multiple ways:

- Convincing users to enter their password into a false (but authentic looking) log-in screen(possibly using a Man in the Middle strategy)
- Malware such as key stroke software secretly installed through phishing or other means
- **Finding caches of hashes on peripheral or network devices and either:**
  - **Using Rainbow Tables (Lists of known and common passwords and the resulting hash)**
  - **Brute force attacks**

VIRTUALLY EVERY SUCCESSFUL CYBERATTACK INCLUDES ONE OR MORE COMPROMISED PASSWORDS!

Not All Hashing Algorithms Are Created Equal

MD5 in 2023



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Bcrypt 2024

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090
Password hash: bcrypt

HIVE SYSTEMS

› Learn more about this at hivesystems.com/password

MD5 is a less complex algorithm that is prone to “collisions” (when multiple different passwords will produce the same hash value.

Password Rules to Live By

Since none of knows which algorithms are used by various applications and how many caches our hash is hanging out in, we should err towards strong (long and Complex)

- Set a minimum number of characters- 14 or more is typically safe if you use three or four levels of complexity
- Use words or phrases you will remember but modify to your choosing such as no vowels either in the middle or end and first or last letter is always upper case
- Pick a random number or symbol to always start with and a different to end with
- Use a different symbol for categories of accounts work=#, social media=*, financial=@, other =$
- For example: your Wells Fargo password using Conestoga Wagon as the base might be @34cnstgAwgn68@
- Another possibility 1$hOrse2*dOnkey3#mUle

Many IT Directors are now trading complexity and length for less frequency of password changes, but Quantum computing could change the tables dramatically.

Password Rules to Live By

- **DO NOT give hackers a head start!**
  - **These time to solve tables go to minutes or hours if the hacker can guess parts of your password and incorporate it into their brute force attack. Therefore:**
    - **Do not use the or variations of employer's name, your name, the name of the institution or other strongly correlated symbol as the starting point for your password!**
    - **Your work password should be completely different from any personal passwords.**
    - **Report any personal digital security attacks *(i.e. email, social media accounts, shopping accounts etc.)* to IT and immediately change your work password completely.**
    - **Do not use a digital password keeper unless it has multi-factor authentication.**
    - **Ensure that your personal wi-fi and smart house features are secured by robust passwords**
    - **Do not use security questions or password bases that are found on your Facebook page or other social media pages.**

Multi-Factor Authentication

MFA is a two-step authentication processing using one factor from two of three categories:

- What you know (i.e. password or security question)
- What you have (badge, number generating FOB, authenticator on phone)
- Who you are (biometrics-facial recognition, retina scan, fingerprint scan)

The user does not always know that MFA is being used as automatic authenticators can be loaded by IT onto their laptop.

This is 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. **The purpose of Pen Testing is to find the unexpected!**

Tips for meaningful penetration testing:

- Hire a vetted company with a reputation for finding things. There is a great list on the Texas DIR
- Have a complete listing of all assets and IP addresses
- Contract for both internal and external penetration system. If they are stymied by a control, give them access around it and have them continue testing.
- Even if they are being engaged for a specific purpose i.e. HIPPA audit do not limit their scope-let them roam. Challenge them to find something-PEN Testers love a challenge!

What You Don’t Know Will Hurt You

The 2020 SolarWinds (mapping software) 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

It's Not a Case of "If", it's **WHEN!**

Cyber attacks, natural disasters and inadvertent Y2K type incidents are inevitable. Organizations need to plan for these with three primary objectives:

- Limiting the Damage
- Recovering Quickly
- Continuing Operations in the Interim

Limiting the Damage. Consider:

- Physical security and locations of vital equipment
- Are back up facilities geographically diverse.
- Are Intrusion Protection, Detection and End Point Response (EDR) sufficiently robust

It’s Not a Case of “If”, it’s **WHEN!**

- Are system administrators only allowed to use their administrative id and password when they are specifically working on the system? All other typical employee activity (e-mails, web searches etc.) are on a separate id.
  - Don’t forget SCADA and any other department specific administrators not located in IT

Recovering Quickly. To recover quickly are:

- Are **RTO’s** and **RPO’s** (Recovery Time and Recovery Point Objectives) reasonable and reflective of current practice, systems and capabilities?
- **Have critical systems been pre-identified and prioritized in terms of what will be brought back first** (spoiler alert-it’s always payroll), second, third, etc. Do departments know where they are on the pecking order?
- Are retainers or consultants needed for recovery been pre-identified?
- Are certain physical assets such as spare pc’s isolated from the network?

It’s Not a Case of “If”, it’s **WHEN!**

- Are emergency contact lists up to date and alternate means of contacting key personnel quickly preidentified if office phones, email, teams and other traditional methods are unavailable?

Continuing Operations in the Interim. Does:

- **Every department have a plan for continuing operations if automated systems are suddenly unavailable?**
  - **It may (gasp) need to include use of paper forms**
  - It could also utilize pc based software such as Excel or QuickBooks but plans for acquiring the pc’s or software should exist if the departments pc’s are compromised
- Has a Tabletop exercise been performed to ensure that everyone has a plan and understands their role in both recovery and continuing operations?

Threats Question 1

Three of the five categories of IT General Controls are:

a) Security, administrative and access

b) Encryption, vendor and physical

c) Technical, administrative and vendor

d) Administrative, Encryption and Security

Threats Question 2

Which is **false** about passwords?

a) The longer a password is in existence, the more places its hash may be stored and the more likely could be subject to attack

b) Using the same password for multiple uses is safe as long as it is complex and long

c) The best passwords have complexity and length built in but are still easy to remember

d) A password that is strong today may not be strong in a year

Threats Question 3

To be most effective, penetration testing should:

a) Be tightly supervised by IT

b) Focus on a specific area in depth

c) Concentrate on the most common attack vectors

d) Be comprehensive in nature with the tester being given some latitude regarding areas to be tested.

Threats Question 4

A Tabletop Exercise is:

a) A great way to tone up your pectoral, arm and shoulder muscles.

b) An Emergency Management tool used to simulate and assess readiness for specific disaster scenarios.

c) Involves multiple departments and personnel to ensure roles and responsibilities have been clearly communicated and coordinated.

d) Both b) and c).

Threats- Question 5

SIEM is the acronym for:

a) Systems Integration and Exceptions Management

b) Sequel Information and Elevated Measurement

c) Security Information and Event Management

d) Software Insulting by Every Measure

Threats-Question 6

Which is not a common sources of OSINT :

a) An entity's website

b) Social Media for both the entity and its employees

c) Purchase Orders

d) Check Registers

Final Takeaways/Recurring Themes

- **A huge number of tasks take place behind the scenes for IT to function smoothly-**Don't ever say *"I don't know what they do all day"* unless you have taken the time to ask.
- **The interconnectedness of systems have created a complexity and automatic obsolescence of hardware and software that make IT very expensive but given reliance on IT, the cost of not investing adequately can ultimately be devastating.**
- **IT Literacy is a big issue. Top** management must understand at least enough about IT to ensure that it is adequately funded and staff are competent and following best practices
- Risks and Threats can never be completely eliminated but they can be reduced and impact minimized but **Good Security today does not mean Good Security tomorrow-**Threats are constantly evolving.
- **The pace of change is built into the nature and inter-connectedness of IT and is unlikely to slow in the near future.**

Appendices

A-COMMON CERTIFICATIONS

B-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)

ISACA CISA ((Information Systems Audit and Control Association Certified Information Systems Auditor) A certification focusing on auditing, monitoring and assessing IT and business systems.

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.

CCOA (Certified Cybersecurity Operations Analyst) offered by ISACA

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.

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.

Security Resources

APPENDIX B

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.

Leveraging Shared Services

Cybersecurity and Infrastructure Security Agency (CISA)

Part of the Department of Homeland Security, CISA offers a variety of services and resources to both private and Public sector. For Government:

- Multi-State Information Sharing and Analysis Center (MS-ISAC) Fee based service that includes 24x7x365 Security Operations Center (SOC) for threat intelligence, detection and response, free cybersecurity tools., and Risk Advisories and Notifications.
- Malicious Domain Blocking and Reporting (MDBR)
- National Cybersecurity Review (NCSR) Anonymized survey and checklist to help governments assess their cybersecurity maturity, This is required if you apply for Federal or pass-through cyber security grants.

CIS Center for Internet Security®

MS-ISAC® Multi-State Information Sharing & Analysis Center®

NCSR Overview

NATIONWIDE CYBERSECURITY REVIEW

The Nationwide Cybersecurity Review (NCSR) is a no-cost, anonymous, annual self-assessment that is designed to measure gaps and capabilities of U.S. State, Local, Tribal, and Territorial (SLTT) governments' cybersecurity programs. The NCSR is open annually from October 1 to February 28.

The NCSR is aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF provides a common language for understanding, managing, and expressing cybersecurity risk. It can be used to help identify and prioritize actions for reducing cybersecurity risk as well as align policy, business, and technological approaches for managing risk.

Register for the NCSR

To register for the NCSR, please visit www.cisecurity.org/ms-isac/services/ncsr/

Benefits

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress.
- Have the option of anonymously measuring your results against your peers.
- Attain reporting in order to prioritize the "next steps" towards cybersecurity improvement based on area(s) of deficiency.
- Obtain resources and services that can help you fulfill the desired steps towards cybersecurity improvement.
- Access automated mappings of your NCSR scores to the CIS Controls, NIST 800-53, HIPAA, and PCI Requirements.
- Utilize data summaries to justify resource and funding opportunities within your organization.
- Fulfill the NCSR assessment requirement for the Homeland Security Grant Program (HSGP) and the State and Local Cybersecurity Grant Program (SLCGP).

For administrative and technical questions about the NCSR, please contact the NCSR team at ncsr@cisecurity.org.

NCSR Maturity Scale

Responses to the NCSR correspond to scale below. The lowest score is a "1," which indicates a maturity level of "Not Performed." Meanwhile, "7" is the highest score at a maturity level of "Optimized."

7 Optimized	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6 Tested and Verified	Your organization is executing the activity or process and has formally documented policies, standards, and procedures. Implementation is tested and verified.
5 Implementation in Process	Your organization has an activity or process defined within documented policies, standards, and/or procedures. Your organization is in the process of implementing and aligning the documentation to a formal security framework and/or methodology.
4 Partially Documented Standards and/or Procedures	Your organization has a formal policy in place and has begun the process of developing documented standards and/or procedures to support the policy.
3 Documented Policy	Your organization has a formal policy in place that has been approved by senior management.
2 Informally Done	Activities and processes may be substantially performed, and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by senior management.
1 Not Performed	Activities, processes, and technologies are not in place to achieve the referenced objective.

www.cisecurity.org/ms-isac/services/ncsr/

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 Also includes a new Ransomware Readiness Assessment (RRA)

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.

State and Local Cybersecurity Grant Program (https://www.cisa.gov/cybergrants/slcgp)

MS-ISAC (Multi-State Information Sharing and Analysis Center) Sponsored by Center for Internet Security provides information sharing and cybersecurity posture for 17,000 governmental entities.

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