Leadership Guide

Guide to Technical Concepts for Non-technical Leaders

The technology industry is crammed with concepts, terms, brands, and acronyms.

This can be a big problem. Information Technology and Information Security require management. If you are a business leader tasked with overseeing IT and InfoSec [*notice how they were both just abbreviated, but in different ways?*], you *must* make effective decisions. And of course, the only way to make a good decision is to understand the tradeoffs and future ramifications of whatever is being proposed.

Complex concepts, distinctive terms, and byzantine abbreviations are hindrances to effective decision making.

Precise communication is necessary to make the right decision. Imagine learning that your organization is stuck because you approved a "cloud migration" project that you *thought* meant migrating to SaaS cloud, *not* hosting your virtual servers on cloud infrastructure (not sure what that means? Read on).

Or worse, learning that a recent security breach would have been prevented by a cybersecurity layer that was recommended to you *two years ago*. It never moved forward because no one understood exactly what having a "SIEM" really meant (unclear what a SIEM is? Read on).

This guide is a translator. If you are overseeing IT in any capacity, you will likely encounter the concepts, terms, and accompanying abbreviations that we have collected. These explanations are for nontechnical leaders, sacrificing detail for clarity.

If you treat this as a primer, you'll be well ahead of the game. Or treat it as a reference when you find uncertainty in decision making.

Without further ado, here is the Mainstay Technologies Guide to Technical Concepts, henceforth known as the **GTC**, which you can pronounce either as "G-T-C" or if speaking quickly, as "gitcuh," either of which are acceptable.

Index of Terms

Infrastructure

Infrastructure is the foundation of IT. It's the equipment (like servers), architecture (like cloud), and approaches (like disaster recovery) that make software, data, and services available to all your staff. It is a place of great complexity, but a few definitions light the way.

Active Directory (AD)

The abbreviation is pronounced as two separate letters "A-D." On your home computer, logging in is simple enough. Put in your password, push enter, and voila – there's all your stuff.

In a business environment, it's not so simple. Each user must have access to specific resources (but not others), have a unique username (but be standardized), have a secure password (but meet password policy), and access multiple devices (but not *any* if they are terminated!).

How does IT manage all this? Thankfully, Microsoft solved the problem decades ago with Active Directory (AD). Think of AD as a smart address book, setup just for your organization. All the computers and all the users connect to it, then it controls access. *Lucy is logging into computer X123?* Approved. *Gary wants to access the Finance folder?* Denied (sorry Gary). *Computer X056 wants to print to the coper?* Approved.

Active Directory is a core part of any Microsoft-based infrastructure. It can be run on a server (with a server running AD, called a *Domain Controller*), or in the cloud (as a service called *Azure AD*, connecting to devices over the Internet).

Active Directory = let me login!

Business Continuity Planning (BCP)

The abbreviation is pronounced as three separate letters, "B-C-P." A companion to Disaster Recovery Planning (DRP). Where Disaster Recovery Planning focuses on recovery from a crash, Business Continuity Planning focuses on *keeping systems running*. Things crashed and IT was able to recover? Yay. But how did everyone feel about the 2 days the systems were down? Not so great?

Downtime is wretched. The experienced fear it. Business Continuity is the art of keeping systems running, no matter what happens. A good BCP process documents the various systems and processes that rely on IT and how much downtime is "acceptable" (figuring out where the *business impact* starts). IT systems must then be designed to achieve that. Can't have the Internet down? Then IT must design to have a backup ISP (see term), or a fiber connection with an SLA (see term) that meets requirements. Can't have your core software down? Then IT must design using either the cloud (see term) or a very complex onsite architecture with virtualization (see term).

BCP = Keep our systems up!

Cloud

This is one of the most important technical concepts to grasp. It is an overarching term with many connected concepts. At its core, "the cloud" refers to a service from a 3rd party who hosts services for you (like an application, a server, or email) offsite, in a highly scalable, redundant, and secure way. You pay a monthly charge for what you use, rather than owning equipment and accompanying maintenance.

Think of a massive datacenter (a secure facility housing thousands of servers on multi-redundant Internet and power). All the servers are connected, and your data (or email, or software) doesn't just live on ONE of the servers, it lives on *all* of them. You don't own any of it – you simply

"rent" a fraction of the computing power in the datacenter, and you benefit from all the sophistication.

In the old days, your servers and data would live in a server room at your office. With the cloud, it doesn't just move offsite to a datacenter, it moves to a *different technical architecture*.

Of course, not all "clouds" are created equal. The quality of every facet matters, from the engineering team to the hardware. Big, sophisticated clouds (such as Microsoft's Azure platform, or Amazon's Amazon Web Services – AWS for short) have extreme sophistication with immense security and reliability (and allow you to even spread your data over multiple locations). We once worked with an organization who told us, "we are fully on the cloud." We determined their services were actually running on a server, in the basement of their IT guy. "Offsite" doesn't mean "Cloud."

To be a "Cloud" it must:

- Be offsite
- Maintained by someone else
- In a model where you pay for what you use
- On connected infrastructure, with many redundancies.

Public clouds are managed by providers who sell cloud services to their customers. Anyone can lease access. Microsoft Azure and Amazon Web Services are public clouds.

Private clouds are created by companies for themselves, to host their own infrastructure.

Note that the inverse of cloud is "on-premise" ("on-prem" for short), or "local," which refers to infrastructure located onsite, where the rest of the company is.

Cloud = data + software that is offsite, redundant, scalable, someone else manages.

Cloud Model: Software as a Service (SaaS)

The abbreviation is pronounced "sass." SaaS is a model for software. Rather than purchasing the software and installing it on your own equipment, you pay an ongoing fee to access the software over the Internet. The software company itself manages the cloud and provides it with their software.

For example, you can buy QuickBooks accounting software with a one-time cost. In that model, you install it on your own computers (and server), keep your data there, and manage the software yourself. Or, you can buy QuickBook's SaaS offering, called QuickBooks Online. You have no software to install, no data to backup, and nothing to maintain. You pay a monthly fee, and QuickBooks takes care of the rest. Wherever you are, from any computer, you can access the software, through a web browser. This is SaaS.

This is the most common way software is delivered today. It allows the software vendor to update the software, manage security, and ensure it is available. Of course, each SaaS provider has their own approach, and quality varies. Some are accessed through a web browser, some still require an application install but host your data in the cloud. Famous SaaS offerings include Microsoft Office 365 (email and office web apps), Google Workspace, Salesforce, and NetSuite.

When considering SaaS, it is important to investigate the robustness of the SaaS offering. It is also important to evaluate costs of the ongoing fee versus the cost to buy the software and maintain it. Finally, integrations are often a weak point for SaaS. It isn't always easy to integrate multiple SaaS applications together, or to connect them to the devices and data on your network.

SaaS = Software vendor provides the software *and* hosts your data in the cloud

Cloud Model: Infrastructure as a Service (IaaS)

The abbreviation is typically pronounced "eye-asz." In this model, you lease the *physical resources* for servers, but you still manages the server *software* (see term) and configuration directly.

For example, imagine you had a company server rack with 5 physical servers running Windows Server 2016, providing various services for your company. With IaaS, you can keep your same 5 Windows Server 2016 instances running, while eliminating your physical servers. The 5 servers get "migrated" up to the cloud. You simply pay per month for the resources you need. Eureka, the infrastructure works the same, but no more electricity usage, no more physical servers that could fail, no more being tied to one location. Cloud for the win!

In IaaS, your IT team still manages the updates, the software, the configuration of the servers, but NOT the hardware.

IaaS can be used for the full infrastructure or one component, such as with DRaaS.

IaaS = Replacing physical servers with the cloud.

Cloud model: Disaster Recovery as a Service (DRaaS)

The abbreviation is typically pronounced "dee-rass." One common, critical component for IaaS is *backups*. This uses the cloud for full Disaster Recovery. It first ensures *data* is securely offsite, protected from equipment failure, theft, fire, etc. It secondly provides an entire backup of your *servers,* ready to run in the cloud. Lose your local servers due to equipment failure or ice storm? DRaaS allows IT smoothly start those servers in a backup cloud location, keeping the business running.

DRaaS = cloud backups of both data and functionality

Disaster Recovery Planning (DRP)

Abbreviation is pronounced as three separate letters "D-R-P." Disasters happen. Be like a scout: Be prepared. Disaster Recovery Planning assumes disasters will come. It is a process to identify critical processes and systems and create multi-layered backups, beforehand.

Most of us know we need backups. The fear is familiar: "*It's 10pm. Do you know if your data is backed up?*"

Every organization (massive or micro) needs more than backups, however. It needs to be able to recover from more than just a data issue. It must protect against all *types* of disasters – data corruption, equipment failure, fire, flood, theft, accidental overwrite of data, security breach.

To be protected, every organization needs all data backed up multiple times, with stored revisions, stored offsite regularly, onsite for fast recovery (for onsite servers), with "snapshots" of full servers (so they don't have to be rebuilt in a crash), monitored daily, tested regularly, and thoroughly documented.

Planning for all of this is the essence of DRP. But it also includes availability of equipment and scenario planning for various downtime scenarios.

This planning process is documented in a "Disaster Recovery Plan." This Plan should give business leaders confidence in IT disaster preparedness, as well as giving them instructions in the case of a system crash. This is one of foundational documents for any IT Department, and if you don't have one, you should be concerned.

DRP = Necessary planning for worst-case scenarios

Servers

You know what a computer is. A "server" is simply a powerful computer that provides "back-end" functionality. It isn't used directly (no one sits at it with a keyboard and

mouse, unless they work in IT!), but rather it provide a service to many people.

One server might run Active Directory. Another hosts your website. A third stores all your Office files. And a fourth serves up your company's database. They are the servers, your computer is the "client."

Before virtualization (see term) and cloud (see term), "server" was easy to define. You have computers, which connect via the network, to big computers in the back room running all the back-office stuff.

In practice, IT professionals often use the word "server" to refer to both the virtual servers (see term) and physical servers (the hardware that runs them). And they often don't differentiate clearly if the server resides in the cloud or on-premise.

If you are in a conversation about servers, and the subject of the discussion isn't abundantly clear, ask for clarification – "are you referring to a virtual server, or a physical server?"

The most common server Operating System is from Microsoft. They have made multiple versions, each replacing the last: Server 2000, Server2003, Server 2008, Server 2012, 2016, 2019, and Server 2022.
Servers = the big backend computers running services for your organization

Unified Communications (UC)

Unified Communications refers to modern, software-based phone systems that run on VoIP (see term). They aren't called simply "phone systems" for one simple reason: the software provides far more than phone functionality. It also provides chat, away/busy information (called "presence"), video conferencing, and more.

An example is Microsoft Teams – an application part of Office 365. It is a Unified Communications tool that can

replace a traditional phone system while also allowing employees to share data, video chat, host video meetings, instant message, and more. It integrates with Outlook, installs on smartphones and computers alike, and provides for a seamless communication experience.

UC = software that combines phone, video, chat, and more

Virtualization (and "host," "Virtual Machines," and "hypervisor")

Before virtualization, a single Operating System software ran directly on a computer's hardware. Think of your own computer: Press the power button, the hardware turns on, and it loads an operating system (such as Microsoft Windows) that provides your experience. One physical computer, one computing experience. Simple, right? Virtualization turns the *physical computer* into a "host" of multiple computing experiences. Multiple instances of an operating system can run at the same time. With virtualization, you turn on the computer, and now *multiple* operating systems start at the same time and can be used by multiple people. You could work on one directly, while another is hosting files for Sally, and a 3rd is remotely being accessed by Tom. One *physical* resource is hosting multiple *virtual* resources.

Virtualization software introduces a layer *between* the hardware and operating system. When the hardware turns on, it first loads what is called a "hypervisor." This hypervisor turns the hardware into a "host" and runs multiple Virtual Machines (VMs) on the single set of hardware.

The advantages are numerous. Most computers use just a fraction of their resources at any one moment (you can see this for yourself. If you're on a Windows computer, hit CTRL+ALT+DEL and then select "Task Manager" and then the "Performance" tab. You're likely using just a few % of each resource). Through virtualization, that hardware can be used much more efficiently across multiple virtual machines.

Suddenly, a server rack of 12 servers can be replaced by 1 or 2 physical hosts, with all the accompanying cost benefits.

In addition, virtualization allows for *redundancy*. Multiple physical hosts can be connected so that if one fails, the other keeps the VMs running, keeping staff from experiencing any interruption.

The Cloud runs on virtualization. Organizations who maintain their own servers typically use virtualization software by Microsoft (Hyper-V) or VMware. Virtualization is rarely used for employees' direct computers, but it is nearly always used in the back-end infrastructure.

Virtualization = Multiple computers running on one physical computer

Computers

Computers are the marvelous inventions we take for granted each day. They are ubiquitous and need no introduction. In fact, in 1980 Bill Gates declared Microsoft's mission statement as "A computer on every desk and in every home." 33 years later they had to change it… it wasn't aspirational anymore! Cross that one off the list.

Central Processing Unit (CPU)

The processor, or "chip" inside a computer. Think of a small square with thousands of gold pins sticking out of it. The CPU is the logical brain of the computer. It performs the complex calculations necessary for all computing. CPU capability and processing speed is one of the primary factors that determines a computer's overall performance. Your computer's CPU was likely made by Intel, and it is a marvel of innovation!

CPU = your device's logical brain

Bring Your Own Device (BYOD)

Pronounced B-Y-O-D. Don't say "beeyod" or you'll get weird looks! A policy that allows people to connect to corporate resources with their own personal device, instead of having to use corporate issued equipment.

Examples include allowing employees to use personal phones to check company email, to use their personal iPads in the office, or to use their home computer for remote access.

BYOD provides employees freedom and productivity, while keeping central costs down.

However, BYOD represents a significant security risk. If your IT isn't managing the device, you can have no confidence in any protections are in place. The only sane security posture is to assume a hacker has already infiltrated the device. Because of this, IT must evolve security protections to support BYOD (such as Mobile Device Management – see term), and appropriate BYOD policies are ones that balance security with productivity.

BYOD = personal devices used for work

Easter Eggs

Developers are creative. And sometimes they hide things in their code. These hidden surprises are called easter eggs. They are typically found in video games, and the only reason they are in this guide is so I can have my own easter egg. Congratulations, you've found it (the easiest easter egg in history). The true purpose of this entry is to let you in on an industry secret. There are 3 terms known only to technical staff. Most IT people know them, and they may try to use them on you. They are:

1. "Eye-Dee-Ten-Tee." Let's say you're on the phone getting help with your computer. You ask, "What caused the problem?" The response comes back "oh,

this was a hard one. Yep, it was an Eye-Dee-Ten-Tee error." What do you think? Well, grab a pen and paper. Write a capital "I". Then a capital "D." Then the number "10." Then a capital "T," and the easter egg will be revealed.

2. "Short between the seat and the keyboard." This one is usually spoken fast, part of a run on sentence "yep, this issue was tricky we had to look at the applications and then we found the short-between-the-seat-and-the-keyboard." You can figure this out if you take long enough.
3. "Magic smoke." If something goes *very* awry, you'll see smoke come out of your device. It will stop working. Before the smoke, everything worked fine. After, nothing works. That is considered scientific proof that it was magic smoke. While it was still inside the computer, everything worked! Then, once it was released, it stopped. Magic smoke can't ever be reclaimed. Keep magic smoke in all your devices. Always.

Endpoints

An "endpoint" is simply a device that provides a computing experience. This may be a phone, a tablet, a laptop, a desktop computer, or a monitoring device. Instead of just referring to a "computer," this category refers to all devices that might be used and connected to the network, including IoT (see term) – devices. In an age of smartphones, tablets, and *smart* everything, "endpoint" is more precise than "computer."

Endpoint = the device at the end of the connection (typically in someone's hands)

Hard Drives

The storage component inside your computer. Without it, every time you powered off your device, poof, everything would disappear! Long live the hard drive.

In previous years, hard drives were made of spinning disks, and you could hear them whirring and chirping inside the computer like a magical chipmunk. Magnetic heads flew over rapidly spinning metal disks, adjusting the physical properties of the disk to store data.

Today, nearly all hard drives are "solid state disks" (SSD), which uses technology with no moving parts. An SSD is far faster than the old style of hard drives, and their cost has plummeted in recent years. You should avoid purchasing any computer that does not have an SSD.

Hard Drive = storage for your endpoint

Hardware and Software

These terms fit together like peanut butter & jelly. "Hardware" is a computer's physical componentry. The circuits, processors, memory, screen, etc. If you've ever taken the case of your computer (a great exercise, but if you're a Mainstay client reading this, please don't disassemble your work computer. Please), you'll see just how *complex* today's machines are.

But without software, hardware does nothing but whir! Software is *code.* Instructions that tell the hardware what to do. Everything you *do* on a device (from browse Amazon to play games to write emails) requires software.

Hardware and software = device and code. Together forever.

Memory / Random Access Memory (RAM)

RAM is pronounced like the word/animal/truck, 'Ram.' While you're using a device, various software applications are running. When something is "open" the code is moved from the hard drive to RAM. This memory is faster than the hard drive and it holds what's happening *right now.* The downside of RAM is that it is dependent on power. If you turn off the device, whatever was in memory/RAM goes poof!

Note that the word "memory" technically refers to RAM, *not* to the hard drive. Memory is "short term/volatile storage", while hard drives are intended for longer term storage of files and data.

RAM = computing memory that stores what's actively open

Operating System (O/S)

The most fundamental type of software is an Operating System. It's the first thing that runs when you turn on your computer. It interacts directly with the hardware and uses complex instruction sets to make everything happen. It is an incredibly advanced, vast piece of software, and it is used to run all other software.

Ever wonder why Microsoft can't prevent bugs and glitches? Well, this software is *so complex* and enormous that no one person has can understand it all.

Applications (various pieces of software) are installed on top of the Operating System. 74% of all computers run Microsoft Windows as their Operating System. The rest mostly run MacOS from Apple. Phones either run Apple iOS or Google Android for their Operating System (Microsoft ceded defeat in the smartphone wars in 2016 and BlackBerry lost much earlier).

O/S = the software that runs all software

Replacement Cycle

All good things come to an end. That's true not just for dessert, but for your computer too. That device you're using right now will someday be junk in a scrap heap. Before it completely gives up the silicon ghost, it'll start to have issues and individual components will fail. An old computer waits to stop working at the worst possible time.

All effective IT organizations seek to avoid this. IT uses a Replacement Cycle to determine how frequently computers will be replaced. The goal is to get the maximum life

(keeping costs down) while replacing them *right* before they start to have issues (keeping productivity up). Every organization should have a defined replacement cycle with a clearly identified inventory, so they can budget how many computers are replaced each year.

A typical computer Replacement Cycle is 5 years (for some organizations, it should be less, and in some cases it can be stretched), so 20% of the machines must be replaced annually (on average).

Replacement Cycles must also be determined for all IT equipment, including firewalls, switches, access points and the like. When setting a replacement date, IT and the business leaders must consider how impactful downtime is, how impactful higher performance hardware will be, when the manufacturer will no longer support the device, and what the budget needs are.

Replacement cycle = length of time before devices are proactively replaced

Networks

The network is the collection of hardware, protocols, and approaches to transmitting data between multiple devices. As technology embeds more deeply into every organization, every process, and every facet of business, the network's importance grows. Every device's connection must be fast, reliable, and secure.

Access Point

An access point is a physical piece of hardware that sends wireless signals into the air. It provides a wireless network connection (typically called "Wi-Fi"). It broadcasts a type of radio signal that allows devices to transmit data, as if they were physically connected to the network.

The more advanced the access point, the more advanced its security, the more powerful its antenna (how far its reach), and the faster its throughput. There are thousands of models of access points, manufactured by different companies. The right one for your organization must be sized for coverage and for capacity (the number of computers connecting through it).

You'll hear different WiFi protocols referred to by the names of their standards:

- 802.11g (supports 54 megabits per second of throughput)
- 802.11n (supports 450 megabits per second)
- 802.11ac (ranges up to 1700 megabits per second)

Note, if you are wondering why you have WiFi at home but don't have an access point, there is a simple reason: you have an "all-in-one" network device that combines a firewall, a switch, an access point, and perhaps even a modem, into one box.
Access Point = device that provides WiFi

Firewall

The Internet is a big place. We only have one Internet… Moscow Russia, Minneapolis MN, and Milford NH are all on the same Internet. One network, billions of devices.

In the old days, we'd simply connect a computer to the Internet. It was a happy place and time… Unfortunately, now, the Internet is inhabited by a criminal element called "hackers." They develop automated pieces of software that probe every device connected to the internet, looking for easy ways to gain access. The minute you connect, your device starts getting poked and examined by the automated programs of these nefarious ne'er-do-wells.

That's where the firewall comes in. It is a device that keeps traffic *out* of your network. It lets you connect to the internet

safely and invisibly. The Internet Service Provider's (see term) modem plugs into one side, and your internal network plugs into the other. The firewall controls all the traffic in and out. Most firewalls are focused on traffic *in* – your staff can get *out* to the Internet however they'd like, but the only people allowed *in* the other way must be appropriately authenticated. Advanced firewalls also inspect traffic *outbound* for malicious activity inside the network (a sign of a hacker, or someone unwittingly visiting a dangerous website, for instance).

Typically, "firewall" refers to a dedicated piece of hardware. However, a firewall can also be a piece of software.

Wonder why your smartphone doesn't need a firewall? It does. Your phone provider has one. A really, really, really big one. If your smartphone connects to Verizon, for instance, then your phone connects to the Internet from behind the Verizon firewall.

Firewall = the device that blocks unauthorized Internet traffic

Internet Protocol (IP)

The abbreviation is pronounced as two separate letters – "eye-pee." Be careful saying this abbreviation around a 4-year-old boy, as he will likely say "I pee too!"

IP is the basic way that data is transmitted across networks and the Internet. The "language" of networks. It's how data gets from one computer to another (such as from Amazon.com to your smartphone, when you need to order that tube of toothpaste at 11pm).

IP is the agreed-upon way each device sends and receives data. It is a part of the Transmission Control Program (TCP) so commonly referred to as TCP/IP. The annals of Internet history chronicle its development way back in 1973 by two DARPA scientists. It set off the fierce Protocol Wars of the 70s and 80s. TCP/IP fought a brutal battle and decimated the competition by the mid-90s (true story).

For our purposes, we simply need to know that it's a critical set of protocols that solve complex problems for how data gets from one place to another over a network. Every networked device has an "IP address" - a set of numbers that differentiate it from all others on the network.

Internet Protocol = the way network devices talk.

Internet Service Provider (ISP)

The abbreviation is pronounced as three separate letters "eye-ess-pee." An Internet Service Provider is a company that charges for access to the Internet.

ISPs provide access to the internet in various ways. In the old days, they'd give a phone number that would be dialed over a phone line. Now, most small business Internet is provided from a cable provider (such as Comcast).

Organizations who rely heavily on the internet may opt to pay extra for a connection over fiber – a network made of glass that allows for incredibly high speeds and the highest level of reliability.
The cost ISPs charge their customers is driven by the type of connection, the presence of competition (rural markets pay more), and the bandwidth provided – how much data can be transmitted each second.

ISPs run a complex network of heavy-duty infrastructure, connected to all other ISPs, allowing all their customers to access the Internet in a stable way. Customers that have fully moved to the cloud rely heavily on fast ISP speeds and highly available internal LAN (see below) availability.

ISP = Who you pay to get on the Internet

Local Area Network (LAN)

Abbreviation is pronounced "Lann," which rhymes with "pan." This is a collection of networked devices, behind your organization's firewall. Your organization controls the LAN. Only authorized staff are allowed on. Everything connected

to your switches (see term) is your LAN. Each physical location of your organization would have its own LAN. LANS typically are composed of: cable or fiber ISP connectivity to modems/routers, Firewalls, Switches, Wireless Access Points, Patch Panels, and network cabling. This is typically a single physical office location.

The counterpart to LAN is WAN (see term).

LAN = your own private network

Modem

The modem is the device between your internal network and your ISP. It's a converter – from one format to another. Often it converts media – such as from a cable connection to a network connection.

It's important to know what your modem looks like at home and at the office, because sometimes it needs to be rebooted (unplugged and plugged back in).

If you want to impress the tech in your life, mention that you know that "modem" is actually short for "modulator-demodulator."

Modem = device that connects your ISP to your firewall

Quality of Service (QoS)

Abbreviation is pronounced "kwoss." QoS prioritizes traffic on a network. Imagine you were on a VoIP (see term) call with a prospect, with the biggest deal of your life hanging in the balance. Suddenly the call starts breaking up, and you can't hear the other party! Vainly you struggle to understand – what is she saying? You glance at your coworker, and you see he has just started downloading a 5GB database update. That's it! You wave furiously at him to cancel the download, but by the time he understands, the call is over, and the sale didn't happen.

What happened? The network didn't have QoS. The switch and firewall blindly treated your phone call and the database download at the same level of priority.

With proper networking equipment, an engineer can configure QoS across all network devices (access points, switches, firewalls) to carefully prioritize the most important traffic, ensuring bottlenecks don't cause data traffic jams and result in lost deals.

QoS = prioritization of network traffic

Switch

An integral part of your network, the switch connects all your networked devices together. It is what allows each device to talk to the others and connect to the Internet. Ever seen a network jack in the wall (it looks like a phone jack, but with a wider plug)? A cable runs from that jack and eventually plugs into a switch.

The switch is a long, low box with multiple ports (typical sizes range from 4 ports to 48), covered in flashing green and yellow lights, bristling with brightly colored network cables.

You can think of a switch as a highway, with many onramps and offramps. The switch acts as highway and traffic cop – making sure all the devices communicate to each other in an orderly manner and resolving any conflicts swiftly.

The switch is still critical to a wireless network, as it connects your wireless Access Points to the rest of the network.

An "unmanaged switch" simply lets the traffic flow. A "managed switch" allows an engineer to prioritize different traffic (such as voice traffic over YouTube traffic), to segregate devices into their own lanes (VLANs - see term), and to monitor and control important aspects of security.

The switch must be powerful enough to handle all the traffic flowing through it. In a network of multiple switches, the switches must be connected in an optimal fashion, to avoid a

bottleneck, where all the devices on one switch must compress down to a slow rate to get to the devices on another switch.

And of course, switches must be reliable. A switch failure has a devastating impact to the business.

ften when a switch fails it doesn't just go "dead" and clearly need to be replaced – instead it starts playing red-light green-light with the data, causing slowdowns and network crashes, creating a knotty problem for IT to solve, while everyone complains of "random issues!"

Switch = The smart box that all network devices plug into

Virtual Local Area Network (VLAN)

Abbreviation is pronounced "Vee-Lann." Definitely NOT pronounced like "flan." You understand a LAN (see term). To design a network properly, devices often need to be segregated, within a LAN.

VLANs are used for many purposes – to keep a large network running smoothly, to separate physical phones, and to segregate less secure devices from corporate computers.

Ever hear about the casino that was hacked through their internet-connected fish tank monitor? True story. A VLAN would have prevented that.

It is called a "Virtual" LAN because devices across different segments can all be connected to the same switch. Engineers use code to tag and segregate the devices, rather than having to run separate physical cables and physical switches to each device.

VLAN = Segregated LAN

Virtual Private Network (VPN)

This is a method of remote access. Imagine you are at home, and you need to access your company data at the office. The problem? There is a firewall (see term) in the way! You can't

simply connect to the office network. Or can you? A VPN is the answer. It is a secure technology that connects you virtually to the corporate network, from wherever you are. Imagine you were dragging an invisible, secure cable from the network, through the Internet, and plugging it into your computer. That's a VPN.

Functionally, it works as a piece of software on your computer, configured to point at the corporate firewall. You connect, and then authenticate with your password and with Multi-Factor Authentication (see term) – if it's configured securely.

VPN = Secure remote access to corporate network

Voice over IP (VoIP)

Abbreviation is sometimes spelled out "v-o-i-p" and more commonly pronounced "voyp" which rhymes with… nothing I can think of. "Voy" rhymes with "Boy." Then add a "p" at the end. There we go. VoIP.

This is simple: Telephone calls over the internet. No more "phone lines." Your voice is simply transmitted as data over the network. Voice becomes data packets, sent with the Internet Protocol (IP -see term).

VoIP is typically far less expensive than traditional phone lines, and it is far more flexible. Fun fact: a phone line is now known as POTS – Plain Old Telephone Service. Who ever said IT terms weren't fun?

Nearly all phone systems now use VoIP. What we think of as a "phone system" is simply a piece of software (a phone app) that uses the Internet to transmit voices back and forth. The phone app can run on your computer, your smartphone, or a purpose-built physical phone (when someone asks for a physical phone, instead of using a headset with phone software on their computer, you can remind them that today's business phones are just small computers running a phone app…).

The downsides of VoIP? Well, besides the fact that calls are cheaper for scammers and telemarketers too… VoIP isn't always as reliable as regular phone service. The network must be configured correctly (using QoS – see term) to prioritize voice traffic, so that when your coworker downloads a movie, it doesn't hog all the bandwidth and interrupt your phone call.

VOIP = phone calls over the Internet.

Wide Area Network (WAN)

Abbreviation is pronounced "waan" – rhymes with "pan." The counterpart to LAN, this is a network connected *across locations*. The internet itself is a WAN (the mother of all WANs!). If you have two locations and then are connected, that becomes a WAN.

WAN = Network across locations

Software

This category is about the bits of code we use to make technology *do stuff*. Without them, technology just looks nice! With them, technology changes the world.

Application

A software package. An application is a set of code that runs on a device for a particular function. Microsoft Word is an application, so is Chrome, the Angry Birds app, Microsoft Outlook, etc.
Application = piece of software

Application Programming Interface (API)

Each application is coded uniquely and stores data in its own way. This presents a challenge when applications need to talk to each other. When Sales and Finance rely on two

separate applications, but their data needs to be integrated, how can that be done? Through APIs.

APIs are interfaces that can be configured to allow data to flow from one application to another, for the purpose of integration. Programmers working on integration don't have to learn the intricacies of both products; they simply use the API.

You and I use applications through a "User Interface" (see term). API is the back-end version of this. Programs talking directly.

Sometimes, applications come with APIs that have preconfigured integrations. Often, integration through APIs requires custom development. While APIs make things feasible, they don't always make them simple.

APIs = how different applications integrate

Business Intelligence (BI)

Ever tried to make a decision based on a spreadsheet? It is difficult. One stares at the spreadsheet wondering, is the data accurate? Is this actionable? What does it all mean? Business Intelligence seeks to solve this dilemma. It presents *actionable data* in a *compelling format*. It connects directly to a database and provides a graphical representation of the live data.

Business Intelligence tools provide visual tools for presenting the data. Individual views are called "gauges." Collections of gauges into a screen of them is called a "dashboard."

A complicated spreadsheet with rows of figures is replaced with a "sales dashboard." Gauge show sales totals, with a needle showing how close to target, and a color code to make it clear. Rather than a list of zip codes, it shows a map, with placed circles that match the revenue size of your clients.

BI works effectively when the data is accurate, KPIs (Key Performance Indicators) are understood, and a few simple gauges are designed that naturally drive action. These systems must be configured carefully.
BI is an *incredibly* powerful tool. Nearly every organization can benefit from a BI investment. The cost is the tool + developer time to create the gauges and dashboards + management time to hone and fine tune it. The payoff can be enormous, as an unprofitable product goes from being a little-known-fact to a red dot on a profit scatter plot.

Microsoft PowerBI is one of the most popular and inexpensive cloud-based Business Intelligence tools. Others include Tableau, Qlik, and Sisense.

Business Intelligence = graphical dashboards of data that inspire insight and compel action

Customer Relationship Management (CRM and XRM)

Sales and account management teams must manage many aspects of a relationship. They must track personal details of their prospects and clients, communication touch points, sales statuses, projections, renewals, and the like.

A CRM facilitates this. It stores records around a *customer*. Emails are stored, phone calls are logged, personal details inventoried, and sales activities tracked. Processes are created so the sales team follows a standardized approach. CRM Sales reports provide clarity to management on forecasts.

An "XRM" provides the same core software functionality, but for managing other types of relationships, such as vendors, donors, or partners.

SalesForce is the largest CRM/XRM software company in the world. Its software can be heavily customized to run nearly every aspect of an organization. Microsoft's CRM tool is

called Dynamics 365 Sales, and Hubspot offers a compelling alternative for small and mid-sized businesses.

CRM = software for managing relationships

Database

Applications have a front-end (the software interfaces you and I use to navigate) and a back-end (the data it accesses). If you're using Microsoft Word, Word is the front-end, and the back-end is each individual Word file. But if you're using a bigger business application (such as finance software, a CRM, or an ERP), there is way too much data to store in an individual file. Instead, the data is stored in a database.

To picture a database, think of an Excel worksheet, with rows and columns of data. Then imagine many different worksheets all connected and referencing each other in complex (yet organized) ways, and you have imagined a database.

Databases are designed to support immense amounts of data while still performing quickly. Unlike that trusty Excel worksheet, they are designed to support millions of records and thousands of data types and keep it all organized and running smoothly.

Database = structured, organized repository of data

Data Warehouse

What do you do when you have multiple databases, and you want to report across all of them? When you need a single view of sales, finance, and operations systems? You setup a data warehouse.

A data warehouse is designed for reporting only. It is setup as a separate database. Other databases are copied into it, with the data scheduled to update regularly. A developer matches data across the datasets (so Customer ABC in one dataset lines up with the data from Customer ABC in the

next) and exposes the data warehouse to the reporting (or BI) tool.

It can be tricky to initially configure a data warehouse, but it rarely requires much computing power, so it is typically inexpensive to maintain. It also allows report writers to mess about with the data without worrying about harming production data.

Data warehouse = repository for integrating data from multiple databases, for the purpose of reporting

Enterprise Resource Planning (ERP)

*Pronounced as three letters "E-R-P" and certainly **not** like "Earp" and has nothing to do with the Earp brothers of the O.K. Corral gunfight.*

Every department has specific software needs. Business leaders typically choose the best application they can for their department (a technique called "best of breed"). As a business grows, these applications proliferate. Over time, accounting runs one software package, shipping another, and sales a third. Manufacturing has three more applications all on its own and relies on 17 spreadsheets daily.

When the CEO asks for a report on all activity across a customer, everybody panics.

An ERP provides one central piece of software across multiple functions. It is a large, heavily customizable software package. In contrast to "best-of-breed," the power of an ERP comes from integration. All (or most) departments use the same application on the same database. When other applications are necessary, they are integrated with the ERP to ensure continuity of data.

ERPs are expensive and time-consuming to implement. Customization is expensive.

Some ERP packages work across many industries. Examples include: Microsoft Dynamics, NetSuite, and (for those with a

lot to spend) – Oracle or SAP. Others are built simply for one industry. At some point in a business evolution, the cost of building business processes and maintaining data across multiple applications becomes prohibitive, and an ERP becomes a necessity.

ERP = centralized software that runs multiple business units

Structured Query Language (SQL)

Abbreviation is pronounced like the word "sequel." SQL is the most common programming language for databases. It allows developers to structure databases in a common way. Those brave enough to look under the hood learn things like SQL *statements:* ways of controlling the data. And SQL *queries*: ways to write a question of the database and collect back all the related pieces of data.

Microsoft SQL is the most popular database management software for business, and you won't be able to discuss databases for long without hearing its name. The open-source alternative is mySQL, which, confusingly, is pronounced "my S-Q-L" (ess-que-ell)

SQL = The most common database language

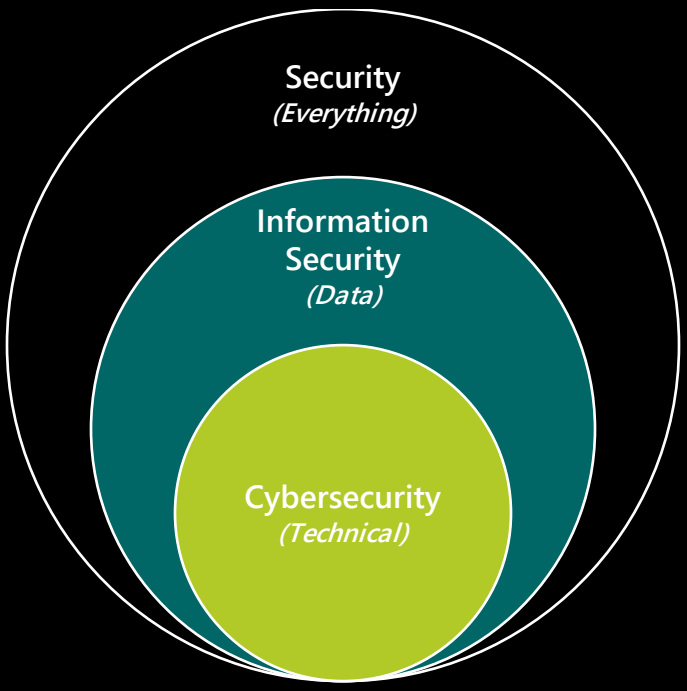
User Interface (UI)

The way an end-user (like you and me) navigates a piece of software. In the early days of programming, user interfaces were a set of punch-cards, lights, and a printer. Today, we typically use a type of UI called "Graphical User Interface" (GUI – pronounced "gooey"). This was the massive innovation that made computers accessible to nearly everyone in the 1980s. We look at graphical displays of the software, navigating using a keyboard and mouse.

UI = the way we see and navigate software

Security (and Information Security (and Cybersecurity))

If there's an especially confusing area of technology today, it's security. Adding to the confusion, few security companies communicate with precision. Terms are interchanged and concepts blurred.
Let's do our best to bring clarity by starting with the *category*. Are we talking about Security, Information Security, or Cybersecurity? Are they the same thing? No. The terms are **not** interchangeable. Think of it as concentric circles, getting smaller:



Security: Scope: Everything. Protecting the organization, assets (physical and digital), its people, and its data. This ranges from locks on doors to methods of keeping financials private to antivirus software.

Information Security (InfoSec): Scope: Data**.** Also known as Data Security**,** this is the practice of protecting all *data*, in all forms, at all times. InfoSec sets policy, manages risk, and drives to compliance.

InfoSec encompasses the IT systems but also the people, processes, and physical facilities that relate to data risk. InfoSec focuses on the whole organization, but it's all about compliance and data.

Cybersecurity: Scope: Technology. The practice of protecting the organization's *technology* with various technical layers and processes. This includes encryption, firewalls, web filtering, etc.

Now let the fun begin …

Antivirus

A cybersecurity control. Antivirus is the earliest form of security software! In the good old days, all you needed was antivirus software, a firewall, a password, and some Windows Updates. That protected against the threats of 2005 quite nicely. The role of trusty antivirus software is to run silently in the background, checking all new files and applications for malicious intent. It uses a combination of intelligent rules and "signature checks" where it checks against a database of known malicious "signatures." Today, antivirus is still important, but it is increasingly built into more advanced tools.

Antivirus = software that blocks nasty code, like viruses

Application whitelisting/Application blacklisting

A cybersecurity control. Application whitelisting is a technical method of *only allowing a pre-approved set of applications to run on a device.* It is an incredibly effective tool to keep a computer safe. It makes sense: create a list of only approved applications and just block the rest. Malicious software doesn't stand a chance.

The downside? Application whitelisting can require costly security software and can be a nuisance – both for IT and for all staff. ALL new applications must go through an approval process, including that handy utility you'd like to download,

or that software to make the new copier run, or the financial program you run once a year the night before taxes are due…

Application Blacklisting on the other hand is much easier to implement with some best practice controls and having the proper Microsoft Technologies and licensing in place.

Application whitelisting or blacklisting is required by some advanced compliances, such as CMMC Level 2.

Application Whitelisting = only run preapproved software

Application Blacklisting = blocking known malicious software and processes automatically as well as hardening overall cloud application security, control and posture.

Compliance

Compliance is the practice of *complying* with a set of regulatory or contract requirements that spell out methods of securing data. Common compliances include HIPAA, CMMC, NIST, state laws, GDPR, or client contract (large organizations increasingly require cybersecurity measures for their entire supply chain).

Compliance starts with a regulating body who wants to ensure a level of security – perhaps across the supply chain (such as with Cybersecurity Maturity Model Certification and the US Government's attempts to keep military secrets safe) or perhaps to product citizens (such as with state laws that try valiantly to keep your identity from being stolen). They create a set of requirements that spell out specific cybersecurity controls, policies, and process requirements.

While each compliance requires a different set of controls and has specific requirements, thankfully there is a lot of overlap, as they are all trying to do the same thing: Force good security practices.

Compliance = a set of security requirements that must be followed

Data Loss Prevention (DLP)

Abbreviation is pronounced as three separate letters – "dee-ell-pee." A cybersecurity control. DLP is a method of keeping sensitive data from leaving the company environment. This isn't about keeping hackers out, it's about keeping sensitive data *in*. To do their jobs, employees must have access to sensitive organization data. However, what if they misuse it?

Accidentally or maliciously share it with others? Imagine an executive decides to work for a competitor. Before he leaves, he quietly tries to email the company client list to his personal email address.

Detecting and blocking this is the purpose of DLP.

Simple DLP methods include configuring email systems to automatically scan and blocking emails that contain social security numbers, disabling USB drives, and blocking file sharing programs (such as Dropbox).

Advanced DLP solutions look for data that has been tagged as Confidential and blocks any type of transmission. This can be done at the firewall, through Microsoft 365, and with dedicated products.

Advanced DLP requires data that is appropriate classified and tagged and can have significant administrative overhead. But if American Superconductor had this, it might have saved hundreds of millions of dollars and 700 jobs…

Data Loss Prevention = limiting how sensitive data can leave the environment

Encryption

A cybersecurity control. Encryption is a method of converting data into a long, scrambled code. A decryption key is required to unscramble it and make the data readable. Encryption is necessary to protect data both at rest (where it lives) and in transit (when it moves).

Encryption = technical method of keeping data private

Endpoint Detection and Response (EDR) and Managed Detection and Response (MDR)

Today's threats are far more advanced than trusty old antivirus software can handle. Hackers are targeting your organization's devices in multiple ways. They are trying to compromise the integrity of whatever device you're reading this on, and they have an ever-growing bag of tricks.

Endpoint Detection and Response (EDR) software use advanced techniques to look at all behavior on a device, determining when it is from a malicious actor. The software can raise a red flag as well as taking automated steps, such as isolating the computer from the rest of the network. Microsoft Defender for Endpoint and Microsoft Defender for Business are an example of EDR software, and it uses Microsoft's AI in the cloud to pinpoint cybersecurity events with great accuracy. Microsoft receives over 24 trillion signals a day to learn from this threat intelligence.

Managed Detection and Response takes this technology and adds a team of "threat hunters." These are trained cybersecurity professionals who monitor and respond to alerts. The typically live in a Security Operations Center (see term).

EDR & MDR = advanced security software detecting hacker behavior. The "M" adds security staff who watch the software

Information Security Policies

Information Security Policies are documents that spell out Information Security controls, processes, and prohibitions. Policies are more than pieces of paper. They are the record of decisions for how data is handled. They contain the rules that all staff must follow. They provide the foundation of compliance and must be tailored to each organization. Hint: If you don't have robust, recently updated policies, you are not compliant with even the simplest of regulations.

Information Security Policies = the documents that formalize decisions about the Information Security Program

Information Security Program

An Information Security Program is a structured, ongoing way of managing risk. An Information Security Program draws together policies, technical controls, physical protections, training programs, testing methods, and business processes into one cohesive program. It is managed by an InfoSec professional and reports on ongoing to business leaders.

Imagine a quarterly meeting, including numerous business leaders, led by an InfoSec professional who understands your business. The InfoSec professional walks you through the latest phishing test (not good, 5% of staff failed it), the latest incidents (all good, hackers were repelled), the status of each item from the last risk assessment plan of action (decent, 75% done), a pending budget discussion (several options to consider), and walks you through an incident response tabletop exercise (scary, lot to learn from that one).

That is a working Information Security Program. It is required by nearly every compliance standard (CMMC, NIST CSF, NIST SP 800.171, ISO 27001, some state PII laws, etc.), and it is the way to integrate whole-organization security. It encompasses security for all aspects of data. Where cybersecurity is an IT function, Information Security works with all the stakeholders of the business, integrating with HR, management, leadership, IT, facilities, often facilitating reporting and training to the board.

Information Security Program = what facilitates whole organization security

Managed Information Security Program (MISP)

MISP is a Mainstay offering that delivers all aspects of an Information Security Program, led by a trained professional,

for a fraction of the cost of hiring. It is scaled and tailored to each client organization and integrates deeply into the client organization.

Mainstay Information Security Program = Information Security Programs made easy

Network Access Control (NAC)

A cybersecurity control. Network Access Control protects the physical network by screening the devices that are plugged in.

Imagine that one sunny Tuesday, you are working in the office when Tom shows up. He is the sales rep for one of your favorite vendors, and he is excited to demo their latest software product. It's the demo you have been waiting for! Excitedly you take him to the conference room. "I just need an Internet connection, where can I plug in?" asks Tom. You show him the jack on the wall, he connects, and the meeting is off.

Later that afternoon, you hear distressed sounds. Rushing over to investigate, you find that your Controller's computer shows the dreaded cryptolocker message: The computer is unusable unless you pay a ransom in bitcoin. What happened?

Tom was well meaning. But his company wasn't managing security well. His computer was compromised with malware (see term). When he connected to your network, he gained access *behind the firewall* (see term). His compromised computer was given access to same network where all your servers and sensitive data resided. Not good.

Network Access Control prevents this. It protects all network connections. Devices must authenticate (such as with Active Directory - see term) before gaining access to a sensitive area of the network. Otherwise, they are either blocked, or they are put into a separate, safe VLAN (see term) where they can access the Internet but can't do any harm internally.

NAC is either configured on the switch (see term) or provided by a separate piece of hardware.

NAC = only authorized devices can connect to the network

Malware

Malware is malicious software. It is written by malevolent miscreants intent on malfeasance and mayhem! Malware either runs silently in the background (it's like carbon monoxide for your computer…) or it masquerades as normal software (this can be called a Trojan Horse. Because of, you know, the Trojan Horse in Greek mythology). Malware is a broad term covering all nasty software. Viruses, worms, adware, spyware, and keyloggers are all specific *types* of malware.

Malware = code you don't want anywhere near you!

Mobile Device Management (MDM)

A cybersecurity and business control. MDM protects mobile devices such as smartphones, tablets, windows IoS and MacOS devices.

Who doesn't access sensitive data a smartphone anymore? We expect our data to be with us everywhere, on any device. That means security must be too. MDM software installs on the mobile device and enforces security. MDM often allows for "containerization" (a really fun word). This keeps company data in an encrypted container, separate from all other applications on the device, so that an issue with Angry Birds doesn't create an Angry Boss.

MDM = managing and security mobile devices

Phishing

Phishing emails are emails that look legit but are sent by a hacker, trying to trick the recipient. 91% of cyberattacks start with a phishing email, and there isn't an email user alive who

hasn't been a target. Millions of phishing emails are sent out each day.

Hackers rely on our sense of urgency and our desire to quickly deal with email, to attempt to trick us into clicking a malicious link that masquerades as a legitimate email. These used to be easy to spot – they were replete with grammatical errors and unlikely situations (your bank is not emailing you that your account has been emptied…). Today, they are sophisticated and often exactly match a legitimate email, such as an alert from a credit card. Proper cybersecurity increasingly requires solutions such as Microsoft Defender for Office 365 which provides extra layers of protection against phishing.

"Spear Phishing" is when *only you* are the target, and the email is custom crafted to get you to like it.

Phishing = emails that look legitimate but are not

Privacy

While security is about *protecting* your data, privacy is about *what you're allowed* to do with it. Privacy is typically governed by regulation. For example, HIPAA (Health Insurance Portability and Accountability Act) governs what the health industry can do with patients' medical data. Share it with another doctor for a consultation? Check. Share it with a 3rd party to cold call a patient with medication offers? NOT check.

Outside of the medical field, the most restrictive privacy law currently is GDPR in the European Union. It is an incredibly robust set of privacy restrictions. While it is aimed primarily at large tech companies such as Facebook, it ultimately applying to large and small companies alike who do business in Europe. It includes restrictions on how websites can track their users, which is why so many websites have an "Accept cookies" button now.

Privacy = what you can and can't do with data that isn't yours

Security Awareness Training (SAT)

Abbreviation is pronounced as three letters "ess-ay-tee." A common term for cybersecurity use training for all an organization's employees. Security is never solely the job of one department! It is ***everyone's*** *job***.** Security Awareness Training should be taken by everyone annually (this is required by most compliances) and should instruct on how to be a safe digital citizen. Topic should include how to recognize a phishing test, how to not give out your password even when someone says "pretty pretty please," how to recognize malicious websites, how to follow company policies, and the like.

Security Awareness Training = training for 100% of staff

Security Operations Center (SOC)

Abbreviation is pronounced "sock," but it rarely smells as bad. The SOC is a back-end team responsible for managing and monitoring cybersecurity controls. Comprised of trained cybersecurity professionals they use advanced tools to "watch" the environment and respond to anomalies. They often proactively maintain layers, monitor alerts, and hunt for threats.

SOC = the professionals watching for security events in the background

Security Incident and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR)

Abbreviation of SIEM is pronounced "sim," and SOAR is pronounced how you'd think… it rhymes with roar, bore, fore, and lore. There's a lot happening in your computers, network, and software, right now. Every second, each device records the changes that are occurring into log files. This

vast collection of detailed logs hold the footprints of everyone in your environment – hackers included.

Of course, it is the goal of every Information Security professional to *prevent* a hacker from gaining access to a single device or shred of data. But what if they get in? Once hackers infiltrate, they usually lurk for weeks or even months. They explore, understand what the organization does, and they try to grab all the sensitive data. Every action leaves a breadcrumb in a log.

However, the logs are arcane, lengthy files across hundreds of devices. It's nearly impossible for an individual to review logs and notice anything of interest.

The answer to this challenge is SIEM and SOAR.

A SIEM is a log aggregator. It takes the logs from multiple sources and combines them. It then uses logic rules to look for anomalies and issues. Like "hey, this person logged in from Manchester NH and St. Petersburg Russia within 5 minutes." It then pops an alert for a cybersecurity professional to investigate. It provides a single pane of glass for all events to be reviewed. It also stores the logs, which meets many compliance requirements. It is a defense on the inside of the environment. If a SIEM detects a hack, many other controls have failed.

A SOAR takes SIEM to the next level through automation. Because a SIEM records so much, it can still take cybersecurity staff hours to chase down alerts. That's expensive, and potentially not timely enough to stop a real hack. SOAR automates responses to increase speed and reduce time required, blocking and restricting access.

These solutions are increasingly affordable to small businesses. They are a necessary part of robust cybersecurity.

SIEM and SOAR = advanced ways of aggregating logs, recognizing patterns, detecting nefarious behavior, and blocking it

Web (or URL) Filtering

A cybersecurity control. Web filtering is a solution that monitors corporate web traffic, blocking access to websites, such as those that are known to contain viruses. Web filtering can be configured to be as granular and restrictive as the organization desires. It is typically configured to block categories of websites that have no reason to be visited in the workplace.
Some organizations use it as a productivity tool as well, blocking non-work sites such as online shopping. Most use it simply as an extra layer of cybersecurity protection.

Web filtering = control which sites can be visited from work devices

Trends

3D Printing

We all have a 2D printer! It spits ink on paper. Very handy. A 3D printer acts the same way: But instead of laying down one layer of ink, it lays down layer after layer of a material (typically plastic) to build a 3-Dimensional object.

A 3D printer naturally needs to be larger than whatever object it is creating. Hobbyist 3D printers are usually square boxes that can sit on a desk. Using CAD (Computer Aided Design) software, the user can design an object, then use the 3D printer to fashion it in real life. The printer precisely sprays the material in successive layers, until the object is complete. Hobbyists can print decorations, pencil holders, phone stands, and the like.

For business, it is powerful for prototypes, or for specific parts. Rather than keeping stock of rare parts, one could simply print the part when it is needed. The materials are typically resins, nylon, and plastics, which limit applications.

There are metal 3D printers which can "print" certain types of metal. Unfortunately, it is currently a costly and complex process. If (when?) this cost plummets, it will revolutionize traditional manufacturing.

Even today, with plastic, the opportunities are significant. 3D printers have successfully made functioning firearms (creating an enormous regulatory and safety challenge), environmentally friendly houses, and even (most of) a car. While still in its infancy, this technology could change the way most goods are created.

Whether or not you are in manufacturing, 3D printing is a trend to monitor.

3D Printing = printing *things* instead of words

5G

5G is the latest version of the wireless technology that connects a mobile device to the Internet. "5G" stands for "5th Generation" of the technology and it can deliver *extremely* fast speeds. The infrastructure to deliver 5G is still being built, and the highest speeds require the antenna to be within very close range of the devices (a few hundred meters), which means that the highest speeds are typically only experienced in densely populated areas.

5G may sound like simply "faster Internet for your phone." For most of us, that isn't noteworthy. What makes 5G remarkable is its promise of delivering extremely fast, extremely reliable Internet nearly everywhere. This creates new opportunities for the Internet of Things (see term) and for laptop users who travel frequently. 5G is unlikely to replace traditional home and office Internet, however, as

there are still reasons to have devices on one network, and to share a single Internet connection (such as cost savings).

5G = fast Internet for mobile devices and IoT

Artificial Intelligence (AI)

When hearing the term "AI," we often think of digital personality – a thinking, talking digital being. What today's technologists have (and are developing) is far from this. It is instead a very particular *kind* of AI. A kind that has certain applications. Because AI threatens to disrupt nearly every industry, every business leader must understand what AI is – and what it isn't.

The pursuit of AI began before WWII, started by brilliant mathematician Alan Turing. For decades, it advanced glacially. Computer scientists attempted to build AI by coding instructions to every possible scenario. If *X* happens, do *Y*. The code grew, but intelligence did not. Scientists were largely blocked.

In the 2000s, a new approach was explored. AI researchers began leveraging cloud computing power and designing neural networks – an approach that mimics the design of the connections of neurons in human brains. A neural network is a model that can learn. It is *trained* by being fed data. Training replaced coding instructions. Feed a neural network 1,000,000 pictures of cats, and it can recognize and tag the next 1,000,000 pictures all on its own.

The results have been staggering. Just since 2015, AI has transformed services we rely on every day – from Google Search to Translate to iPhone autocorrect. The accuracy and usefulness of these services has exploded. AI is already integrated into our digital lives. And trainable AI is now a "tool" that developers can leverage through the cloud, integrating easily into new applications.

If you have large sets of data, AI is *very* good at detecting patterns and making good predictions. This has had

immediate application to areas like translation or credit card fraud detection. It is also disrupting industries like radiology. Doctors must read a complex image, attempting to predict what masses are cancerous. AI is already more accurate than trained radiologists, under repeated tests (radiologists shouldn't fear: the best results come from AI and a Radiologist working together).

The significance of the recent AI breakthroughs and the resulting explosion of capabilities has created a sense of AI's limitless possibilities.

That promise should be tempered with the recognition that the current AI model is a *prediction machine*. It looks at data and makes accurate predictions, based on existing data it has analyzed. Wildly powerful. Yet this shows us what AI is *not*. It is not intuitive. It is not rational. It is not a *decision maker*. In areas of uncertainty, AI can provide predictions, but it is incapable of having *insights*.

Human intelligence is multi-faceted. It is intuitive, emotional, creative, multi-layered, and embodied. It is also *conscious* – a state of being that Cognitive Science still struggles to even explain, much less replicate. AI is *far* from those things. It is powerful, yes. But its applications are targeted.

Understanding this allows us to recognize why self-driving cars made such rapid progress, but also why that progress has stalled. With millions of miles of observing human driving, AI can now predict the best next move for the car with extremely high accuracy. However, that level of accuracy doesn't translate to intuition. For example, AI is having a hard time detecting highly unusual objects. A paper bag blowing across the highway is outside the scope of its prediction powers, so it is interpreted by AI as a small child – a mistake a human would never make.

Will researchers solve this for self-driving? Almost certainly. However, it will likely take years.

For the rest of us, consider your industry. Where will your industry use large amounts of data to increase accuracy of prediction? Answering that will answer how disruption happens.

It is AI and humans together that make the best partnership. We humans are limited in our ability to detect patterns in large sets of data. AI is limited in intuition.

As an example, lawyers are already becoming AI-empowered. The AI reviews the contract and makes recommendations based on a vast set of experience. The attorney then interprets and makes recommendations to the client. When will AI interpret the unique complexity of your organization's risk and advise a strategy directly? No time soon.

> *Reflection on the future: If you have used YouTube very often, you've likely noticed how good its recommendations are. The more you use the service, the more it feeds videos interesting to you. Soon, AI will be able to know enough about your musical taste to directly compose music - just for you. If you had the ability to listen to music that exactly suited your taste, that was composed for an audience of 1, by an unfeeling AI… would you? What do we gain, and what do we lose in that world? If this sounds far-fetched, Google*

AI = data-trained prediction machines

Blockchain

Blockchain is the underlying technology that makes cryptocurrency (such as bitcoin) possible. Cryptocurrency is just one of many applications for the blockchain technology.

Blockchain fans speak of blockchain like it is the harbinger of a new utopia. Supposedly it has the power to change industries, empower individuals, revolutionize contracts, and remake the financial industry.

What is it, exactly? Blockchain is a technology that creates a *permanent, secure, distributed record*. It allows data to be recorded in a way that *cannot* be changed and is inherently secure. This is why cryptocurrency is possible; Normally anything digital could simply be copied infinitely. But with blockchain, the record of a digital currency is unique. Unchangeable. Your bitcoin is truly yours – a digital record no one else can copy.

Technically, blockchain does this through a *distributed ledger*. Think of your financial ledger. You have one single ledger, and it gets updated. New changes overwrite old ones. You control it, and you store your ledger.

With blockchain, that ledger would be stored on numerous computers. Those computers won't allow changes to be made in the past – only new records added. They run under a complex set of rules for how updates are handled, and the distributed nature of it ensures its security and permanence. Innovations that use blockchain are not always intuitive. One example is a smart contract, built on blockchain technology. It acts as a 3rd party to 2 entities doing business. Both agree on conditions for the contract. Once they are met, the smart contract automatically completes the contract (such as issuing payment). It provides for a secure, safe, reliable, neutral 3rd party. This has immediate application in global finance, insurance, lending, and the like.

Blockchain could be used to secure our personal information, empower voting, facilitate sharing of sensitive data, and allow artists to create unique digital art (NFTs– Non-fungible tokens – are a blockchain technology allowing a customer to own a unique copy of a digital object).

Consider blockchain an architecture – an approach to storing data – that creates new technical possibilities. Bitcoin is simply one of them.

Blockchain = safe, unchangeable digital ledger

Exponential Growth

We often hear of technology growing "exponentially" without pausing to reflect on its meaning. Linear growth is in a straight line. 2 + 2 + 2 is 6. Exponential is cumulative. 2 x 2 x 2 is 8. A subtle difference at first becomes nearly a straight vertical line over time.

There is an ancient Persian tale of the inventor of the game of chess. When the ruler of the land was presented with the chessboard, he was so pleased he offered a gift of the inventor's choosing. The inventor asked for rice. He put a single grain of rice on the first square, and his request was simple: he asked that the rice double for each square. The emperor readily agreed, believing he had gotten off easily!

The result? For the final square alone, the king owed 18,446,744,073,709,551,616 grains of rice. The entire country's wealth was forfeit to keep the promise.

Those familiar with technology often refer to "Moore's Law" – so named for the Intel co-founder Gordon Moore who postulated it in 1965. He predicted that transistors on processors (used for processing power) would double every two years. Many predicted this would be a short-term law and could not continue for long. Yet nearly 50 years later, *it is continuing*.

Ever heard of the "Cray Supercomputer"? It was the fastest machine in the world in 1985. The Apple Watch is more powerful than *2 of them*.

Processing speed isn't the only area of technology advancing at an exponential pace.

We are accustomed to rapid change, so it can be difficult to comprehend how rapidly technology is reshaping our society. The smartphone in your pocket provides a better communication tool than the President of the United States had access to just 30 years ago, and it provides access to more data than he had access to just 15 years ago.

Technology impacts the shape of our lives – it influences the people we stay in contact with, the people we date (and marry), the type of information we consume, the way we consume it, and what we do with it.

What do the next 50 years hold? One can only imagine what exponential technological growth will do to the field of personalized medicine, to the clean water shortages of Africa, and to business innovation in America. Technology's exponential growth rate means we are now accomplishing in one year what previously took centuries. The degree of innovation that is occurring – even at this moment as you read this article – is staggering.

We are living amidst an explosion of technology.

Exponential growth = growth that doubles what came before, then doubles again and again…

Internet of Things (IoT)

Abbreviation pronounced as three letters, "eye-oh-tee."
Computers were the first to connect to the Internet. Then came smartphones. Now, nearly every device can connect.

Thermostat? Check. Car? Check. TV? Lights? Water bottle? Check, check, and check! (yes, the smart water bottle is real. It "empowers you to live healthier by monitoring your hydration").

As sensors become ever smaller and cheaper, they are becoming ubiquitous. *Everything* can have a sensor embedded and be connected to the Internet. And before long, everything will be. This is the IoT revolution. Monitor your office, your product, your dog.

In organizations, there are obvious applications for managing facilities, controlling machines, tracking vehicles, and optimizing logistics. But the explosion of IoT devices

doesn't stop there. Any object that needs manual monitoring or control is a candidate for IoT.

There are somewhere around 10 *billion* connected IoT devices globally. That is expected to more than double in this decade.

IoT = physical objects connected to the Internet

Robotics

The Roomba vacuum launched back in 2002. In the subsequent years, robotics has advanced rapidly. Search YouTube for "Boston Dynamics" for jaw-dropping examples today's capabilities. Distribution centers have been revolutionized by large, complicated robotic installations. Smart factories are increasing productivity rapidly. The military has a wide array of uses for robots.

But while advancing rapidly, physical robots still struggle to perform tasks we take for granted. It is exceptionally difficult to mimic the capabilities of a human body.

And there is a darker side: a programmatical glitch in a robot's coding can cause harm. The first human killed by a robot was an assembly line worker back in 1979. In South Africa, in 2007 a robotic gun glitched and began erratically firing, killing 9.

Innovation will continue, however. Find a task you'd like to delegate to a robot, and there is sure to be a researcher working on it somewhere! It is a technology of great promise.

However, physical robots aren't the only area of robotic innovation. Robotic Process Automation (RPA) is a rapidly accelerating set of technologies that uses software to automate routine tasks. For example, if your accounting department regularly must copy data from one system to another (and no backend integration is possible), RPA can

record the mouse and keyboard strokes and automate the whole process at rapid speed. Wherever there are repetitive, high-volume, low-value technical tasks, RPA should be considered.

Robotics = machines and software that assist humans with our tasks

Virtual Reality (VR) and Augmented Reality (AR)

Virtual Reality requires a full headset, blocking out natural light. Strap one on, and you are transported to another world: the sights of a created reality fill your vision. Augmented Reality takes a different approach: It leaves the wearer in the natural world but superimposes digital objects. A wearer of AR glasses could still navigate a room, while seeing the room peopled with video game characters.

VR was first developed in 1968. As computers have become more powerful, displays more precise, and motion tracking technology more available, headsets have become better in quality, as well as radically less expensive. Software companies have begun developing immersive VR worlds.

It is a trend powerful enough that Facebook has spent billions on VR, even changing its company name to Meta, reflecting the meta (virtual) universe it is seeking to create and bring its billions of users into.
VR and AR adherents speak of a future world where we navigate a seamlessly a hybrid digital/physical world. Don't like the view out of your apartment? Change it to an ocean landscape. Bored on the train? Play a game with characters who jump over seats. Ready to video conference? Put yourself in a room with the other attendees and see them in 3D. Tired of life? Escape to a reality that immerses all your senses in whatever way you choose. VR represents a chance to remake the world we experience (and it isn't just sight and sound – VR innovations also focus on touch and even smell).

Sociologists speak of a concern that if the technology *does* work that well, that millions will abandon real life for the virtual reality of their choosing, abandoning the pursuit of meaning in their lives.

So where is the technology today?

The gaming industry is propelling significant advances, as games are becoming increasingly sophisticated. The military is reportedly investing heavily in VR training.

VR and AR simulations are already helpful in interior design, industrial training, retail store planning, product design, sports coaching, and even in certain kinds of therapy. The annual market for VR is already a multi-billion-dollar industry and growing rapidly.

How AR and VR will remake the business world is yet to be seen. Every business leader should consider the implications of this technology for their industry. With tech companies investing billions in R&D each year, there is massive change on the virtual horizon.

VR and AR = the promise of utopia or dystopia (you decide)

Work-From-Anywhere (WFA)

Also known as "Remote work" or "Work-From-Home" (WFH), the most precise term is "Work-From-Anywhere," (WFA). Because, once an employee has the freedom to work out of the office, that freedom will be used. Work is done from coffee shops and conferences, from hotel rooms and home offices, from living rooms and limousines.

Before the pandemic of the early 2020s, WFA was considered a luxury. During the pandemic, employee expectations changed. Millions became accustomed to the work rhythms and freedoms of working in any location. After the pandemic, companies who did not allow WFA experienced higher attrition and higher recruiting challenges compared to those who continued WFA.

This trend is expected to continue. *Most* companies will need to support staff who work remotely much (or all) of the time. There are clear life/work balance advantages to the employee and obvious efficiency gains to the company (cutting out a commute and eliminating chit-chat in the hallways are just two examples).

WFA is not without its downside. Security challenges increase. Remote relationships are not as deep and multi-faceted as relationships in person. Mentoring remotely is difficult. Those working in isolated situations can experience significant loneliness.

Each organization must wrestle with the impact of WFA. There is no one-size-fits-all recipe. Organizations are finding success with varied approaches. But it is critical to have an intentional, thoughtful approach. WFA isn't going away.

Work-From-Anywhere = just what it says.