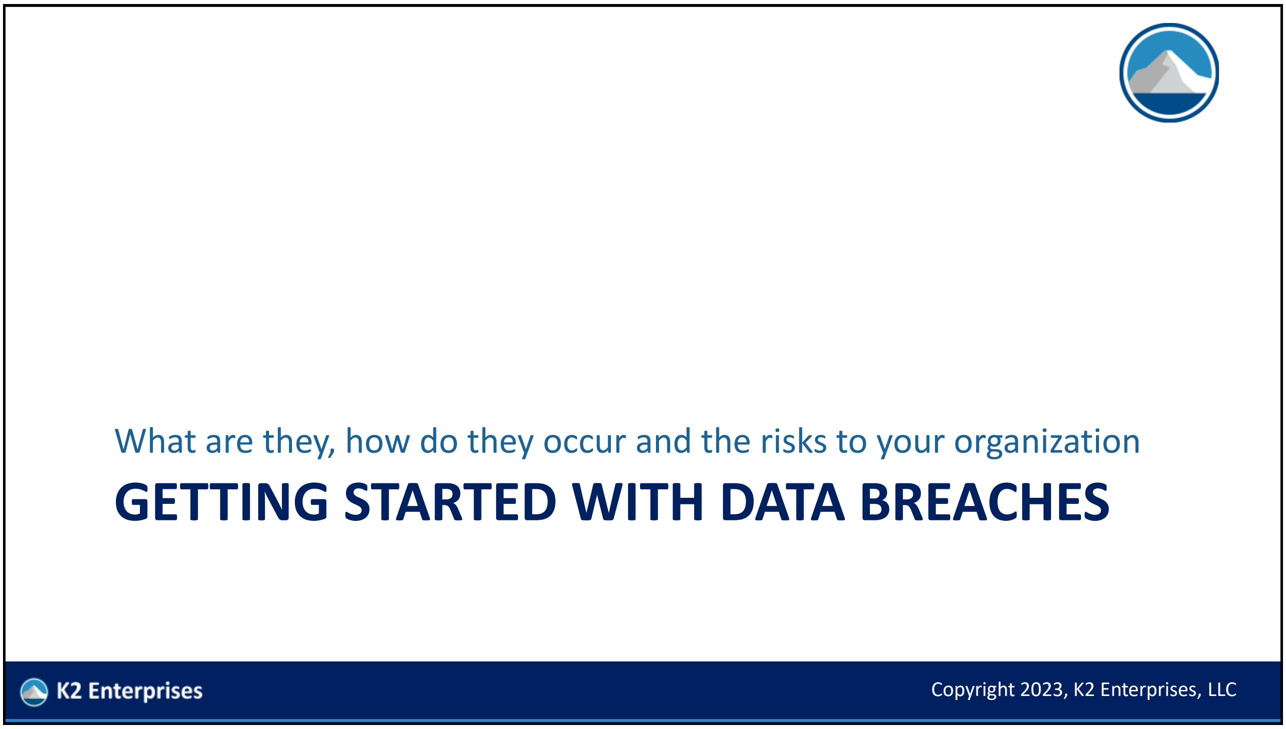
K2's Securing Your Data

Practical Tools For Protecting Information

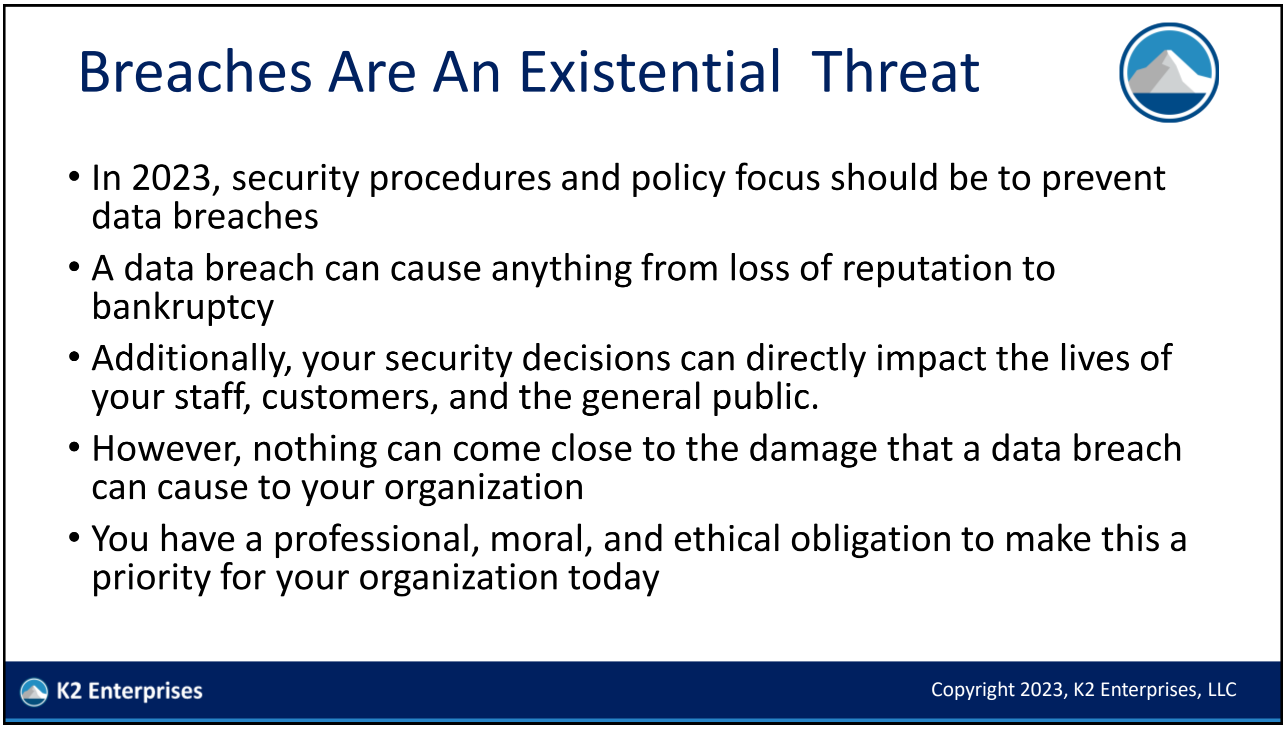
K2 Enterprises



What are they, how do they occur and the risks to your organization

GETTING STARTED WITH DATA BREACHES

K2 Enterprises



Breaches Are An Existential Threat

- In 2023, security procedures and policy focus should be to prevent data breaches
- A data breach can cause anything from loss of reputation to bankruptcy
- Additionally, your security decisions can directly impact the lives of your staff, customers, and the general public.
- However, nothing can come close to the damage that a data breach can cause to your organization
- You have a professional, moral, and ethical obligation to make this a priority for your organization today

K2 Enterprises

Data Breach Defined

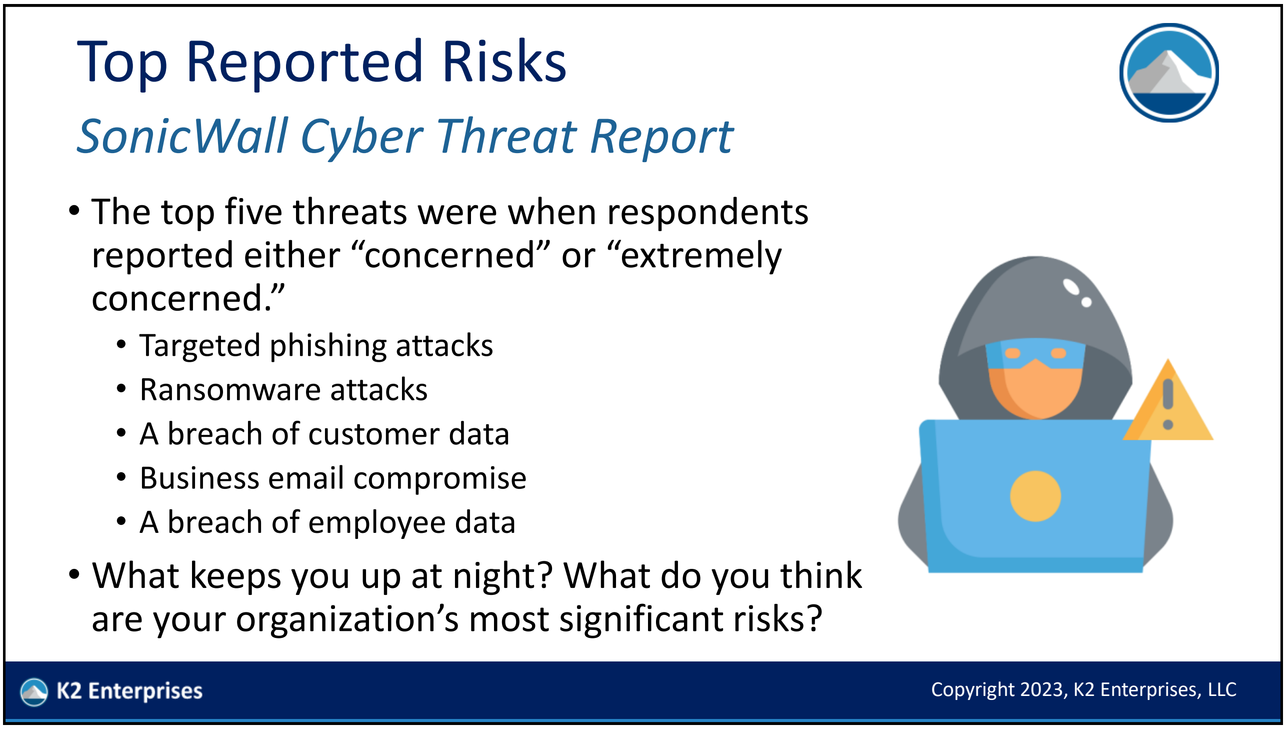
- A data breach occurs when an unauthorized 3rd party penetrates an individual or organization’s information systems and steals their data
- A perpetrator can compromise a system through various technics, from stealing a password to infecting a target with malware. There seems to be an endless number of attack types
- Data breaches are particularly hazardous to organizations with sensitive company, customer, etc., data
- Today, virtually all organizations and individuals are at risk

Major Cybersecurity Trends

Below are the major attack trends for the coming year.

- 5.4 billion malware attacks (-4%)
- 60.1 million IoT malware attached (+6%)
- 5.3 trillion intrusion attempts (+11%)
- 97.1 million cryptojacking attacks (+19%)
- 623.3 million ransomware attacks (+105%)
- 10.4 encrypted threats (+167%)

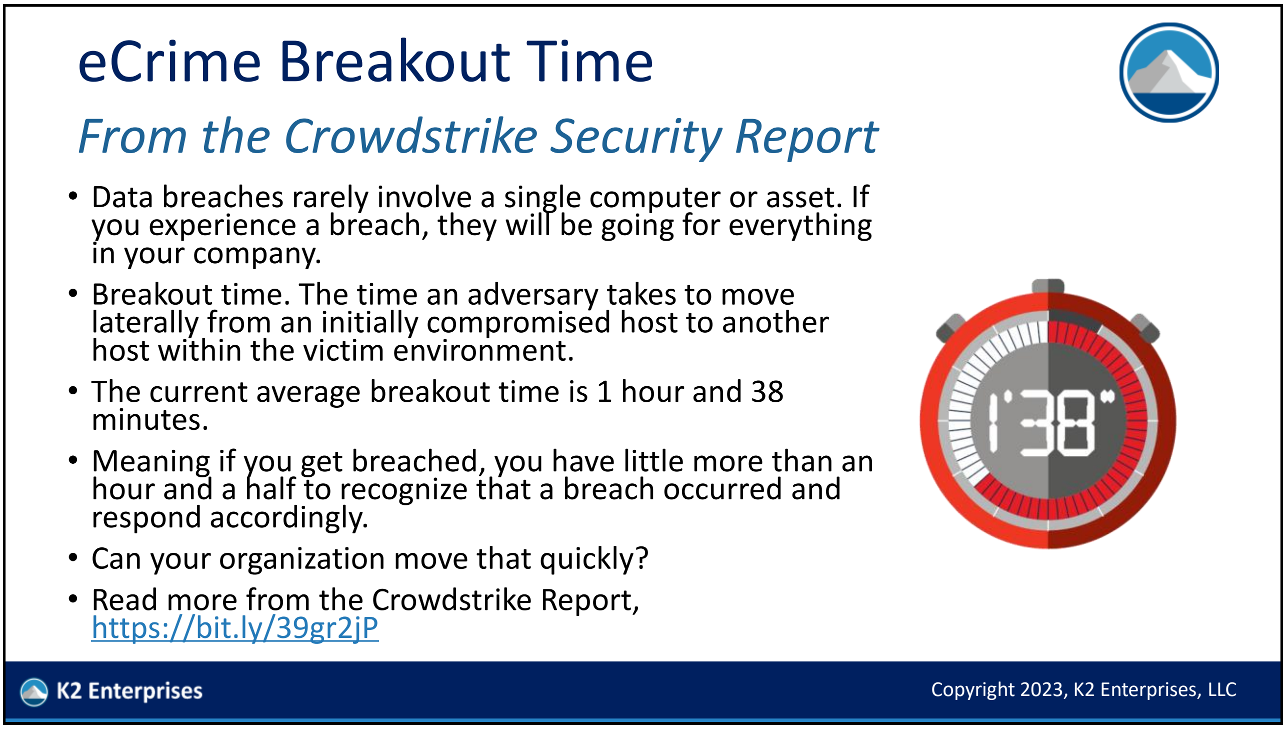
- Read more from SonicWall’s 2022 Cyber Threat Report, https://bit.ly/3FCRAbb



Top Reported Risks

SonicWall Cyber Threat Report

- The top five threats were when respondents reported either “concerned” or “extremely concerned.”
  - Targeted phishing attacks
  - Ransomware attacks
  - A breach of customer data
  - Business email compromise
  - A breach of employee data
- What keeps you up at night? What do you think are your organization’s most significant risks?



eCrime Breakout Time

From the Crowdstrike Security Report

- Data breaches rarely involve a single computer or asset. If you experience a breach, they will be going for everything in your company.
- Breakout time. The time an adversary takes to move laterally from an initially compromised host to another host within the victim environment.
- The current average breakout time is 1 hour and 38 minutes.
- Meaning if you get breached, you have little more than an hour and a half to recognize that a breach occurred and respond accordingly.
- Can your organization move that quickly?
- Read more from the Crowdstrike Report, https://bit.ly/39gr2jP

No opportunity to protect yourself

ZERO DAY EXPLOITS

What Is A Zero Day Attack?

- A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong.
- In fact, a zero-day exploit leaves NO opportunity for detection.
- A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence “zero-day.”
- Learn more at https://bit.ly/3l1Dd6P

How Does A Zero Day Attack Occur?

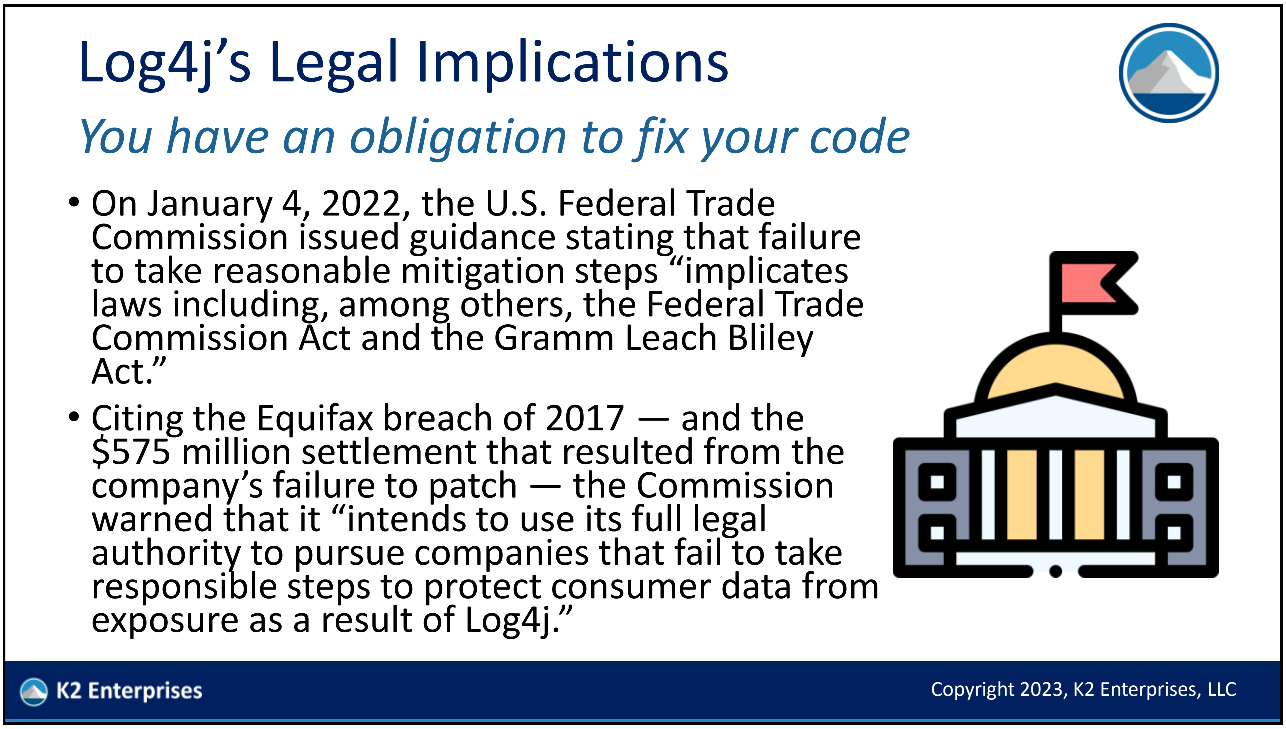
We all find out about it at the same time.

- A company's developers create software, but it contains a vulnerability unbeknownst.
- The threat actor spots that vulnerability either before the developer does or acts on it before the developer has a chance to fix it.
- The attacker writes and implements exploit code while the vulnerability is still open and available
- After releasing the exploit, either the public recognizes it as identity or information theft, or the developer catches it and creates a patch to staunch the cyber-bleeding.
- Learn more about Zero-Day Attacks, https://bit.ly/38rbQAz

The Log4j Vulnerability

The utility you've never heard of but use every day

- The Apache Log4j was the last major zero-day vulnerability reported in 2021 but quickly became one of the most significant of the year.
- The Log4j affects how computers and servers handle log messages. An attacker can hijack the messages and inject malicious code.
- You wouldn't use Log4j directly yourself, but it is built into countless applications and services you use every day.
- From 12/11/20 to 1/31/22, SonicWall recorded approximately 150 million exploit attempts against Log4j vulnerabilities, about 2.7 million each day.
- The primary industries affected are the scientific and technical community (28%), manufacturing (13%), government (9%), finance (5%), retail (5%), and K-12 (5%).
- Read more in the 2022 SonicWall Cyber Threat Report https://bit.ly/3FCRAbb

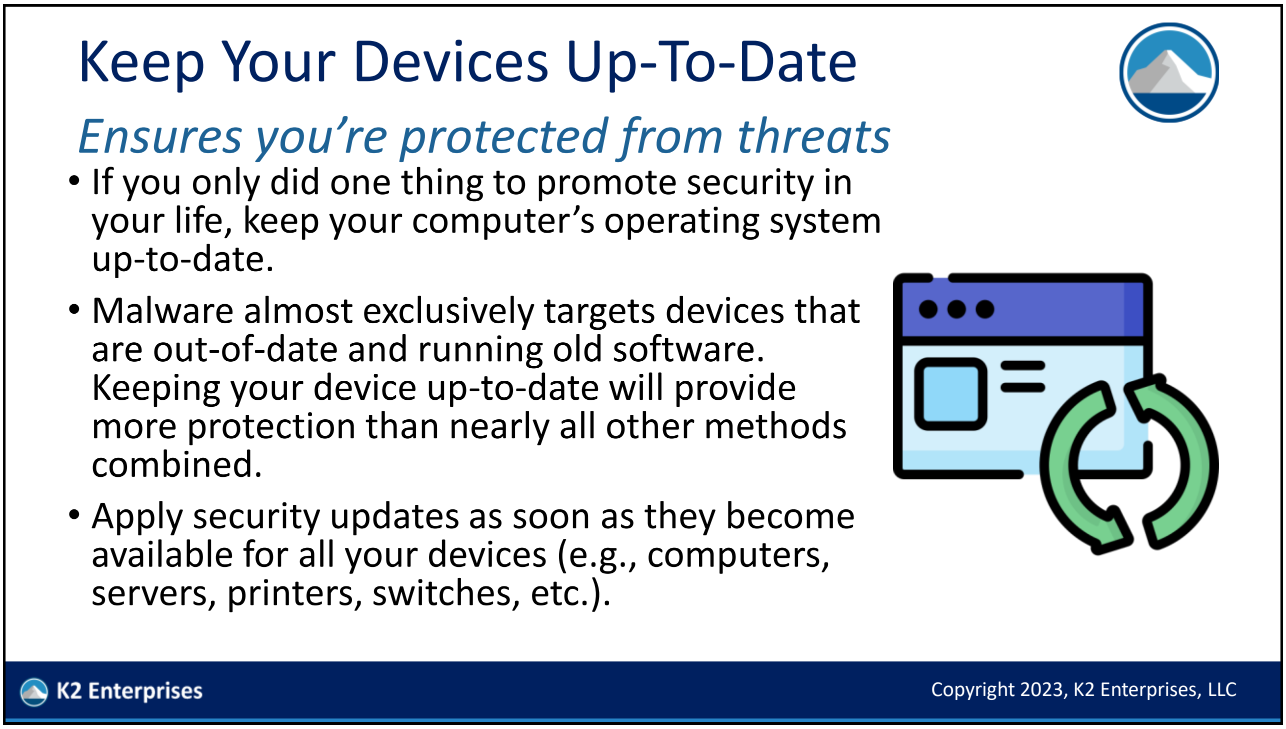


Log4j's Legal Implications

You have an obligation to fix your code

- On January 4, 2022, the U.S. Federal Trade Commission issued guidance stating that failure to take reasonable mitigation steps "implicates laws including, among others, the Federal Trade Commission Act and the Gramm Leach Bliley Act."
- Citing the Equifax breach of 2017 — and the $575 million settlement that resulted from the company's failure to patch — the Commission warned that it "intends to use its full legal authority to pursue companies that fail to take responsible steps to protect consumer data from exposure as a result of Log4j."

K2 Enterprises



Keep Your Devices Up-To-Date

Ensures you're protected from threats

- If you only did one thing to promote security in your life, keep your computer's operating system up-to-date.
- Malware almost exclusively targets devices that are out-of-date and running old software. Keeping your device up-to-date will provide more protection than nearly all other methods combined.
- Apply security updates as soon as they become available for all your devices (e.g., computers, servers, printers, switches, etc.).

K2 Enterprises

Attacking the vendors and suppliers that you work with

SUPPLY CHAIN ATTACK

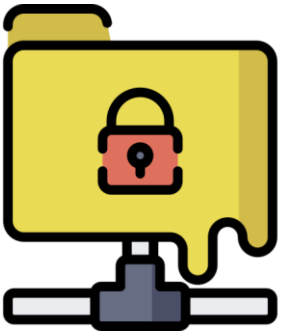
What Is A Supply Chain Attack?

- A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply chain.
- For example, an attacker could compromise the company that develops your custom inventory solution or the software that runs your manufacturing system. You become affected because they were infected.
- Cybercriminals typically tamper with the manufacturing or distribution of a product by installing malware or hardware-based spying components.
- You could not even know you're exposing yourself to risk.
- A supply chain attack can occur in any industry, from the financial sector and oil industry to the government sector.
- A supply chain attack can happen in software or hardware.
- Learn more at https://bit.ly/3MsFQeb

Solar Winds Data Breach

The company and its products

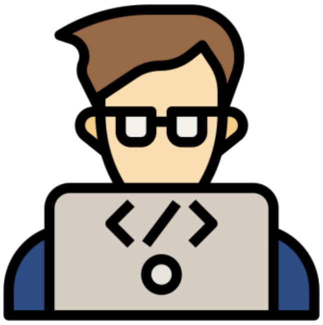
- Solar Winds makes software that helps organizations better manage their physical hardware, software applications, databases, etc.
- Solar Wind’s Orion application monitors and manages all types of IT infrastructure in one place.
- Orion is primarily used in large organizations with significant infrastructures and increased complexity in their operations.
- In early 2020, foreign hackers breached Solar Winds software development infrastructure and injected malware into their secure development environment.
- As with all applications, Orion has a built-in update functionality that ensures clients get the latest features, functionality, and security improvements.

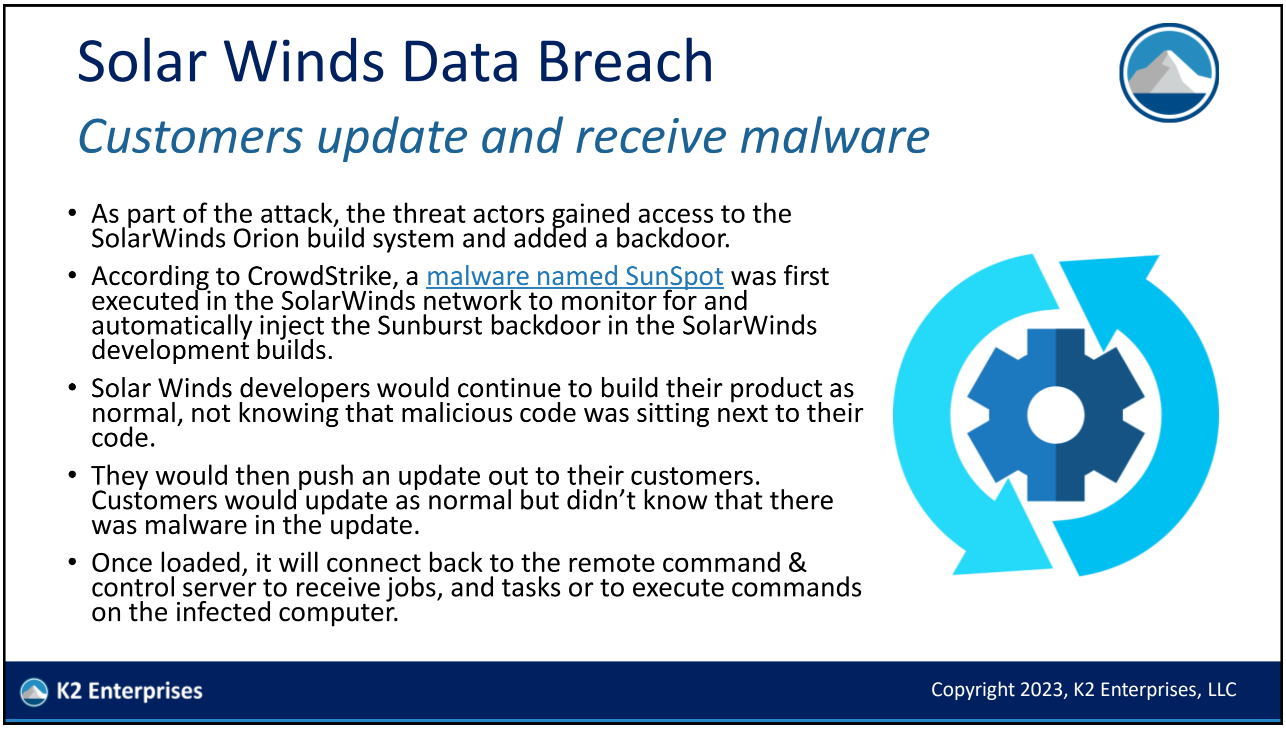


Solar Winds Data Breach

Development process was compromised

- In December 2020, SolarWinds had been hacked by state-sponsored threat actors believed to be part of the Russian S.V.R.
- The threat actor specifically compromised the software development process of Solar Winds. Their primary focus was to insert malware into updates delivered to customers.
- That malware was unknowingly distributed by Solar Wind’s secure update process to thousands of clients worldwide.
- Customers updated their application like normal, but unbeknownst to them they were infecting their systems with malware. To them, it looked like any other software update.
- This malware allowed the hackers to breach further Solar Wind’s clients (18k+), including most of the Fortune 500 and most of the US Federal Government.
- Learn more at https://bit.ly/39dNR7M

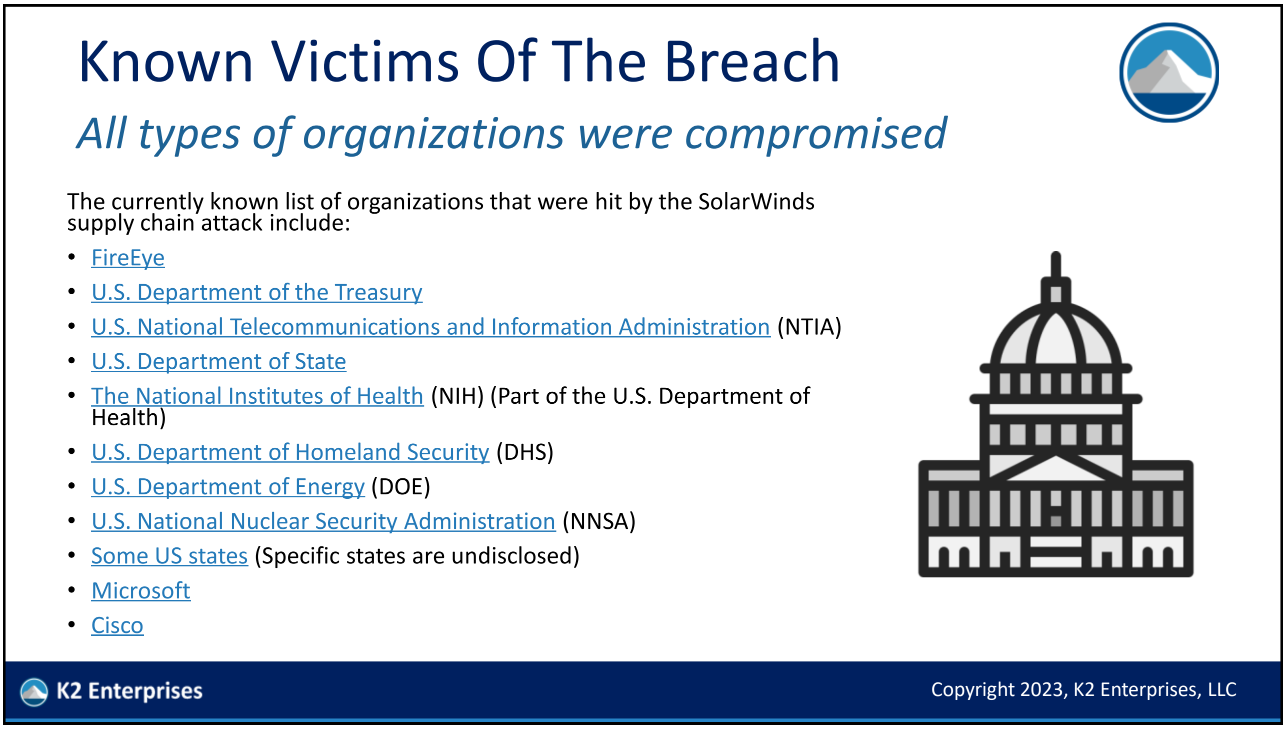




Solar Winds Data Breach

Customers update and receive malware

- As part of the attack, the threat actors gained access to the SolarWinds Orion build system and added a backdoor.
- According to CrowdStrike, a malware named SunSpot was first executed in the SolarWinds network to monitor for and automatically inject the Sunburst backdoor in the SolarWinds development builds.
- Solar Winds developers would continue to build their product as normal, not knowing that malicious code was sitting next to their code.
- They would then push an update out to their customers. Customers would update as normal but didn't know that there was malware in the update.
- Once loaded, it will connect back to the remote command & control server to receive jobs, and tasks or to execute commands on the infected computer.



Known Victims Of The Breach

All types of organizations were compromised

The currently known list of organizations that were hit by the SolarWinds supply chain attack include:

- FireEye
- U.S. Department of the Treasury
- U.S. National Telecommunications and Information Administration (NTIA)
- U.S. Department of State
- The National Institutes of Health (NIH) (Part of the U.S. Department of Health)
- U.S. Department of Homeland Security (DHS)
- U.S. Department of Energy (DOE)
- U.S. National Nuclear Security Administration (NNSA)
- Some US states (Specific states are undisclosed)
- Microsoft
- Cisco

FireEye's Recommendations To Protect From Supply Chain Attacks

- **A small supplier base:** This allows a firm to have tighter control over its suppliers.
- **Stringent vendor controls:** Imposing stringent controls on suppliers to abide by lists of approved protocols. Also, conducting occasional site audits.
- **Security built into design:** Security features, such as check digits (hashes) should be designed into the software to detect any previous unauthorized access to the code.
- Learn more at https://bit.ly/3wchobm

Impersonators in Your Inbox

BUSINESS EMAIL COMPROMISE (BCE)

Social Engineering

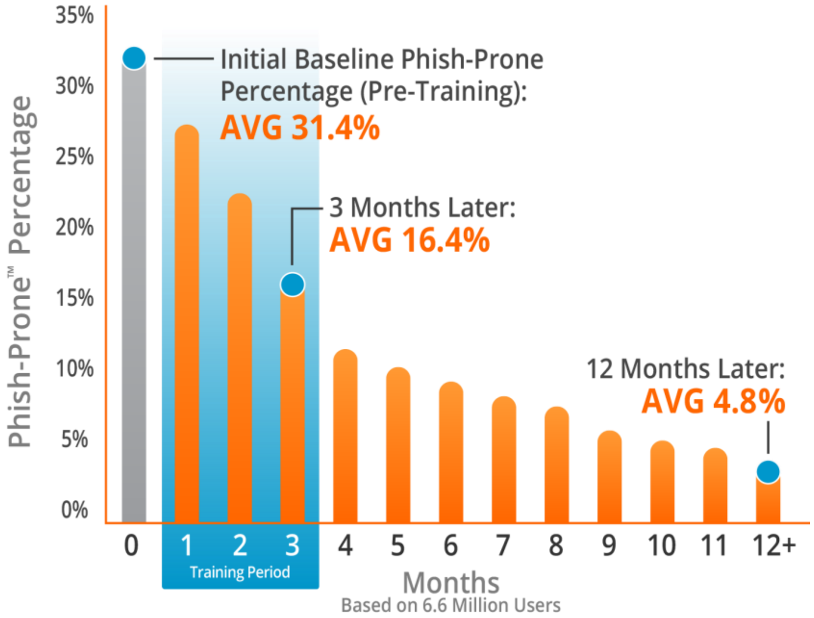
Your biggest threat! Don't fall victim!

- Social engineering manipulates a person into performing actions or divulging confidential information. **It is essentially an excellent ol' fashioned con job.**
- The job is to manipulate a user to give you their password, get them to download malware, or something equally awful. The goal is to extract something valuable from them.
- This method has been used in everything from the Greek Trojan Horse of the age of antiquity to the annoying fake calls from the IRS claiming back taxes are owed.
- Be wary of giving out information over the phone or electronically. Be cautious about people that contact you out of the blue. Consider implementing identification policies to identify authorized people.

KnowBe4

Security Awareness Training

- **Train Your Users.** The world's most extensive library of security awareness training content. Automated training campaigns with scheduled reminder emails.
- **Phish Your Users.** Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.
- **See The Results.** Enterprise-strength reporting, showing stats and graphs for training and phishing, is ready for management. Show the great ROI!
- Learn more at https://www.knowbe4.com/



KnowBe4 Phishing Training Results

Software intentionally designed to cause disruption and damage

MALWARE

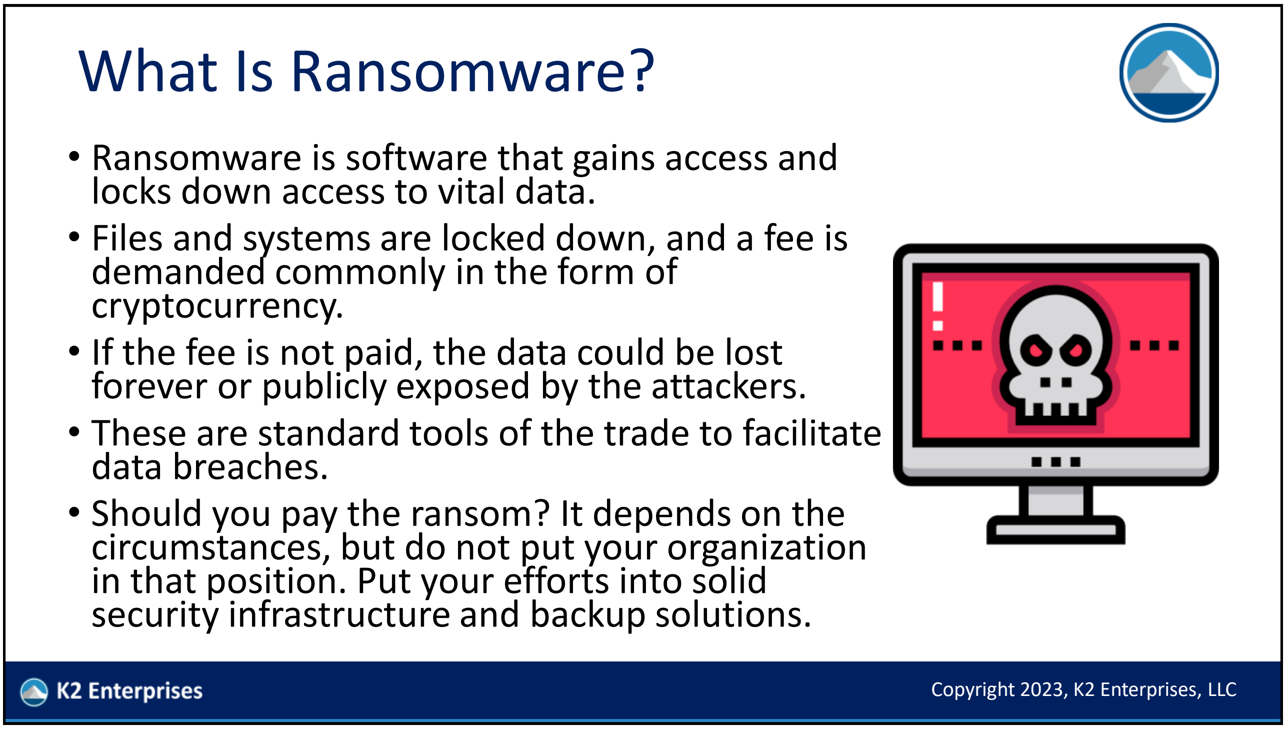
What Is Malware?

- Malware, short for “malicious software,” refers to any intrusive software developed by cybercriminals (often called “hackers”) to steal data and damage or destroy computers and computer systems.
- Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Recent malware attacks have exfiltrated data in mass amounts.
- Malware is a catch-all term describing all software intended to damage or disable a computer or information system.
- Learn more from Cisco at https://bit.ly/3swBMl0

K2 Enterprises

RANSOMWARE

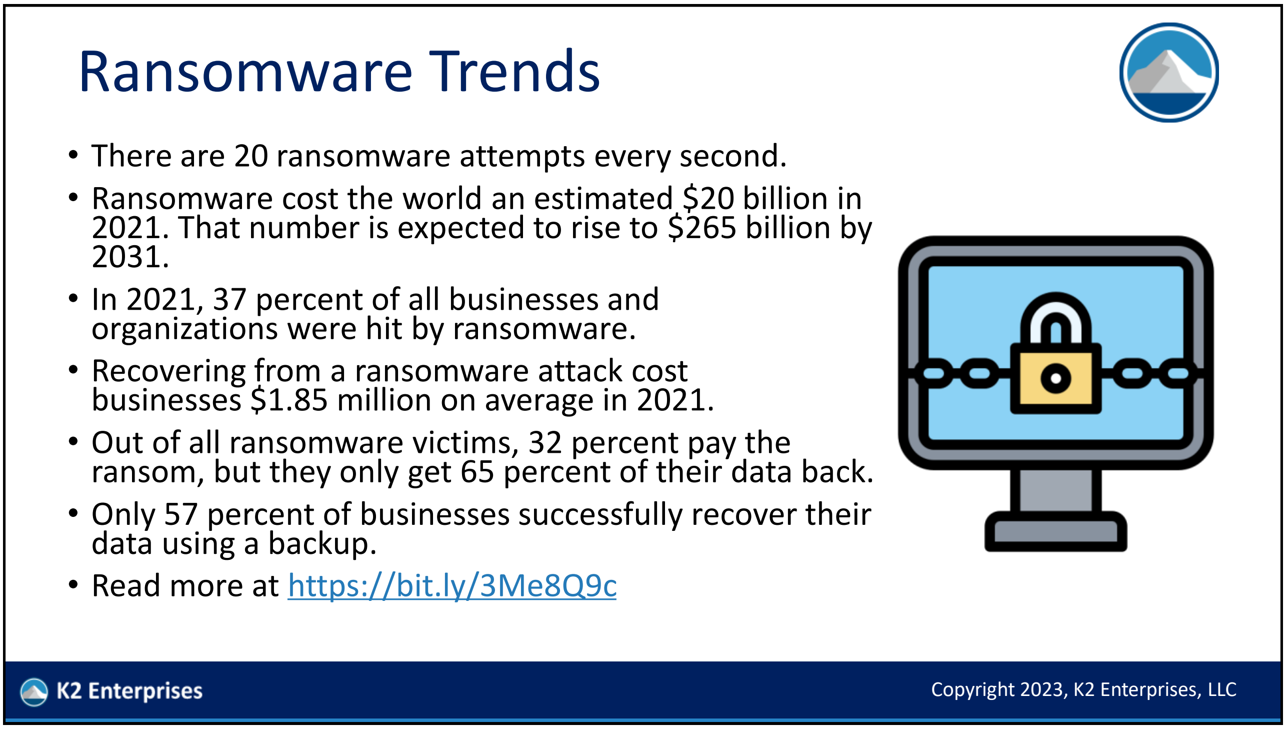
K2 Enterprises



What Is Ransomware?

- Ransomware is software that gains access and locks down access to vital data.
- Files and systems are locked down, and a fee is demanded commonly in the form of cryptocurrency.
- If the fee is not paid, the data could be lost forever or publicly exposed by the attackers.
- These are standard tools of the trade to facilitate data breaches.
- Should you pay the ransom? It depends on the circumstances, but do not put your organization in that position. Put your efforts into solid security infrastructure and backup solutions.

K2 Enterprises



Ransomware Trends

- There are 20 ransomware attempts every second.
- Ransomware cost the world an estimated $20 billion in 2021. That number is expected to rise to $265 billion by 2031.
- In 2021, 37 percent of all businesses and organizations were hit by ransomware.
- Recovering from a ransomware attack cost businesses $1.85 million on average in 2021.
- Out of all ransomware victims, 32 percent pay the ransom, but they only get 65 percent of their data back.
- Only 57 percent of businesses successfully recover their data using a backup.
- Read more at https://bit.ly/3Me8Q9c

K2 Enterprises

Colonial Pipeline Ransomware Attack

- Colonial Pipeline is the largest fuel pipeline in the USA. It is over 5.5k miles long and carries 3M barrels of fuel every day between Texas and New York.
- Hackers gained entry into the company's network in late April.
- They gained access through a former employee's account, which was not removed, nor did it have two-factor authentication.
- It is believed the password might have been leaked in another data breach and sold on the dark web.
- Once the hackers penetrated the network, they infected Colonial's system with ransomware.
- Learn more at https://bloom.bg/3zV4Wfz

Up To Triple Extortion From An Attack

Ransomware can go beyond your organization

- If you are affected by ransomware, be aware the pain and suffering don't necessarily end with you.
- **Level one.** You pay a ransom, and it ends there.
- **Level two.** Double extortion is a scam in which ransomware groups exfiltrate data before issuing a ransom note and encrypting the system, then use that data as leverage to increase the odds of securing payment.
- **Level three.** Triple extortion begins with ransomware operators exfiltrating large quantities of data, usually before encrypting the victim's network. But where double extortion groups threaten to release this data, triple extortionists filter through it, find out who might have the most to lose, and then demand ransom from them.

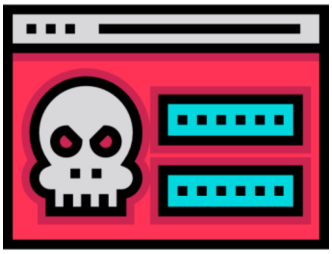
Securing our staff and their devices from anywhere in the world

IMPACT OF WORK FROM ANYWHERE (WFA)

Top Security Concerns With Remote Work

Pretty much the same risks as in the office

- Maintaining compliance
- Phishing emails
- Weak passwords
- Unsecured home devices
- Unencrypted file sharing
- Open Wi-Fi networks
- Learn more at https://bit.ly/3LbeNma



Why WFA Has Inherent Risks

While WFA risks can be mitigated, it is essential to acknowledge some of the intrinsic dangers, including:

- Staff connects to privileged resources using insecure methods (e.g., Wi-Fi with no password) or if other family member devices on the network are infected with malware.
- Staff using company resources and not locking their workstation when away from the keyboard.
- Staff not backing up their devices.
- Staff not able to ask their colleagues questions about potential security issues easily. For example, asking if a co-worker sent an email or if it was spoofed.

Recommendations To Promote Better Cybersecurity With WFA

Recommendations from Touro College Illinois on how to keep WFA secure:

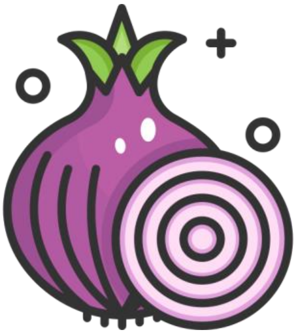
- Keep Your Confidential Files Secure
- Create Strong Passwords for All Logins and Devices
- Use an Authenticator App / Two-Factor Authentication
- Make Sure Your Video Conferences Are Secure
- Stay on Top of Software Updates & Your Operating System
- Learn more at https://bit.ly/3wrx9tS

Tips and tricks to keep your organizations secured

OVERALL SECURITY RECOMMENDATIONS

Security Is Not A Binary State

- Security isn't as simple as flipping a switch. It is not an "on" or "off" thing.
- You should think of security more like an onion, with layers. Their outer layer is your perimeter on the edge of your network. The inner layers could be different segments of your network or computers.
- Don't have all your security on the perimeter; ensure you have protection at multiple layers throughout your network.
- You can be vital in some areas and soft in others. It is a never-ending process of keeping yourself ahead of the threat actors.
- It requires constant vigilance and regular renewal. There is no magic wand.



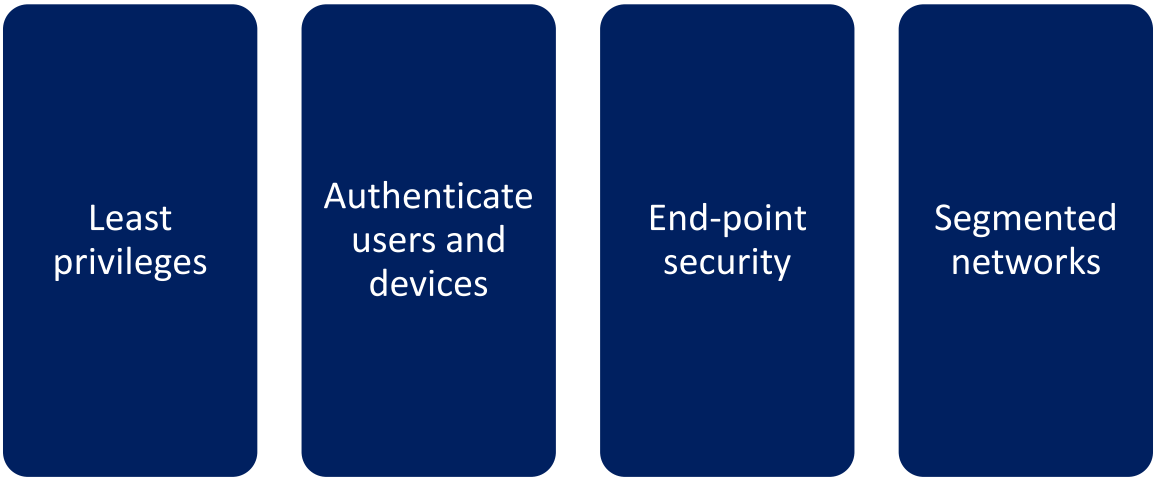
Protect Everything And Everyone

Overall Security Recommendations

- All devices and people in your organization need IT oversight and security.
- Users cannot be trusted to make good and consistent decisions about security.
- Security needs to be applied uniformly and enforced from the CEO to the intern.
- You need to have standard security policies and practices that conform to industry best practices.
- If you are not competent in this area, you must acquire this knowledge. Don’t do it on your own.

Zero Trust Security Model Pillars

Overall Security Recommendations



Least privileges

Authenticate users and devices

End-point security

Segmented networks

Know Your Potential Attackers

Overall Security Recommendations

- Every organization has a specific attack profile. If you're unsure of your attack profile, check out the Verizon DBIR report.
- It would be suitable for you to know your most likely threat actor (e.g., insider, nation-state, etc.).
- It would also be good to know your most likely attack vector (e.g., ransomware, phishing, etc.).
- You should also know what is most likely to be stolen (e.g., financial assets, customer data, trade secrets, etc.) and protect it accordingly.

Be Prepared And Ready To Act

Overall Security Recommendations

- You should consider developing a disaster recovery and a business continuity plan.
- A formalized written program that you can immediately put into effect would be invaluable in a disaster.
- A disaster recovery plan focuses on the first 72-hours after an incident. It focuses on human life safety and securing property, plant, and equipment. The plan's goal is to get your organization up and running as quickly as possible.
- A business continuity plan focuses on the next 12-24 months and ensuring your organization can survive.

Humans Are Your Biggest Risk

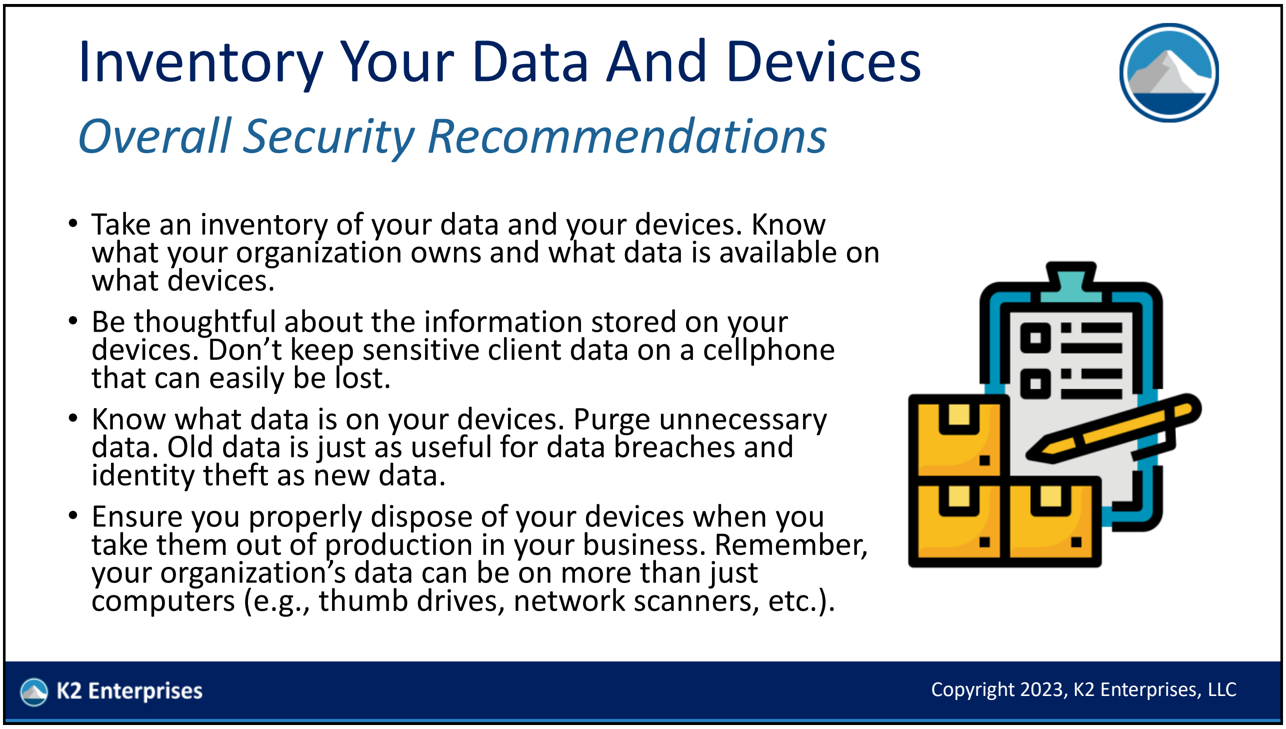
Overall Security Recommendations

- If your organization has a security event, it is more likely than not to result from human behavior. For example, clicking on a phishing link or downloading an email attachment with malware.
- The best method to reduce your risk and exposure is to educate yourself and your team.
- Seriously, training is the best thing you can do is get educated on security and privacy. You need to know how this stuff works. After all, it's your data and livelihood.
- Consider using a resource such as KnowBe4 or GoPhish to give them some experience and insight on an attack before it happens.

SANS Institute Security Policies

Overall Security Recommendations

- In collaboration with information security subject-matter experts and leaders who volunteered their security policy know-how and time, SANS has developed and posted a set of security policy templates for your use.
- The provided security policies cover virtually all aspects of IT governance from acceptable use, password construction guidelines, remote access, and more.
- Security policies are FREE in Word (.docx) and PDF format.
- Pick some policies that reflect your staff and your organization's specific risks. You might want to include them in your staff's employee handwork.
- Check out the FREE security policies provided by the SANS Institute at https://www.sans.org/



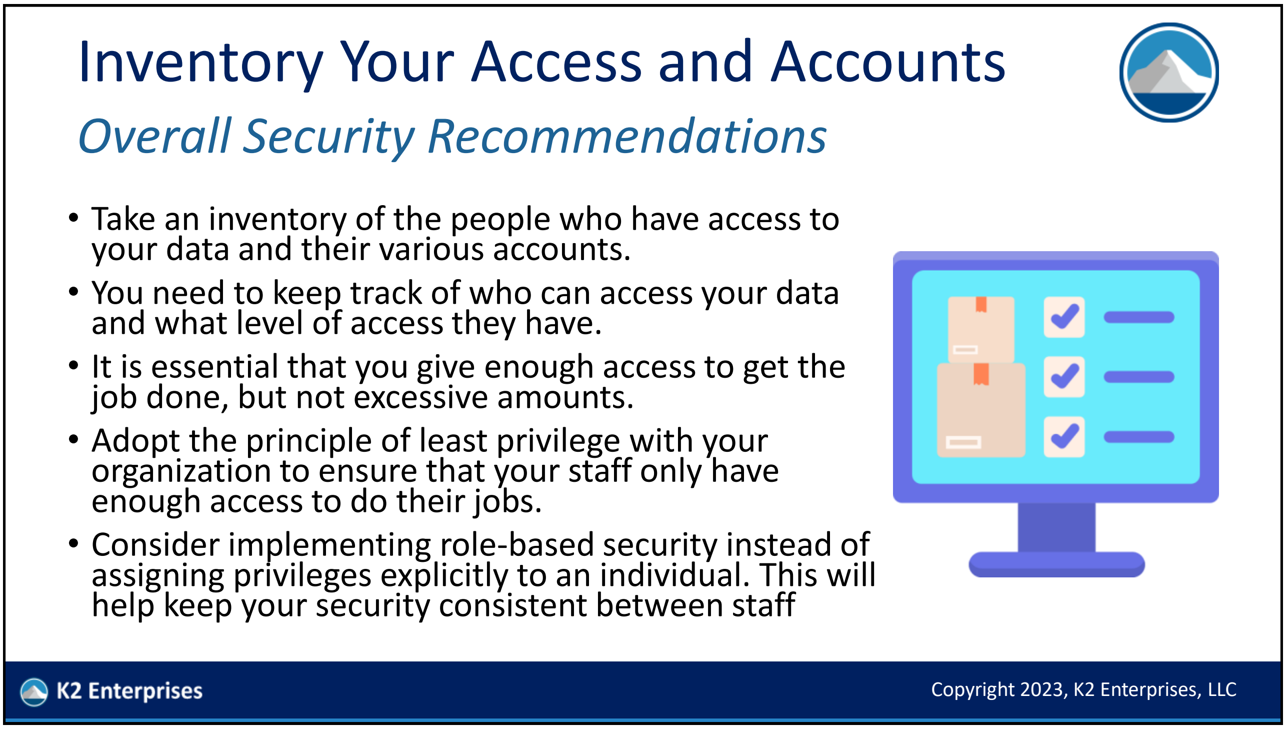
Inventory Your Data And Devices

Overall Security Recommendations

- Take an inventory of your data and your devices. Know what your organization owns and what data is available on what devices.
- Be thoughtful about the information stored on your devices. Don’t keep sensitive client data on a cellphone that can easily be lost.
- Know what data is on your devices. Purge unnecessary data. Old data is just as useful for data breaches and identity theft as new data.
- Ensure you properly dispose of your devices when you take them out of production in your business. Remember, your organization’s data can be on more than just computers (e.g., thumb drives, network scanners, etc.).

K2 Enterprises

Copyright 2023, K2 Enterprises, LLC



Inventory Your Access and Accounts

Overall Security Recommendations

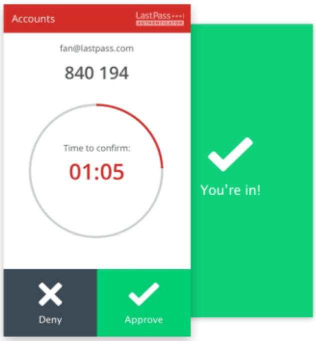
- Take an inventory of the people who have access to your data and their various accounts.
- You need to keep track of who can access your data and what level of access they have.
- It is essential that you give enough access to get the job done, but not excessive amounts.
- Adopt the principle of least privilege with your organization to ensure that your staff only have enough access to do their jobs.
- Consider implementing role-based security instead of assigning privileges explicitly to an individual. This will help keep your security consistent between staff

K2 Enterprises

Copyright 2023, K2 Enterprises, LLC

Multi-Factor Authentication

- The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password.
- Most MFA authentication methodology is based on one of three types of additional information:
  - Things you know (knowledge), such as a password or PIN
  - Things you have (possession), such as a badge or smartphone
  - Things you are (inherence), such as a biometric like fingerprints or voice recognition
- What is multifactor authentication? http://bit.ly/2KE9aTH



tommy@k2e.com

THANKS!