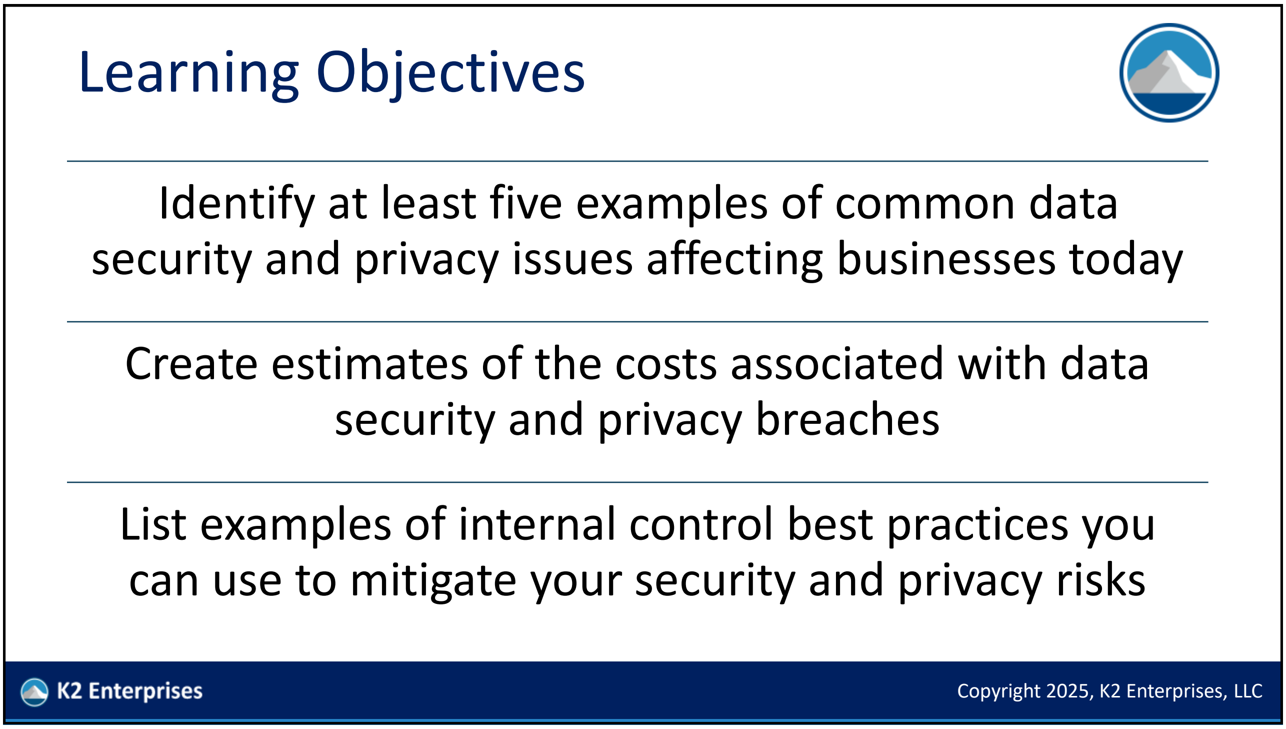
K2's Data Security And Privacy Issues And Solutions

The Never-Ending Problem!

K2 Enterprises



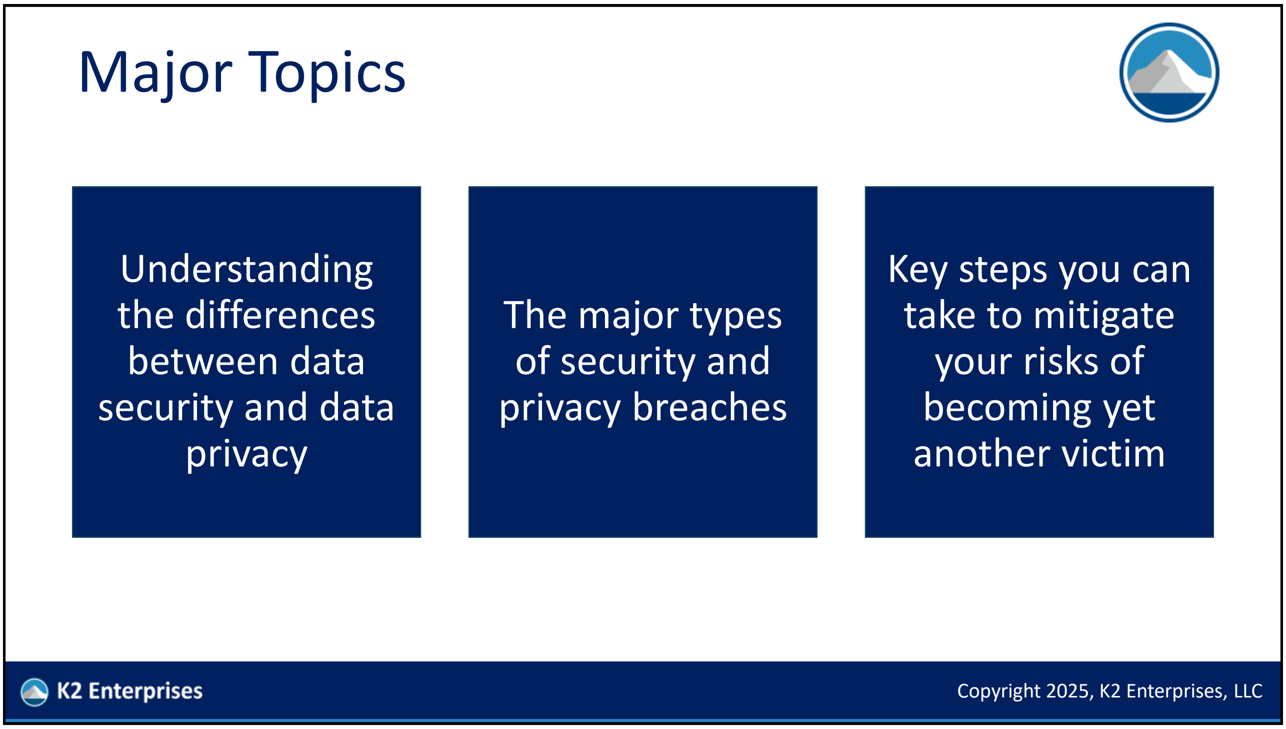
Learning Objectives

Identify at least five examples of common data security and privacy issues affecting businesses today

Create estimates of the costs associated with data security and privacy breaches

List examples of internal control best practices you can use to mitigate your security and privacy risks

K2 Enterprises

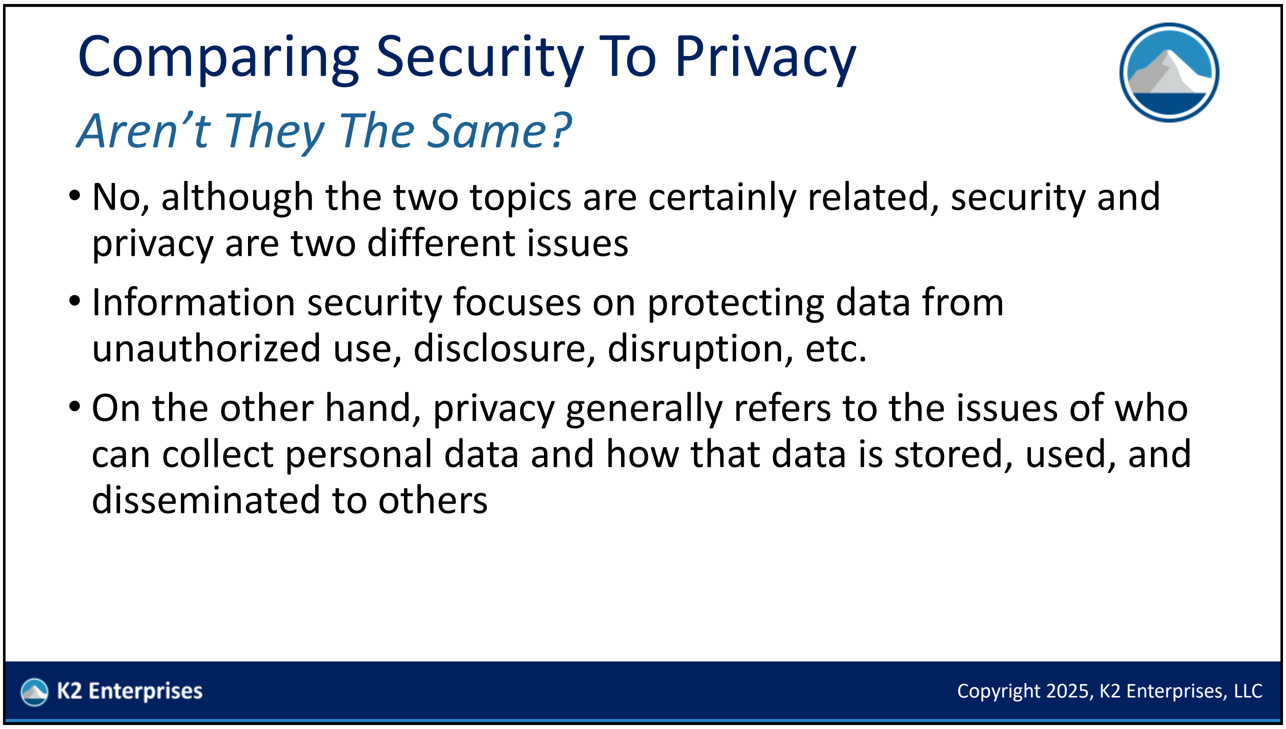


Major Topics

- Understanding the differences between data security and data privacy
- The major types of security and privacy breaches
- Key steps you can take to mitigate your risks of becoming yet another victim

K2 Enterprises

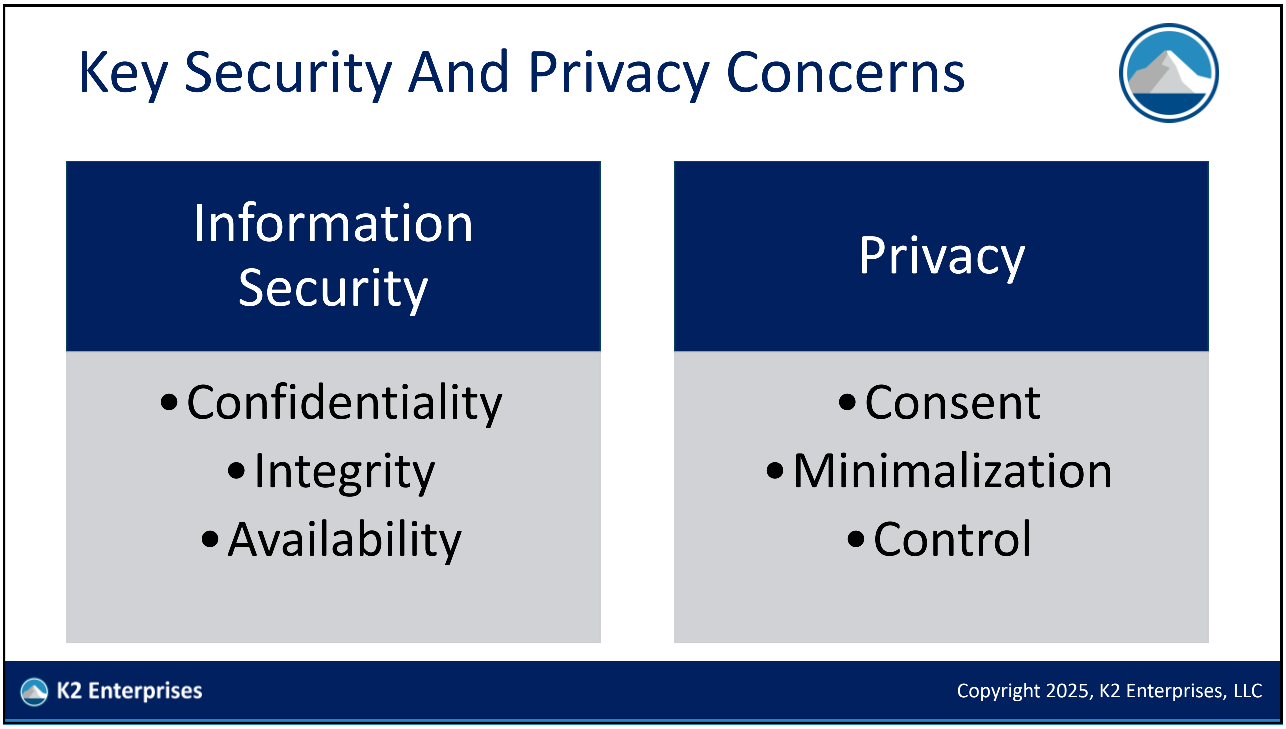
LET'S GET STARTED…



Comparing Security To Privacy

Aren't They The Same?

- No, although the two topics are certainly related, security and privacy are two different issues
- Information security focuses on protecting data from unauthorized use, disclosure, disruption, etc.
- On the other hand, privacy generally refers to the issues of who can collect personal data and how that data is stored, used, and disseminated to others



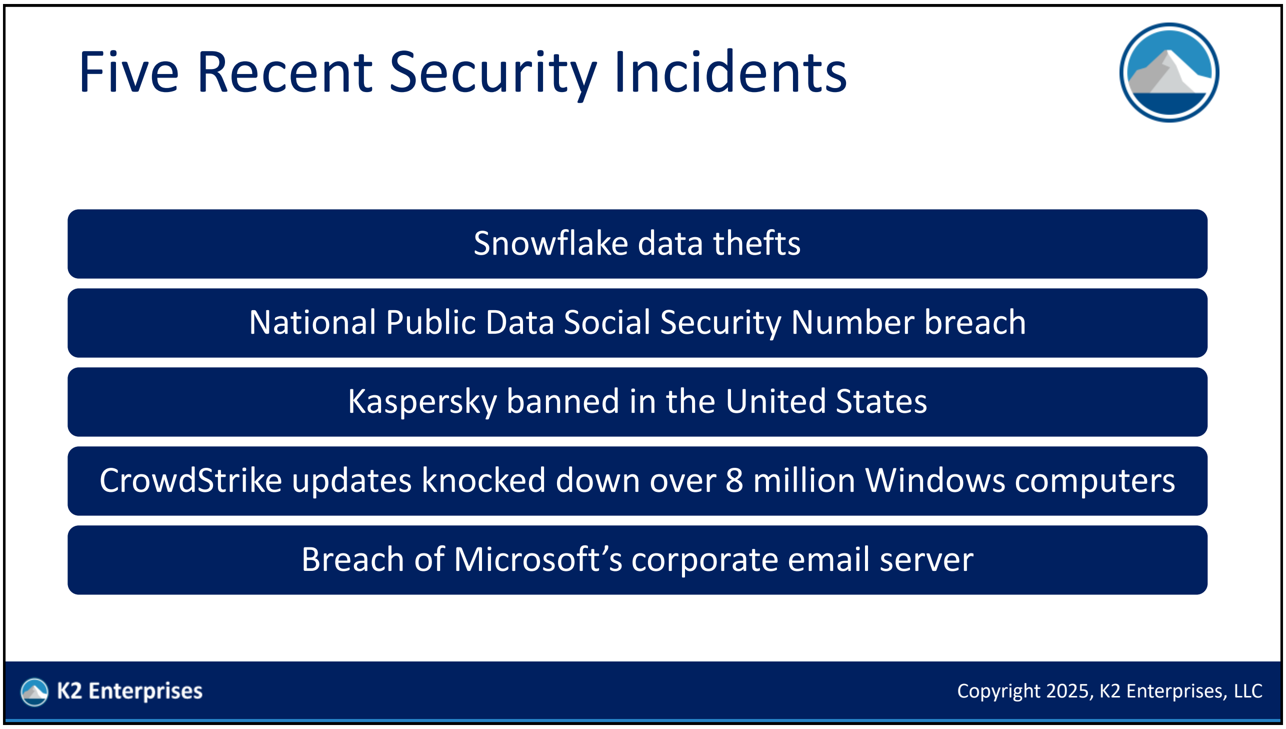
Key Security And Privacy Concerns

Information Security

- Confidentiality
- Integrity
- Availability

Privacy

- Consent
- Minimalization
- Control



Five Recent Security Incidents

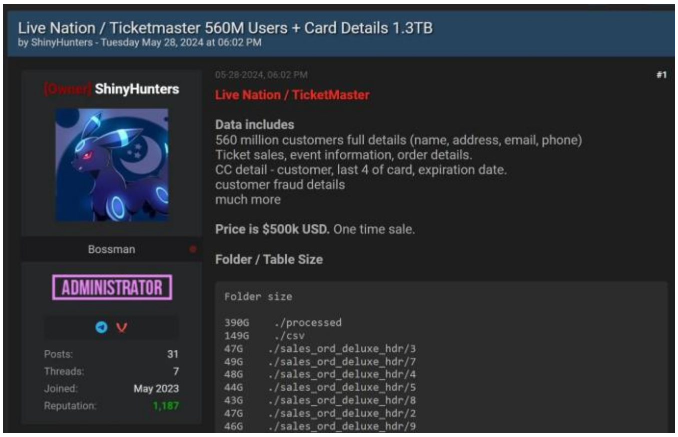
- Snowflake data thefts
- National Public Data Social Security Number breach
- Kaspersky banned in the United States
- CrowdStrike updates knocked down over 8 million Windows computers
- Breach of Microsoft’s corporate email server

Snowflake

- In May 2024, cybercriminals known as ShinyHunters began selling data they claimed was stolen from Snowflake’s cloud data platform
  - Snowflake is a Cloud-based data storage company in Bozeman, MT
- The hackers gained access to the data using compromised credentials to log in to the accounts
- Once they logged in, they gained access to the data and extorted companies such as AT&T (109 million affected customers) and Ticketmaster (560 million customers)

Snowflake Data Theft

The crooks attempted to sell the data for $500k



Live Nation / Ticketmaster 560M Users + Card Details 1.3TB
by ShinyHunters - Tuesday May 28, 2024 at 06:02 PM

[Owner] ShinyHunters

Bossman

ADMINISTRATOR

Posts: 31
Threads: 7
Joined: May 2023
Reputation: 1,187

05-28-2024, 06:02 PM #1

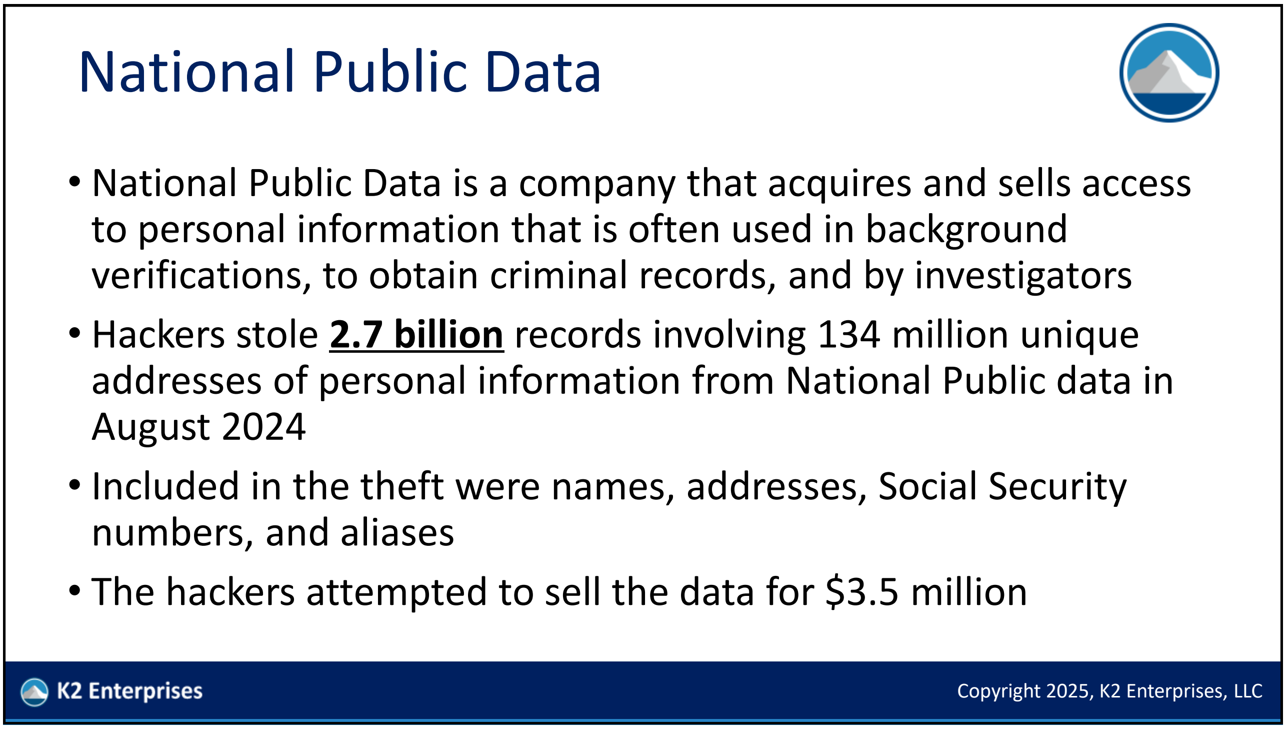
Live Nation / TicketMaster

Data includes
560 million customers full details (name, address, email, phone)
Ticket sales, event information, order details.
CC detail - customer, last 4 of card, expiration date.
customer fraud details
much more

Price is $500k USD. One time sale.

Folder / Table Size

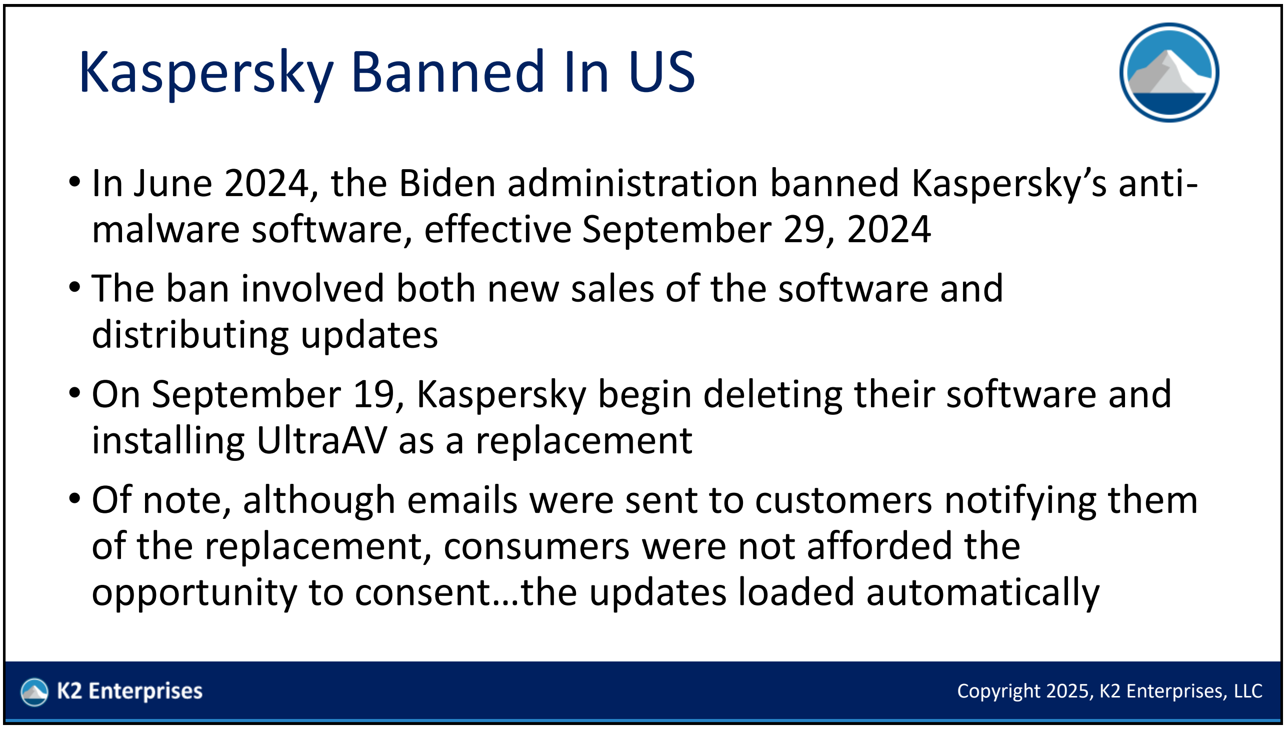
```
Folder size

390G   ./processed
149G   ./csv
47G   ./sales_ord_deluxe_hdr/3
49G   ./sales_ord_deluxe_hdr/7
48G   ./sales_ord_deluxe_hdr/4
44G   ./sales_ord_deluxe_hdr/5
43G   ./sales_ord_deluxe_hdr/8
47G   ./sales_ord_deluxe_hdr/2
46G   ./sales_ord_deluxe_hdr/9
```



National Public Data

- National Public Data is a company that acquires and sells access to personal information that is often used in background verifications, to obtain criminal records, and by investigators
- Hackers stole **2.7 billion** records involving 134 million unique addresses of personal information from National Public data in August 2024
- Included in the theft were names, addresses, Social Security numbers, and aliases
- The hackers attempted to sell the data for $3.5 million

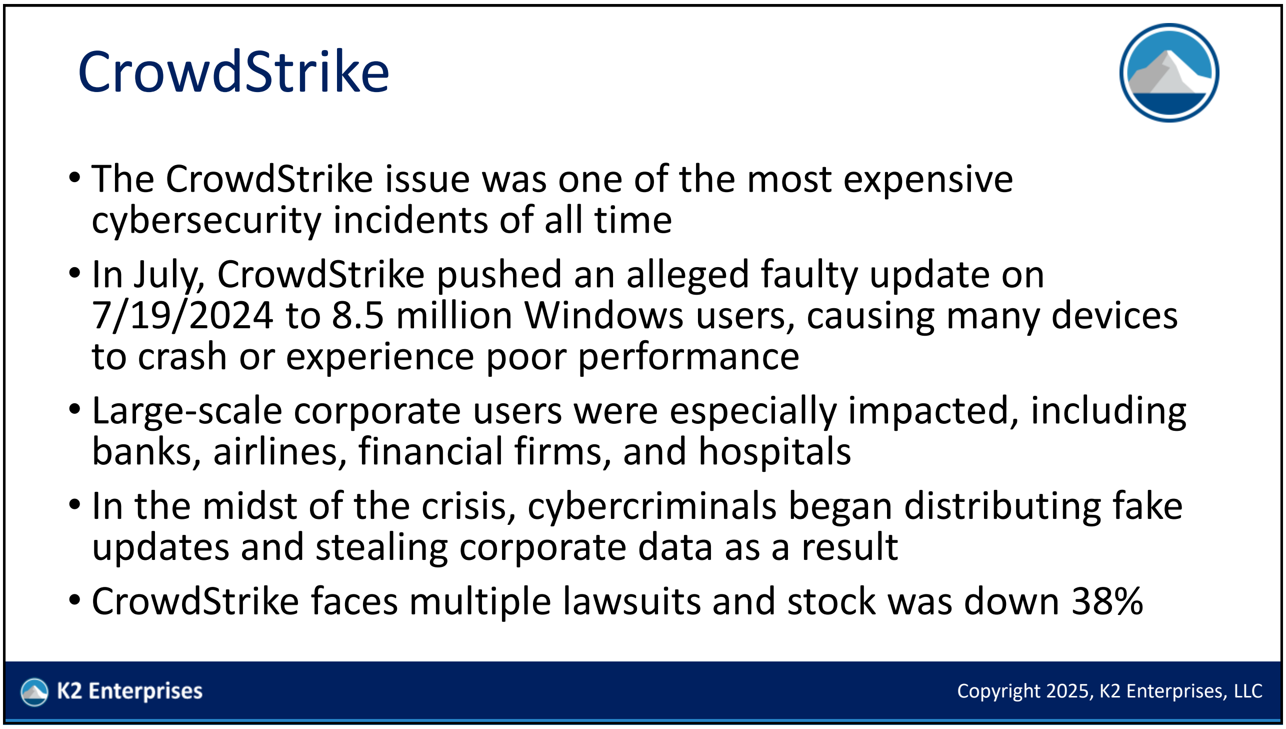
K2 Enterprises



Kaspersky Banned In US

- In June 2024, the Biden administration banned Kaspersky’s anti-malware software, effective September 29, 2024
- The ban involved both new sales of the software and distributing updates
- On September 19, Kaspersky begin deleting their software and installing UltraAV as a replacement
- Of note, although emails were sent to customers notifying them of the replacement, consumers were not afforded the opportunity to consent…the updates loaded automatically

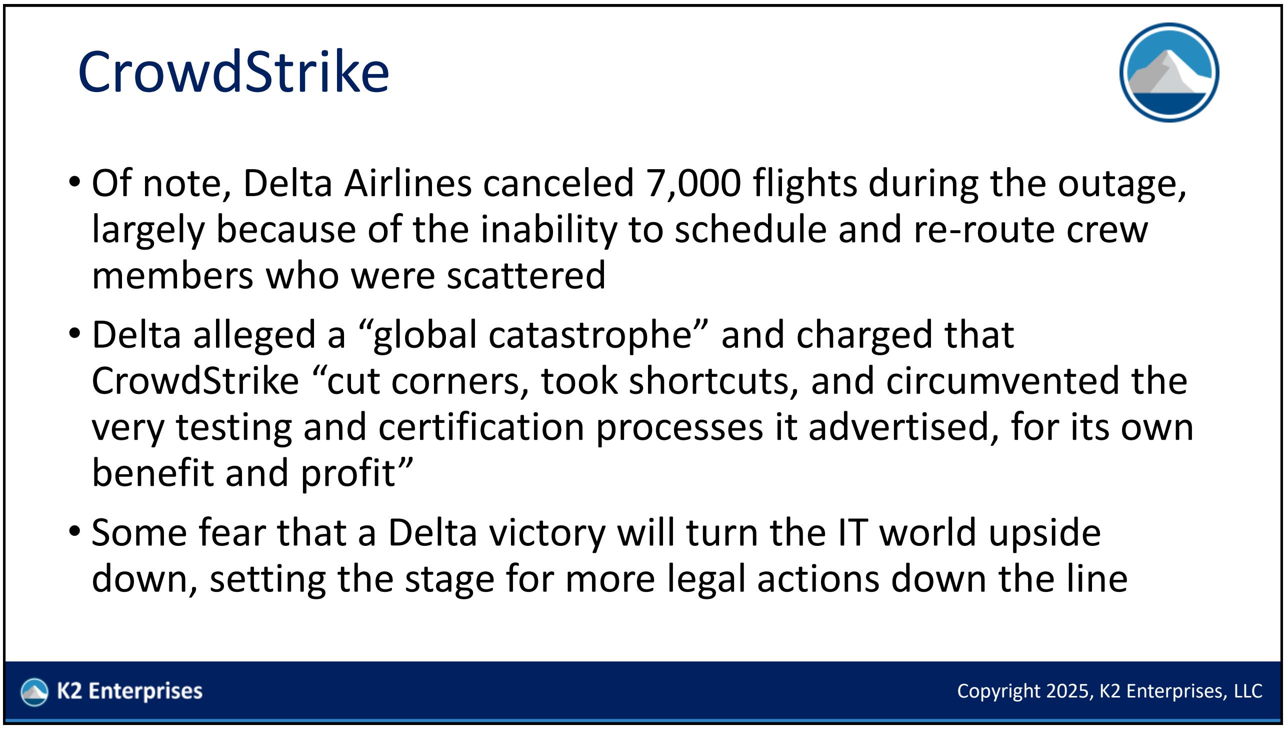
K2 Enterprises



CrowdStrike

- The CrowdStrike issue was one of the most expensive cybersecurity incidents of all time
- In July, CrowdStrike pushed an alleged faulty update on 7/19/2024 to 8.5 million Windows users, causing many devices to crash or experience poor performance
- Large-scale corporate users were especially impacted, including banks, airlines, financial firms, and hospitals
- In the midst of the crisis, cybercriminals began distributing fake updates and stealing corporate data as a result
- CrowdStrike faces multiple lawsuits and stock was down 38%

K2 Enterprises



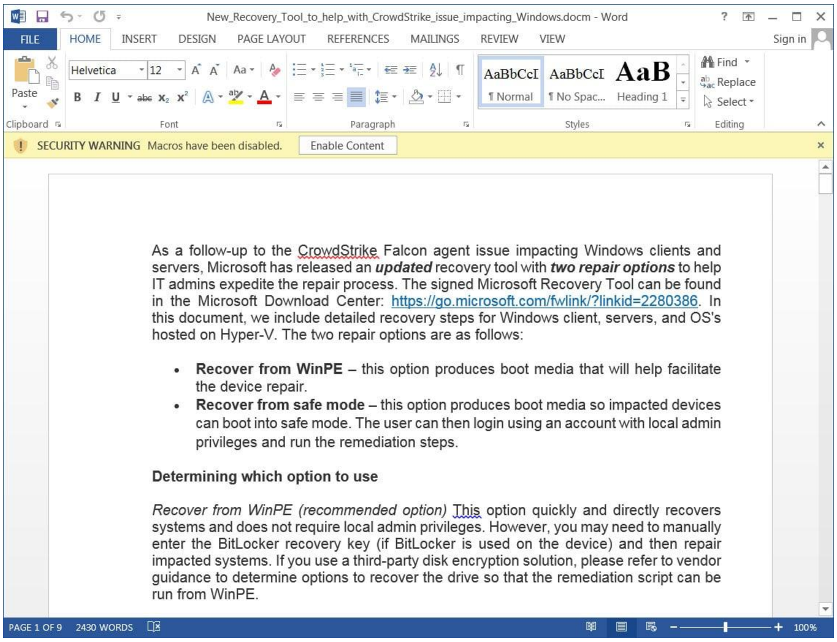
CrowdStrike

- Of note, Delta Airlines canceled 7,000 flights during the outage, largely because of the inability to schedule and re-route crew members who were scattered
- Delta alleged a “global catastrophe” and charged that CrowdStrike “cut corners, took shortcuts, and circumvented the very testing and certification processes it advertised, for its own benefit and profit”
- Some fear that a Delta victory will turn the IT world upside down, setting the stage for more legal actions down the line

K2 Enterprises

Some Smelled Blood In The Water

- Amid the crisis, some bad actors began posing as CrowdStrike employees or contractors and offering to “solve” the problem
- Of course, the criminals weren’t there to solve the problem
- On the contrary, they sought access to the affected computers and servers so they could harvest the data stored on them



As a follow-up to the CrowdStrike Falcon agent issue impacting Windows clients and servers, Microsoft has released an ***updated*** recovery tool with ***two repair options*** to help IT admins expedite the repair process. The signed Microsoft Recovery Tool can be found in the Microsoft Download Center: https://go.microsoft.com/fwlink/?linkid=2280386. In this document, we include detailed recovery steps for Windows client, servers, and OS's hosted on Hyper-V. The two repair options are as follows:

- **Recover from WinPE** – this option produces boot media that will help facilitate the device repair.
- **Recover from safe mode** – this option produces boot media so impacted devices can boot into safe mode. The user can then login using an account with local admin privileges and run the remediation steps.

Determining which option to use

Recover from WinPE (recommended option) This option quickly and directly recovers systems and does not require local admin privileges. However, you may need to manually enter the BitLocker recovery key (if BitLocker is used on the device) and then repair impacted systems. If you use a third-party disk encryption solution, please refer to vendor guidance to determine options to recover the drive so that the remediation script can be run from WinPE.

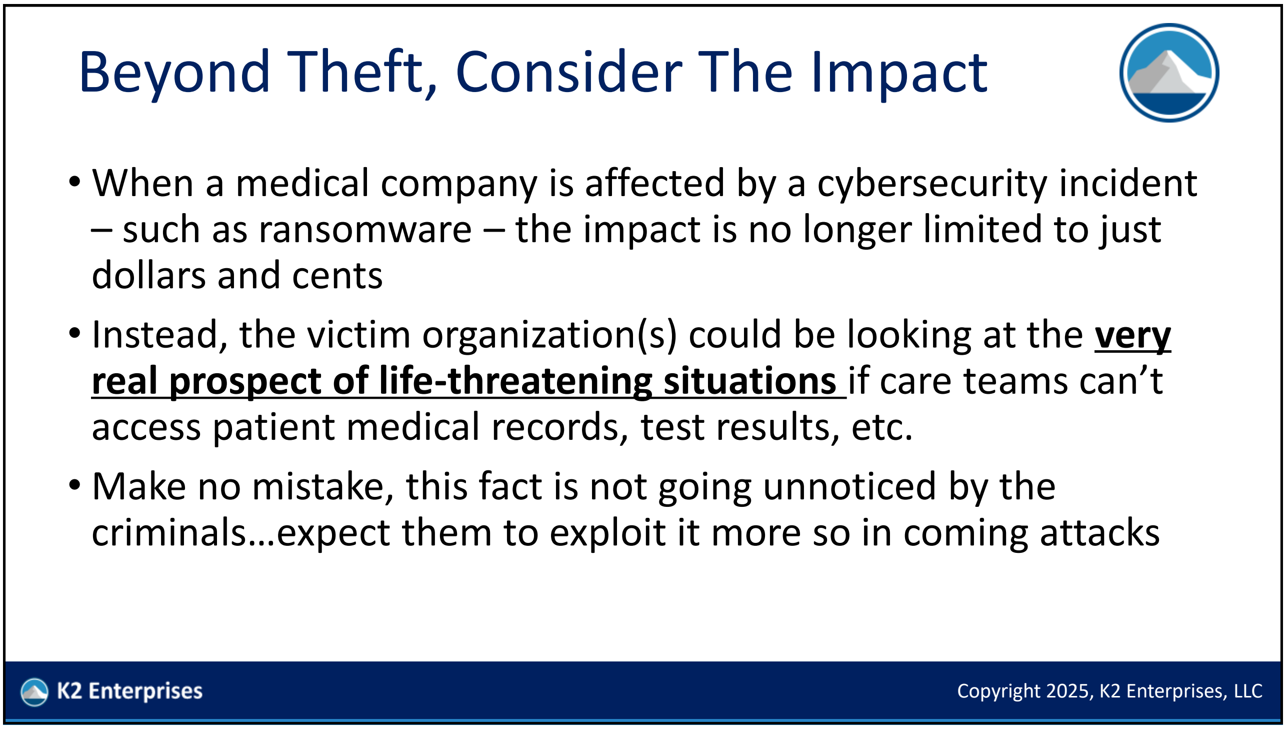
Fake Notice Offering “Solution” To The CrowdStrike Falcon Update Issue

CrowdStrike: A Supply Chain Attack

- The CrowdStrike issue provides an example of what is known as a “supply-chain attack”
- We typically think of supply chains in terms of goods and products, such as groceries, clothing, and equipment
- However, in the IT environment, a supply chain is a digital one, not physical
- Thus, a purposeful disruption of information technology and data processing represents a supply-chain attack in this sector

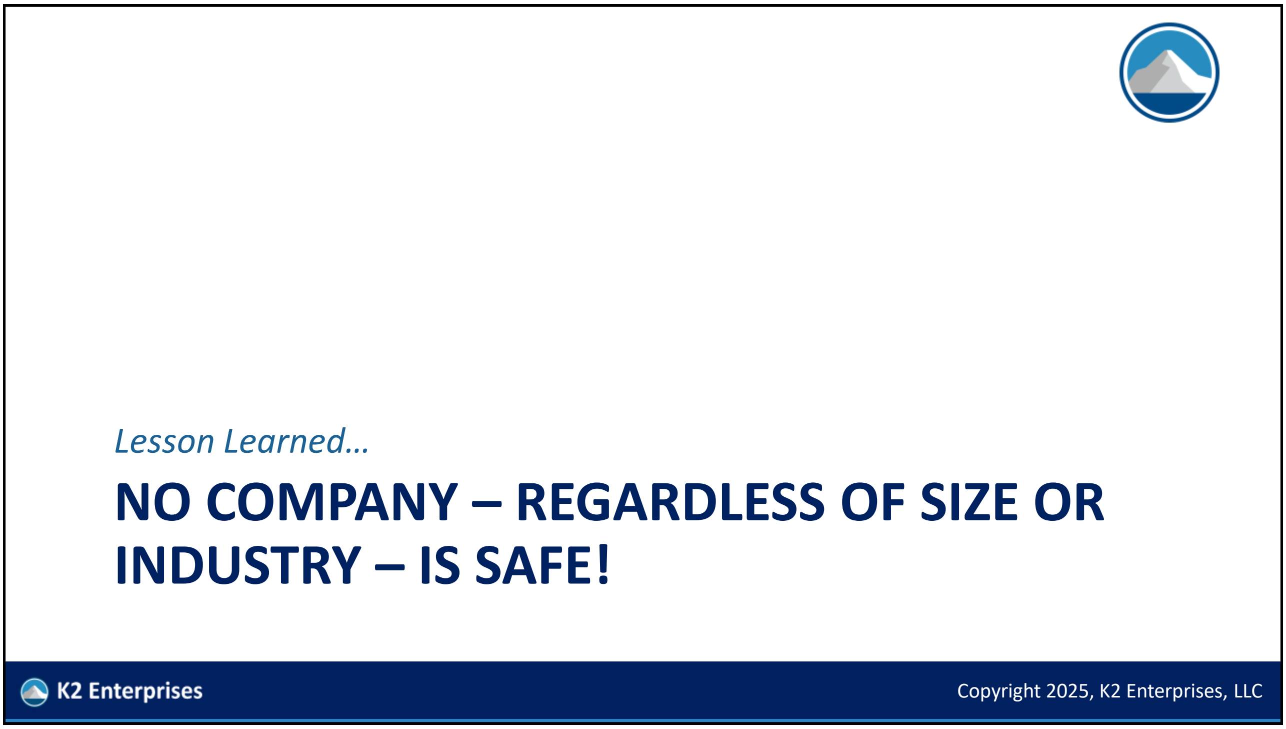
UnitedHealth Ransomware Attack

- Change Healthcare – a subsidiary of United Healthcare – experienced a significant ransomware attack in February 2024
- The attack compromised over 6TB of data and was precipitated by stolen credentials used to breach the company’s remote access service – without multifactor authentication enabled!
- Over 100 million people had their personal and healthcare data compromised in the attack
- The company paid the ransom, allegedly $22 million



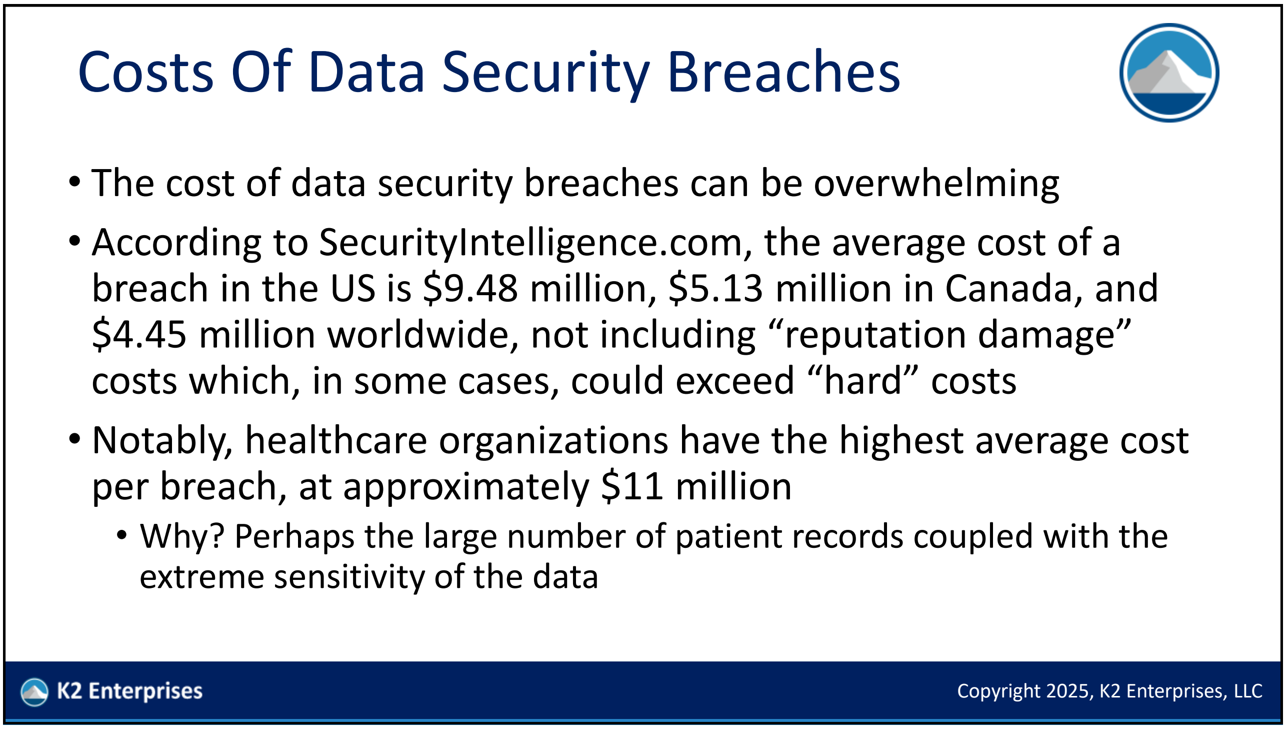
Beyond Theft, Consider The Impact

- When a medical company is affected by a cybersecurity incident – such as ransomware – the impact is no longer limited to just dollars and cents
- Instead, the victim organization(s) could be looking at the **very real prospect of life-threatening situations** if care teams can't access patient medical records, test results, etc.
- Make no mistake, this fact is not going unnoticed by the criminals…expect them to exploit it more so in coming attacks



Lesson Learned…

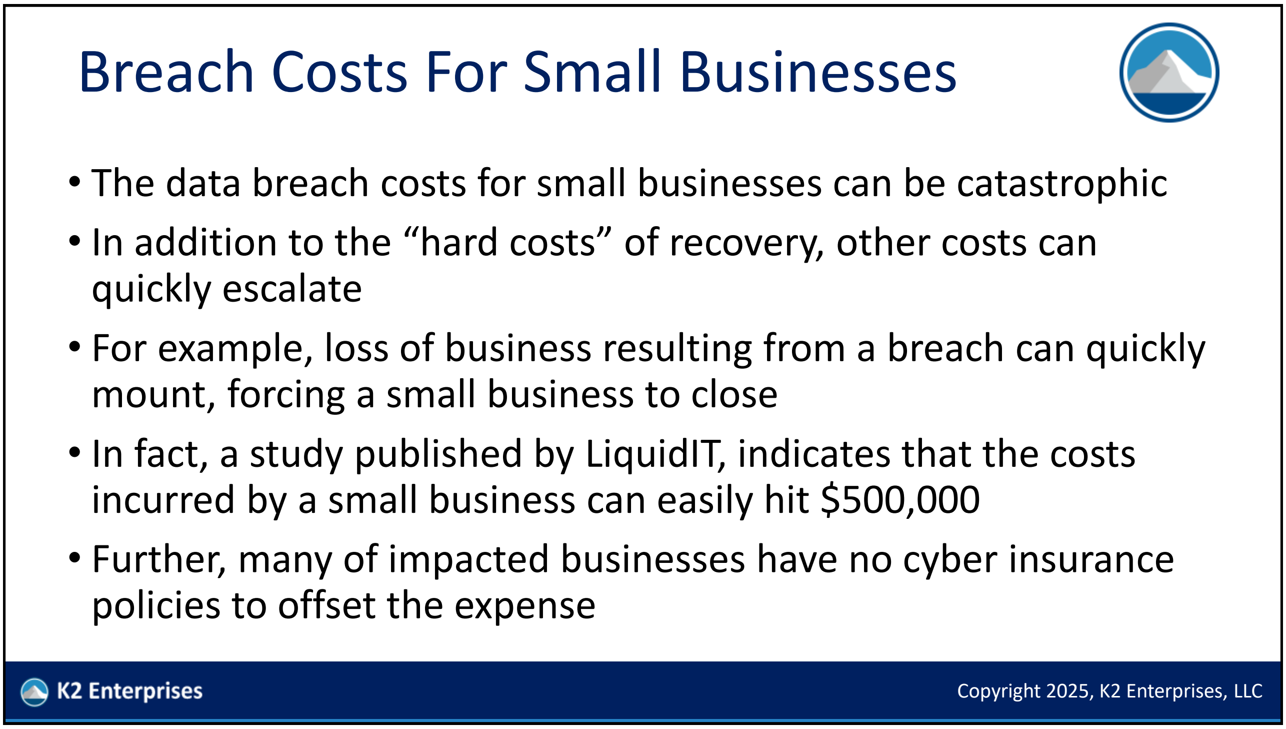
NO COMPANY – REGARDLESS OF SIZE OR INDUSTRY – IS SAFE!



Costs Of Data Security Breaches

- The cost of data security breaches can be overwhelming
- According to SecurityIntelligence.com, the average cost of a breach in the US is $9.48 million, $5.13 million in Canada, and $4.45 million worldwide, not including “reputation damage” costs which, in some cases, could exceed “hard” costs
- Notably, healthcare organizations have the highest average cost per breach, at approximately $11 million
  - Why? Perhaps the large number of patient records coupled with the extreme sensitivity of the data

K2 Enterprises



Breach Costs For Small Businesses

- The data breach costs for small businesses can be catastrophic
- In addition to the “hard costs” of recovery, other costs can quickly escalate
- For example, loss of business resulting from a breach can quickly mount, forcing a small business to close
- In fact, a study published by LiquidIT, indicates that the costs incurred by a small business can easily hit $500,000
- Further, many of impacted businesses have no cyber insurance policies to offset the expense

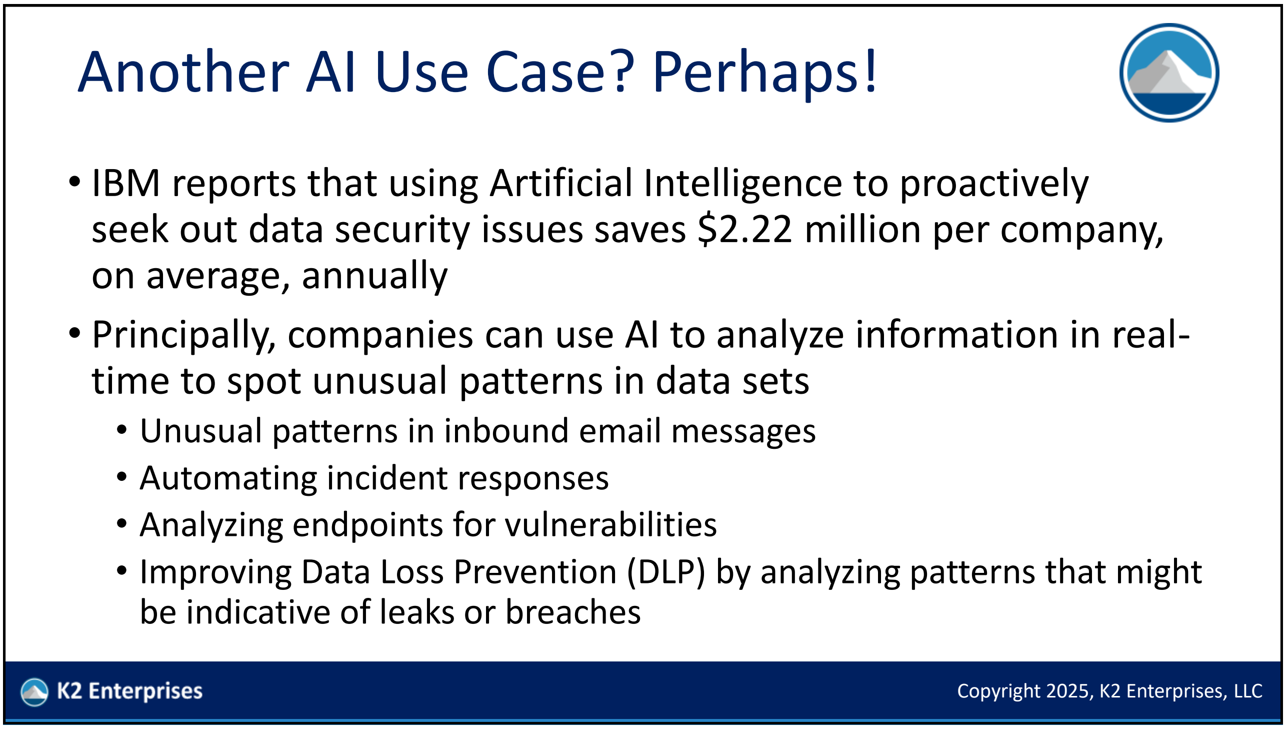
K2 Enterprises

Costs Of Data Security Breaches

- Direct remediation costs
- Indirect costs, such as customer churn and reputation damage
- Regulatory fines and penalties, which can vary significantly depending on size and type of business
- Operations disruptions, such as those incurred by Delta Airlines in the CrowdStrike incident
- Long term indirect costs, such as insurance premiums and legal fees

Costs Of Data Security Breaches

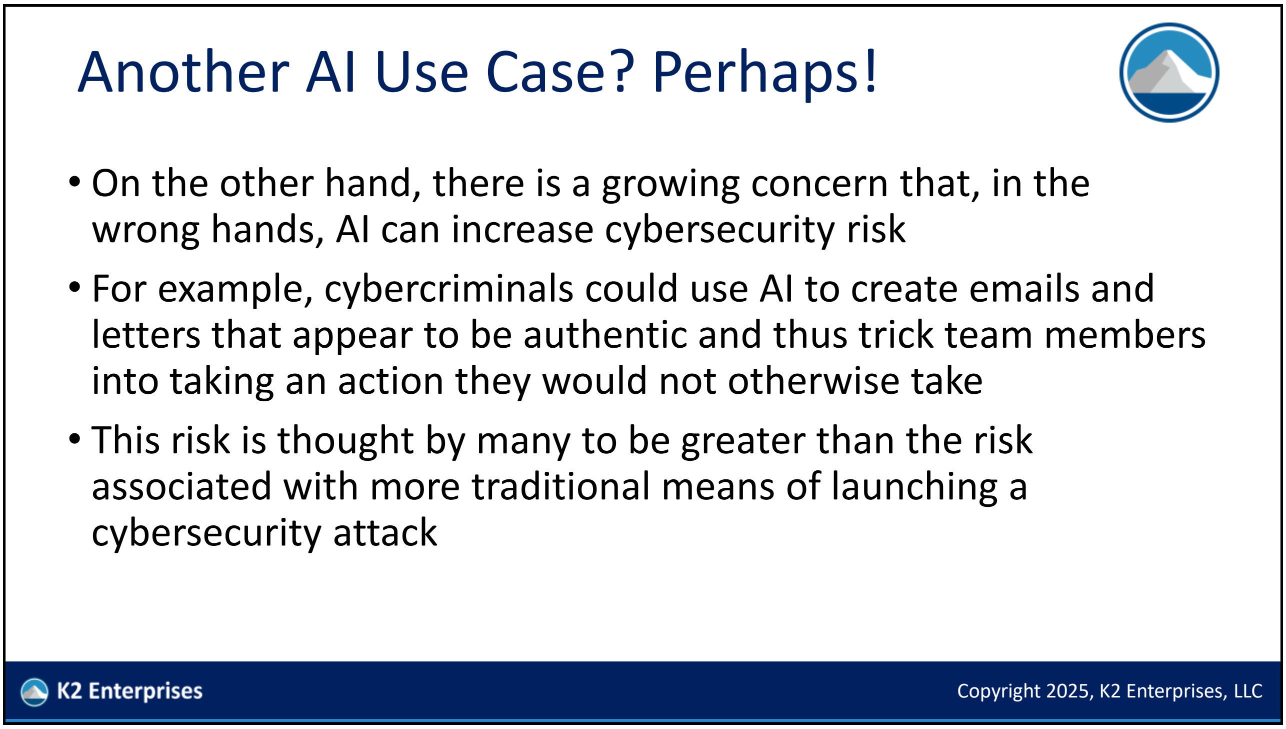
- Note that costs can vary significantly by size and type of business involved
- For example, IBM reports that companies in healthcare, finance, and pharmaceuticals have higher remediation and recovery costs than those in other lines of business
- Additionally, breaches that involve personally identifiable information are the most expensive to resolve



Another AI Use Case? Perhaps!

- IBM reports that using Artificial Intelligence to proactively seek out data security issues saves $2.22 million per company, on average, annually
- Principally, companies can use AI to analyze information in real-time to spot unusual patterns in data sets
  - Unusual patterns in inbound email messages
  - Automating incident responses
  - Analyzing endpoints for vulnerabilities
  - Improving Data Loss Prevention (DLP) by analyzing patterns that might be indicative of leaks or breaches

K2 Enterprises



Another AI Use Case? Perhaps!

- On the other hand, there is a growing concern that, in the wrong hands, AI can increase cybersecurity risk
- For example, cybercriminals could use AI to create emails and letters that appear to be authentic and thus trick team members into taking an action they would not otherwise take
- This risk is thought by many to be greater than the risk associated with more traditional means of launching a cybersecurity attack

K2 Enterprises

A Dangerous And Persistent Threat

RANSOMWARE

Ransomware Remains A Top Risk

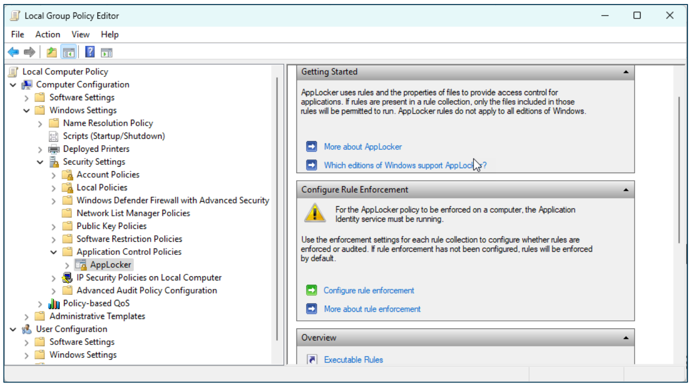
- In a ransomware attack, the threat actor(s) gain access to and take control of your data and hold it hostage in exchange for a ransom payment
- The threat actors recognize that your data may be your most valuable asset; as such, many victims will pay whatever it takes to regain their data
- Caution! An emerging trend with ransomware is to extort the same victim multiple times

AppLocker

- You can control which apps run on a computer by activating AppLocker, a Windows feature
- With AppLocker active, you can minimize the chances that unauthorized software can run on your device
- If unauthorized software can't run, it's going to be much less likely that ransomware or other forms of malware can be installed by the device's user(s)
- AppLocker can also reduce the likelihood of a team member violating software licensing policies

AppLocker

- You can use AppLocker to perform the following functions
  - Control who can run specified applications
  - Prevent users from running unauthorized or unlicensed applications
  - Block unsupported applications from use


Local Group Policy Editor
File
Action
View
Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Getting Started
More about AppLocker
Which editions of Windows support AppLocker?
Configure Rule Enforcement
Configure rule enforcement
More about rule enforcement
Overview
Executable Rules

AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.

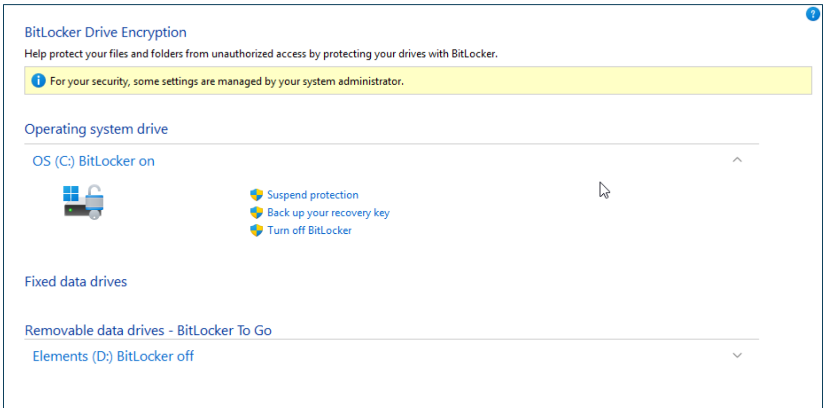
For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.

Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.

BitLocker

- BitLocker – which first appeared in 2007 with the release of Windows Vista – is a Microsoft security tool embedded into the Windows operating system
- BitLocker is a whole-disk encryption tool that encrypts all the contents of your hard disk automatically
- Thus, if a bad actor gains physical access to your device, they are not able to access its contents if they don't have access to the encryption key
- As such, it is less likely they can make changes to the files

BitLocker



BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

OS (C:) BitLocker on

Suspend protection

Back up your recovery key

Turn off BitLocker

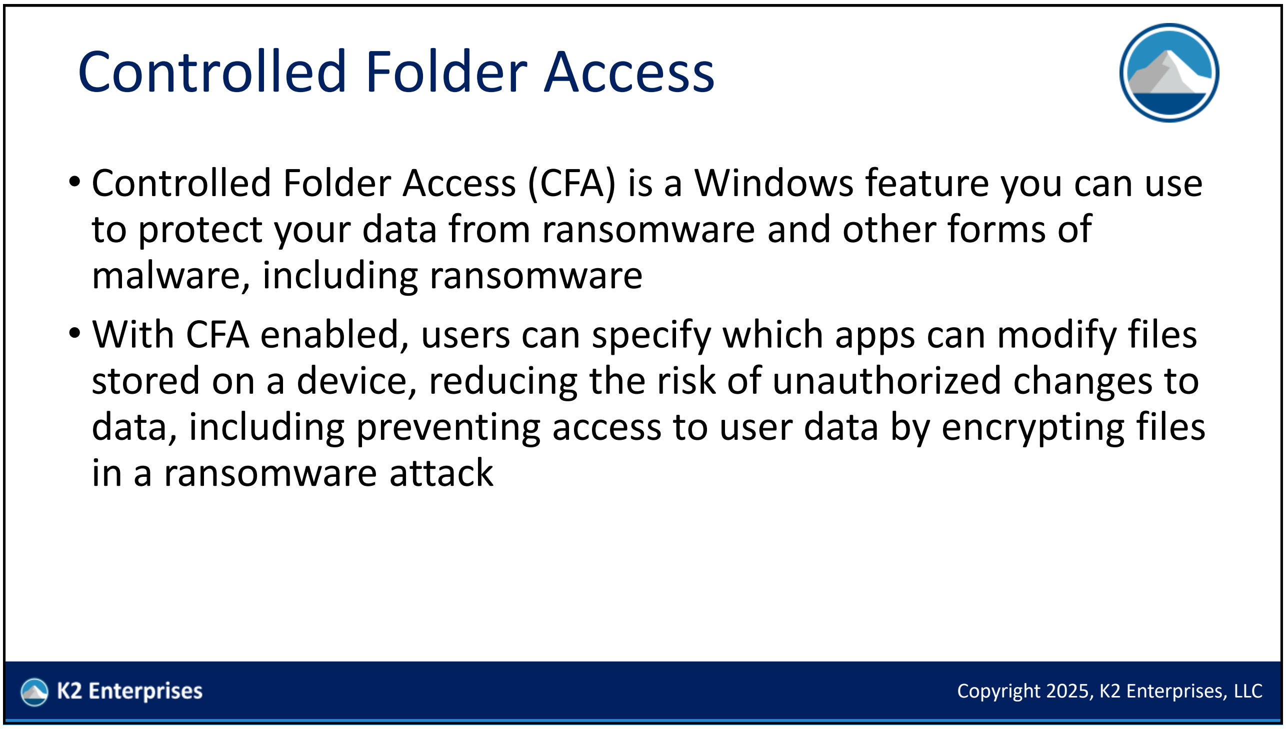
Fixed data drives

Removable data drives - BitLocker To Go

Elements (D:) BitLocker off

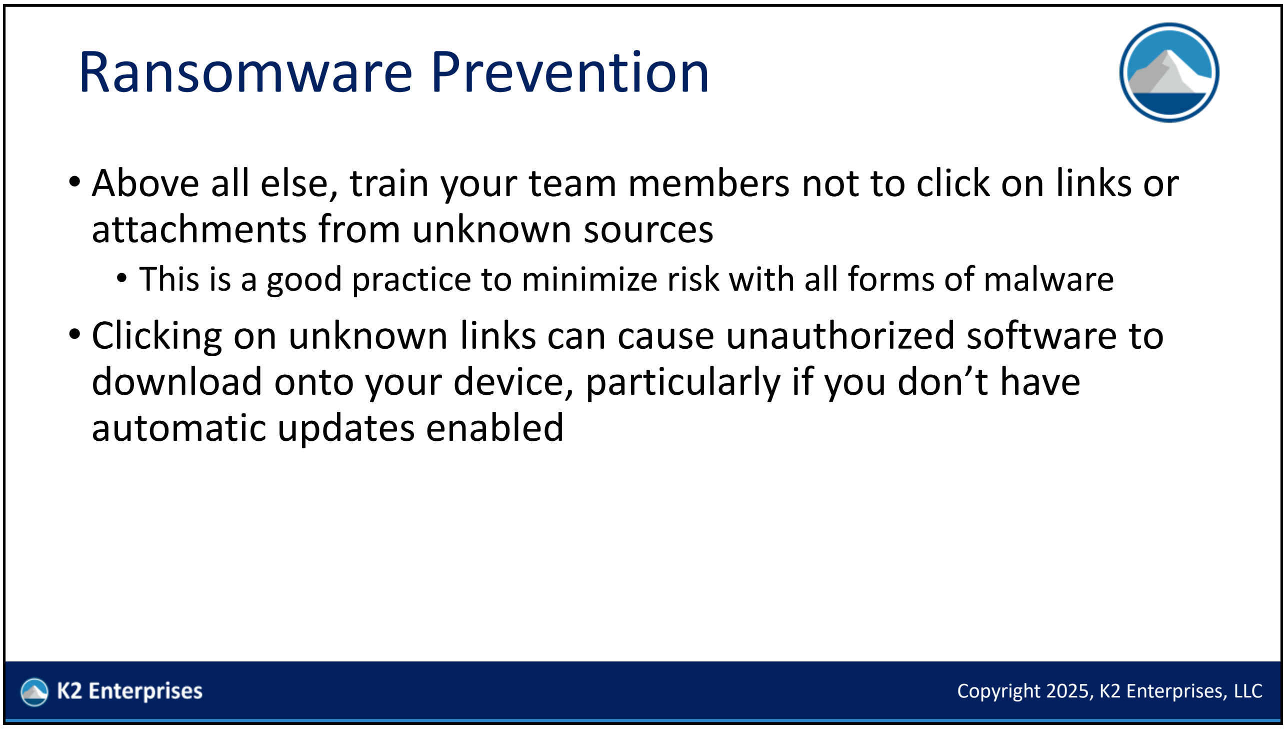
If you need to recover your key, visit https://k2e.fyi/bitlocker

- Note that you will want to backup your recovery key to
  1. Azure AD account,
  2. Microsoft account,
  3. Save to a file, and/or
  4. Print the key



Controlled Folder Access

- Controlled Folder Access (CFA) is a Windows feature you can use to protect your data from ransomware and other forms of malware, including ransomware
- With CFA enabled, users can specify which apps can modify files stored on a device, reducing the risk of unauthorized changes to data, including preventing access to user data by encrypting files in a ransomware attack



Ransomware Prevention

- Above all else, train your team members not to click on links or attachments from unknown sources
  - This is a good practice to minimize risk with all forms of malware
- Clicking on unknown links can cause unauthorized software to download onto your device, particularly if you don't have automatic updates enabled

Microsoft’s Update Service

- Through Microsoft’s update service, Microsoft “pushes” security updates and enhancements that can help reduce the risk of ransomware and other forms of malware
- Configuring your device for **automatic update** is strongly recommended to reduce the risk of ransomware and other forms of malware
- When the WannaCry ransomware outbreak occurred in 2017, the devices impacted were those that **had not installed a previous Microsoft update**

Keep your devices patched!!!

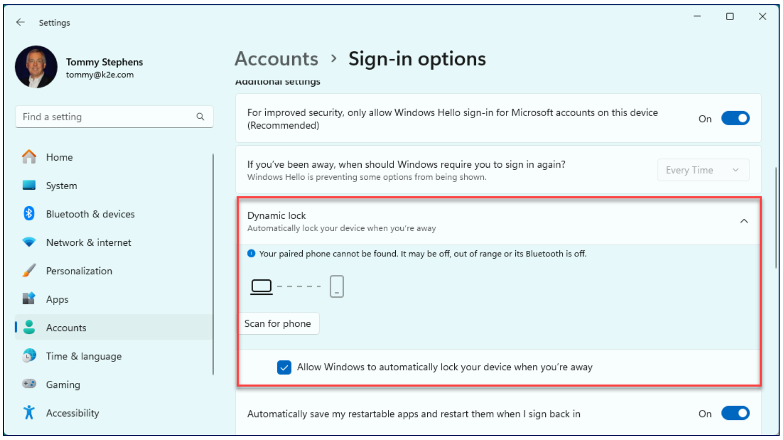
OTHER WINDOWS SECURITY FEATURES

Dynamic Lock

- Dynamic Lock is a Windows feature that helps to minimize the risk of unauthorized access to your device
- With Dynamic Lock enabled, when you walk away from your desk, your computer automatically locks, preventing others from accessing your device or the data on it
- Dynamic Lock requires you to pair a Bluetooth device, such as your smartphone, to your computer…then, if you leave your desk with your Bluetooth device in tow, your computer locks automatically reducing data security risks

Dynamic Lock

- To use Dynamic Lock, you must enable Bluetooth on your device
- Upon doing so, and enabling the feature, your computer locks whenever your device is no longer paired



Accounts › Sign-in options

Additional settings

For improved security, only allow Windows Hello sign-in for Microsoft accounts on this device (Recommended) On

If you've been away, when should Windows require you to sign in again? Every Time
Windows Hello is preventing some options from being shown.

Dynamic lock
Automatically lock your device when you're away

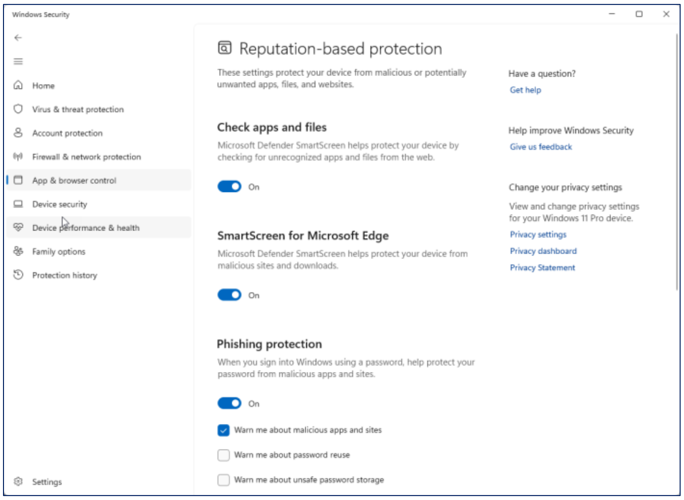
Your paired phone cannot be found. It may be off, out of range or its Bluetooth is off.

Scan for phone

☑ Allow Windows to automatically lock your device when you're away

Automatically save my restartable apps and restart them when I sign back in On

Enable Reputation-Based Protection



Reputation-based protection

These settings protect your device from malicious or potentially unwanted apps, files, and websites.

Check apps and files

Microsoft Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.

On

SmartScreen for Microsoft Edge

Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.

On

Phishing protection

When you sign into Windows using a password, help protect your password from malicious apps and sites.

On

☑ Warn me about malicious apps and sites

□ Warn me about password reuse

□ Warn me about unsafe password storage

Change your privacy settings

View and change privacy settings for your Windows 11 Pro device.

- Reputation-based protection checks the apps/files/websites you attempt to use and lets you know if there are reputational concerns about the app/file/website

Smart App Control

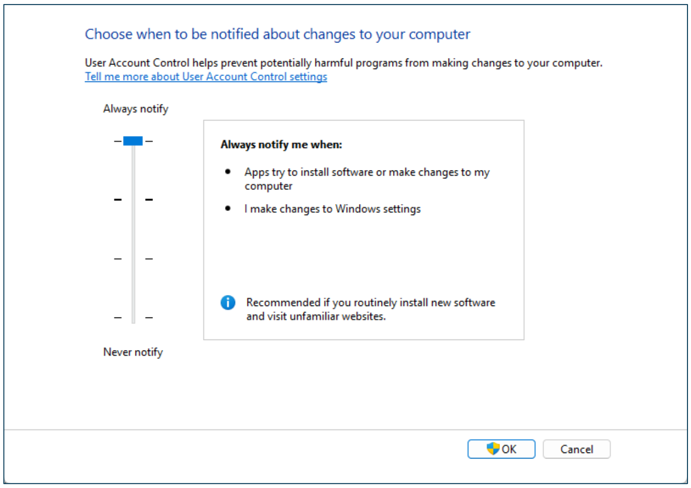
- Smart App Control (SAC) is a feature that is presently available only on “clean” installations of Windows 11
- If you enable SAC, whenever you launch an app, it checks to see if its’ Cloud-based service can confidently predict that the app is safe for use
  - It SAC deems the app “safe,” it provides permission to use the app
  - Otherwise, it blocks the app
- Notably, end-users cannot bypass or override a “block” that SAC invokes on a given app

User Account Control (UAC)

- User Account Control (UAC) is a Windows feature designed to prevent accidental or unauthorized changes to a device
- When UAC is active, only users with administrative rights can make certain changes to the device, such as installing software
- To complete a “blocked” action, a user must elevate their rights by entering their Admin password
  - Of course, if they don’t have an Admin password, UAC blocks them from performing the task or action they were attempting to complete

User Account Control

- You can configure UAC to notify you of any change that you’re making to your device that could be potentially harmful or malicious
- The setting shown is the most secure option available with UAC



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify

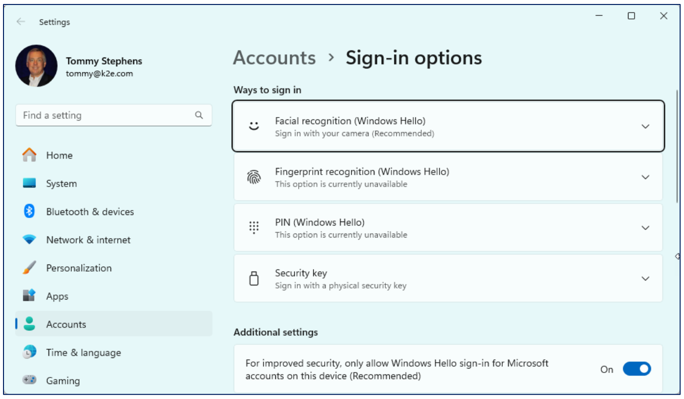
Always notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Never notify

User Authentication



Accounts › Sign-in options

Ways to sign in

Facial recognition (Windows Hello)
Sign in with your camera (Recommended)

Fingerprint recognition (Windows Hello)
This option is currently unavailable

PIN (Windows Hello)
This option is currently unavailable

Security key
Sign in with a physical security key

Additional settings

For improved security, only allow Windows Hello sign-in for Microsoft accounts on this device (Recommended) — On

- Windows 11 continues to support signing in with a Microsoft or local account password
- However, the Windows Hello feature allows you to use biometric authentication for a faster and more secure sign-in

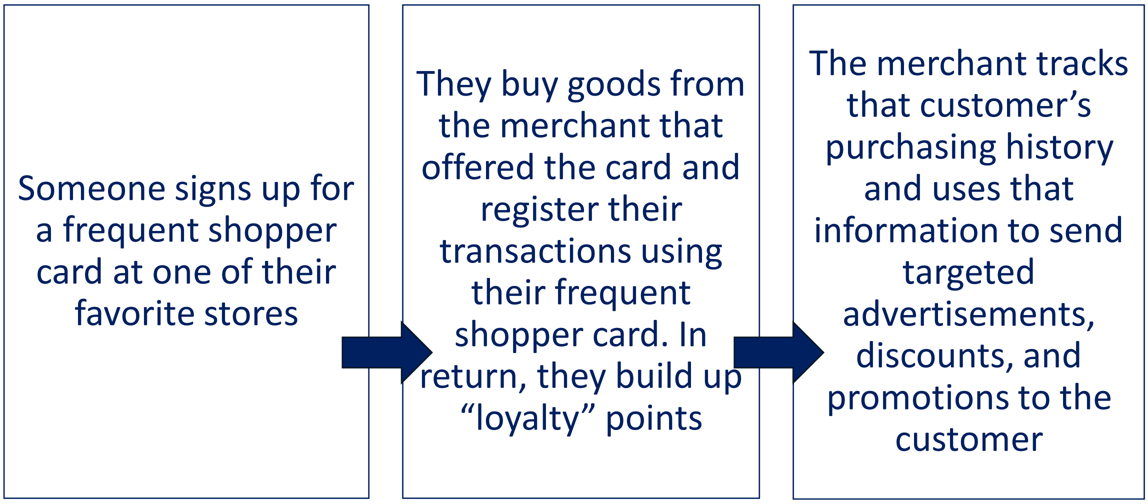
Switching Gears…

PRIVACY ISSUES AND CONCERNS

What Is Data Privacy, Really?

- "Privacy" addresses the rights of individuals to control who has access to personal data about them and how that data is used
- For example, when someone signs up for a "frequent shopper card," how much data is collected about that person, how long will that data remain in the possession of the collector, what will the collector do with the data, and can the collector sell or share the data with others
- In addition, will the collector abide by relevant laws and regulations in the appropriate jurisdictions?

An Example…



Someone signs up for a frequent shopper card at one of their favorite stores

They buy goods from the merchant that offered the card and register their transactions using their frequent shopper card. In return, they build up "loyalty" points

The merchant tracks that customer's purchasing history and uses that information to send targeted advertisements, discounts, and promotions to the customer

IN THE PREVIOUS EXAMPLE, IS THE MERCHANT ACTING *RESPONSIBLY* AND *LEGALLY*? THE ANSWER IS "IT DEPENDS"

In The Previous Example…

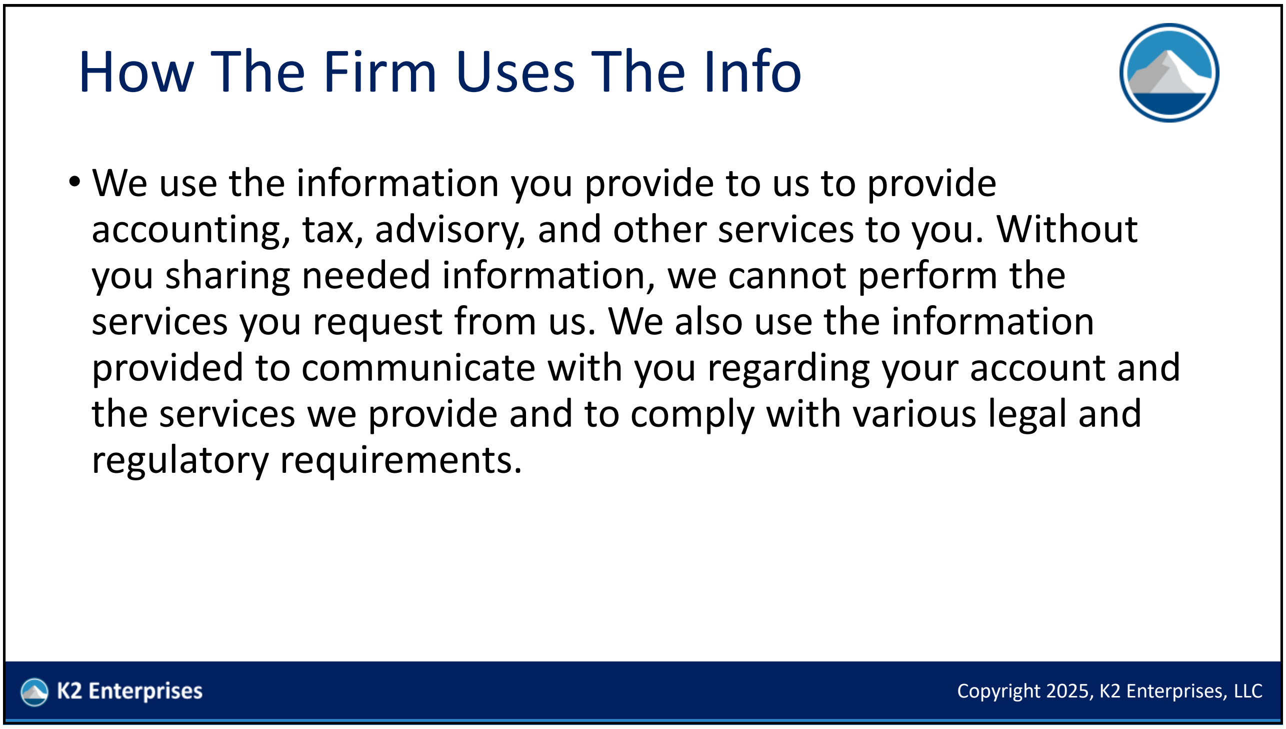
- Is there an expectation of privacy?
- Is there any law controlling how much data could be collected and how long it could be retained?
- Is there any limitation on how the data could be used?
- Is there any law or regulation controlling transferring the data to a third party?

Six Common Elements Of A Privacy Policy

- The nature and type of the information to be collected
- How the collector will use the information
- Information sharing and disclosure to third parties
- An overview of data security measures that are in place
- The consumer’s rights, including access to information, request/demand for correction of errors, and deletion once the transaction cycle is complete
- Suppose the company is a CPA firm…following is sample text that **might** be found in the firm’s Privacy Policy

Information To Be Collected

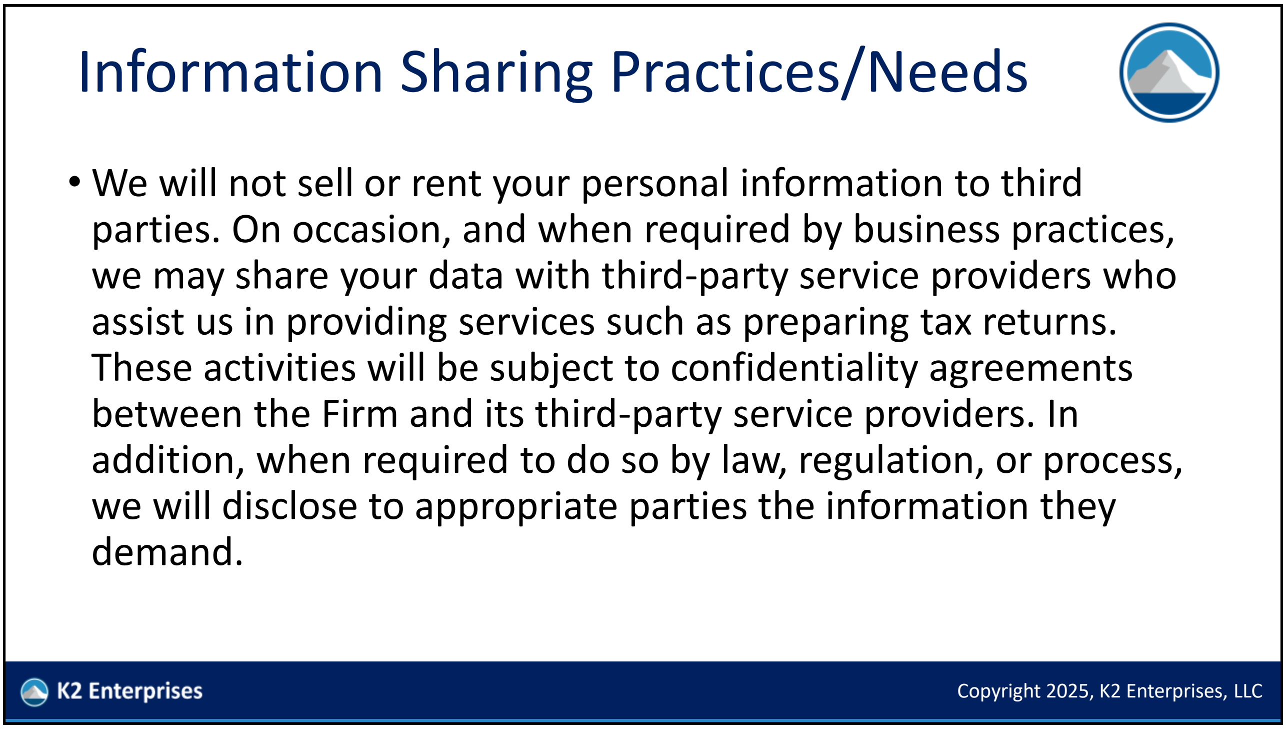
- We will collect various elements of personal information about you with the services you request. Included in the collected information are the following items:
  - Name, physical address, email address, phone number, Social Security Number, and other information, such as a driver’s license number
  - Bank account details, including account number, tax information, and other financial records as necessary to complete the services you request from us
  - Employment information, such as the name of your employer, your occupation, and other relevant details



How The Firm Uses The Info

- We use the information you provide to us to provide accounting, tax, advisory, and other services to you. Without you sharing needed information, we cannot perform the services you request from us. We also use the information provided to communicate with you regarding your account and the services we provide and to comply with various legal and regulatory requirements.

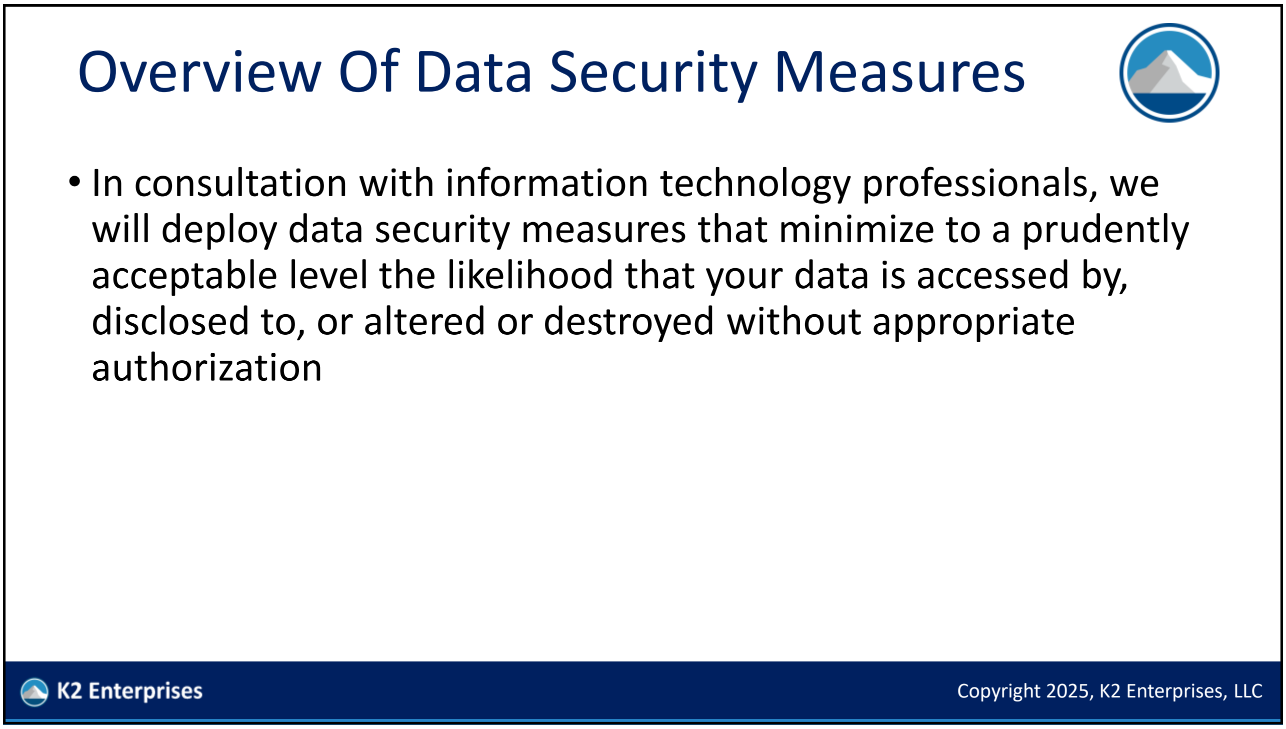
K2 Enterprises



Information Sharing Practices/Needs

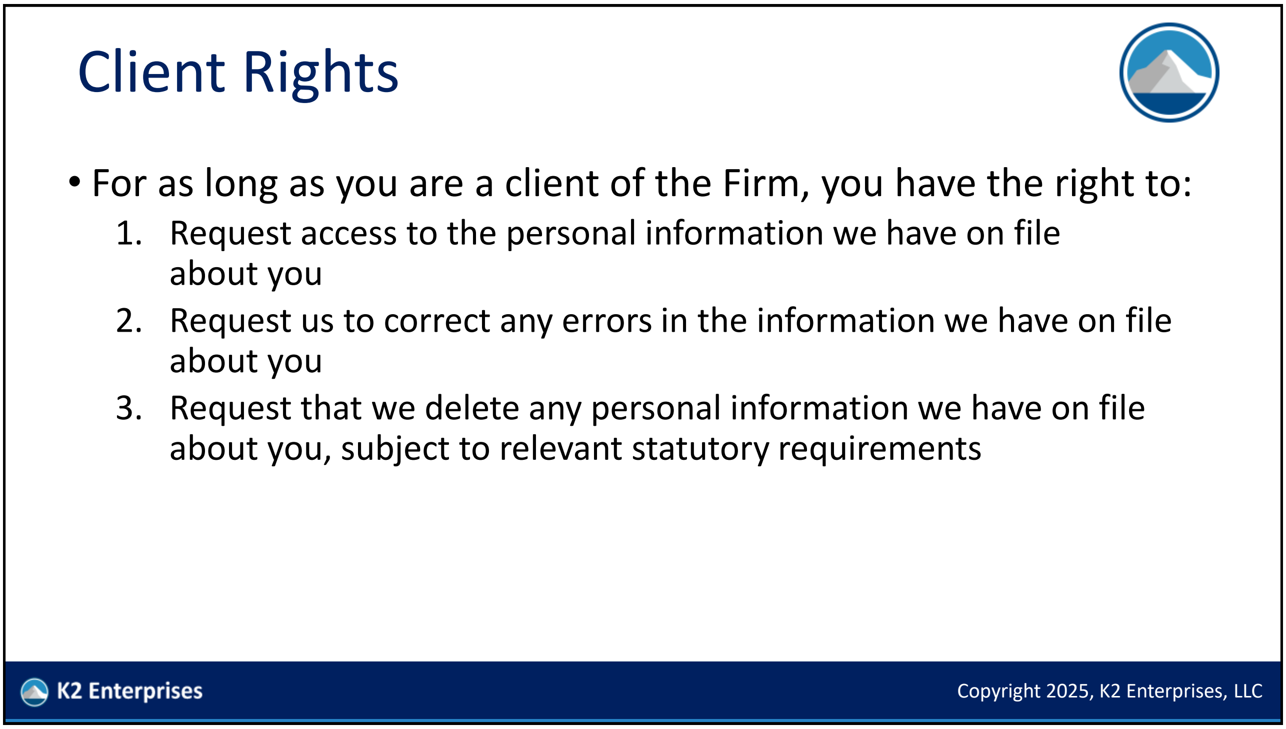
- We will not sell or rent your personal information to third parties. On occasion, and when required by business practices, we may share your data with third-party service providers who assist us in providing services such as preparing tax returns. These activities will be subject to confidentiality agreements between the Firm and its third-party service providers. In addition, when required to do so by law, regulation, or process, we will disclose to appropriate parties the information they demand.

K2 Enterprises



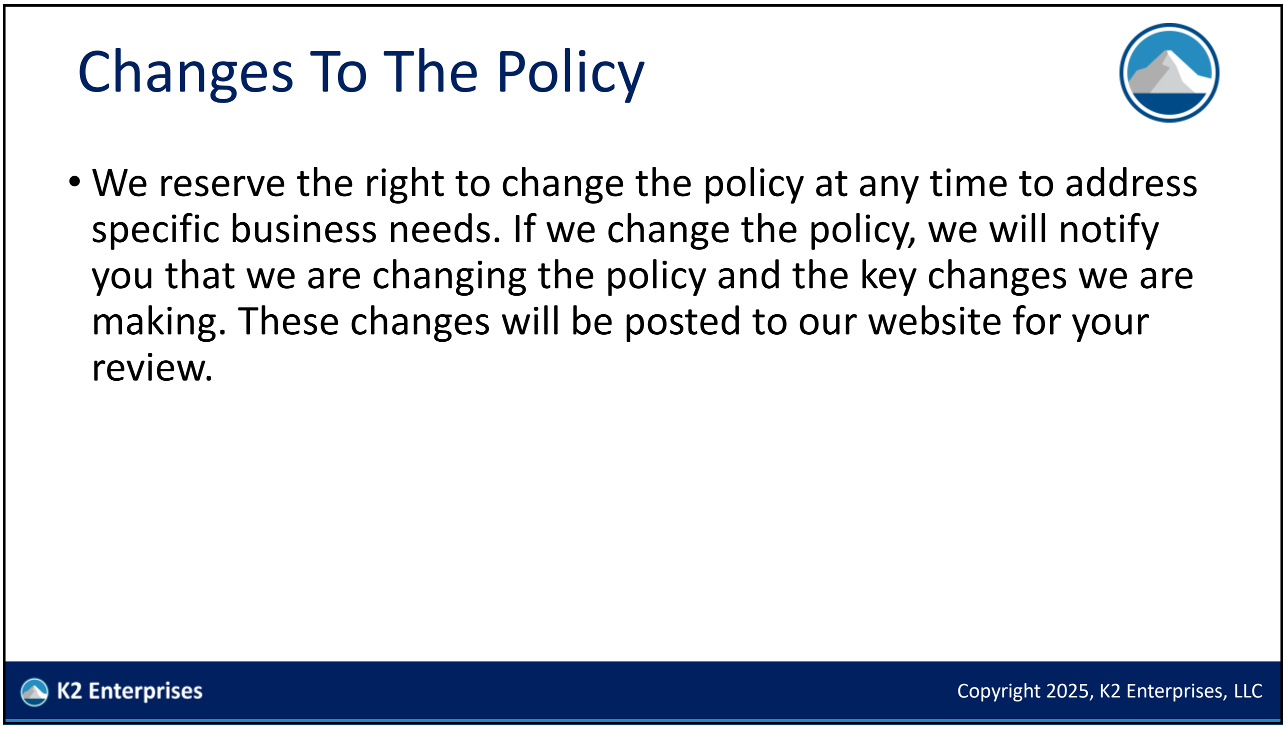
Overview Of Data Security Measures

- In consultation with information technology professionals, we will deploy data security measures that minimize to a prudently acceptable level the likelihood that your data is accessed by, disclosed to, or altered or destroyed without appropriate authorization



Client Rights

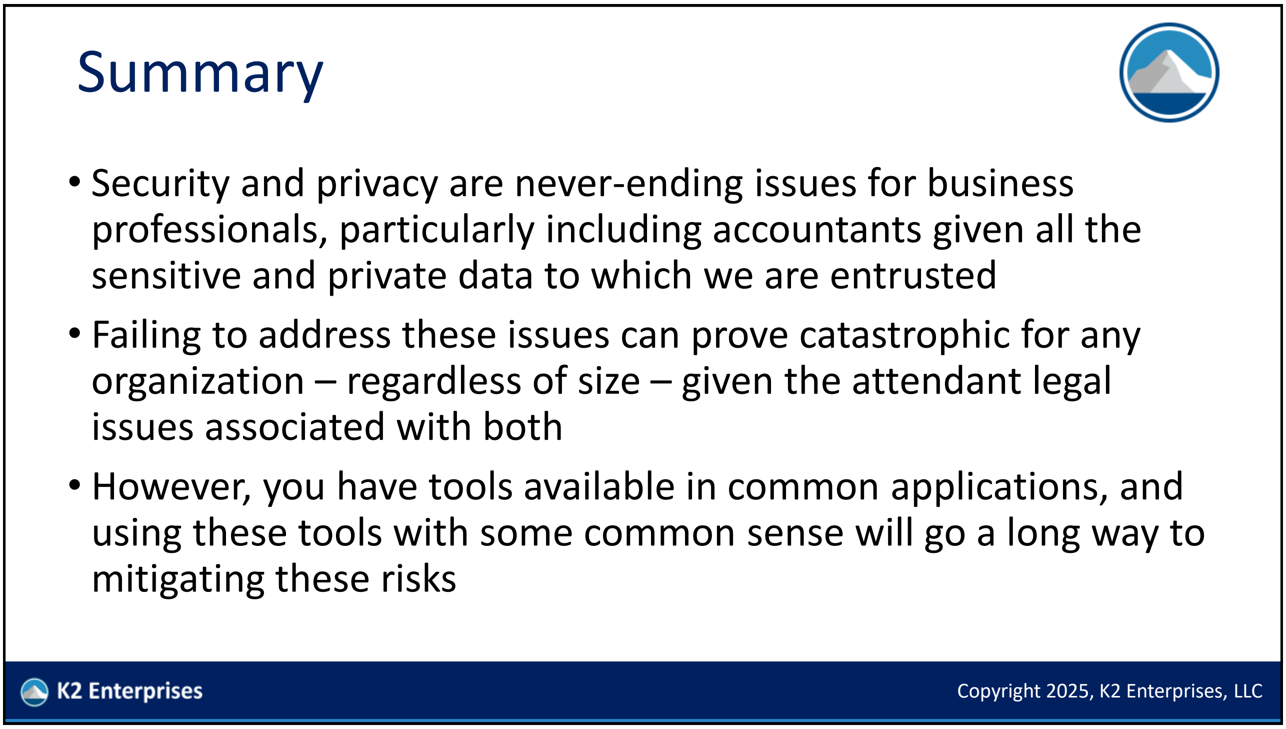
- For as long as you are a client of the Firm, you have the right to:
  1. Request access to the personal information we have on file about you
  2. Request us to correct any errors in the information we have on file about you
  3. Request that we delete any personal information we have on file about you, subject to relevant statutory requirements



Changes To The Policy

- We reserve the right to change the policy at any time to address specific business needs. If we change the policy, we will notify you that we are changing the policy and the key changes we are making. These changes will be posted to our website for your review.

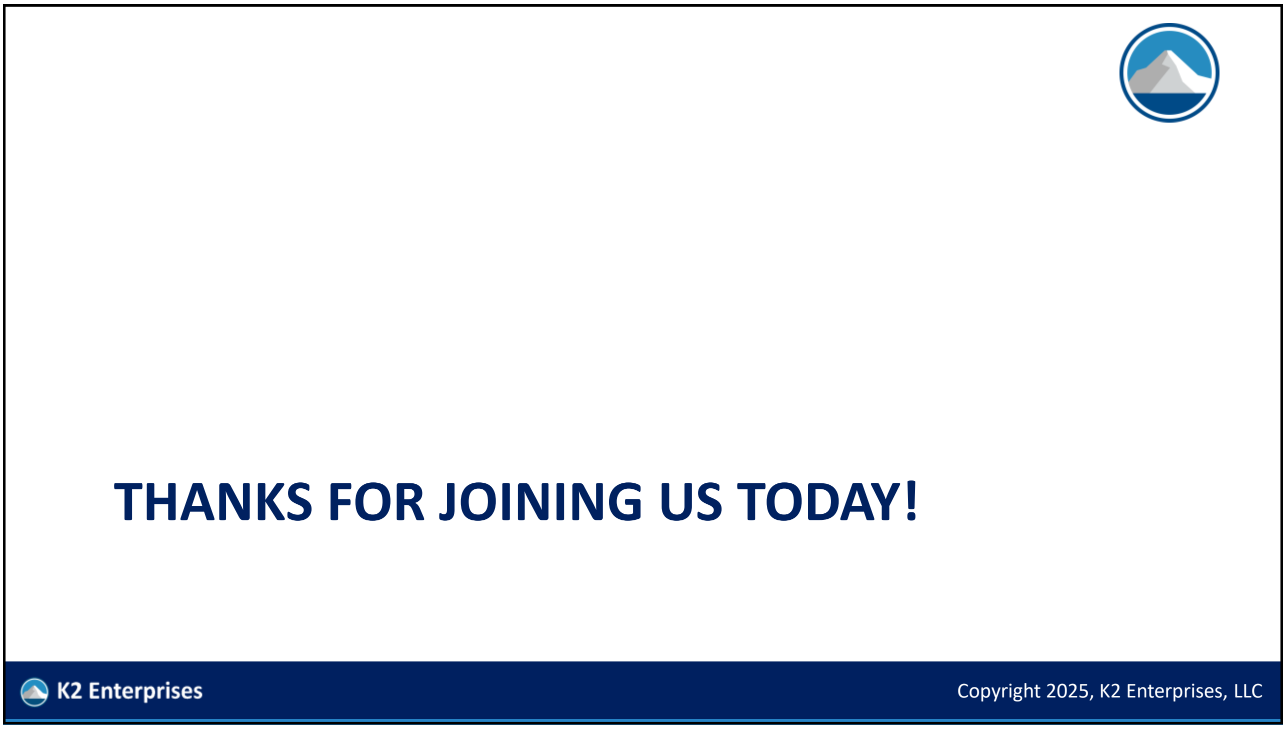
K2 Enterprises



Summary

- Security and privacy are never-ending issues for business professionals, particularly including accountants given all the sensitive and private data to which we are entrusted
- Failing to address these issues can prove catastrophic for any organization – regardless of size – given the attendant legal issues associated with both
- However, you have tools available in common applications, and using these tools with some common sense will go a long way to mitigating these risks

K2 Enterprises



THANKS FOR JOINING US TODAY!

K2 Enterprises