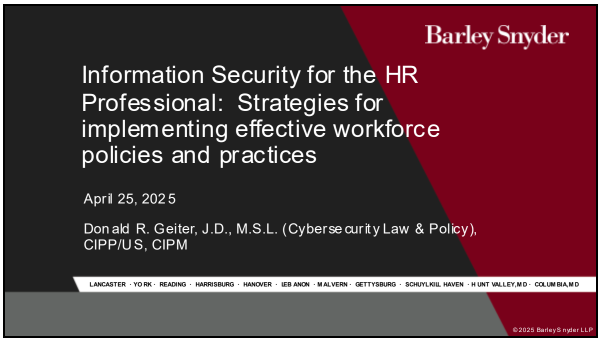


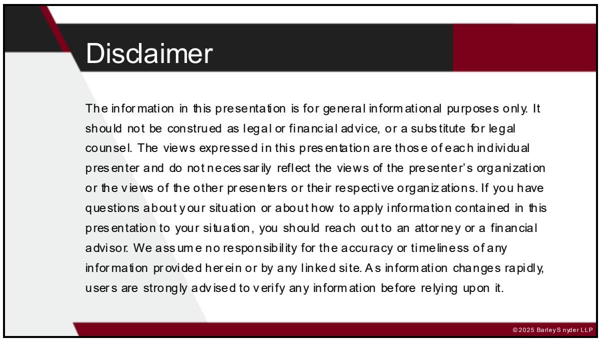
Barley Snyder

Information Security for the HR Professional: Strategies for implementing effective workforce policies and practices

April 25, 2025

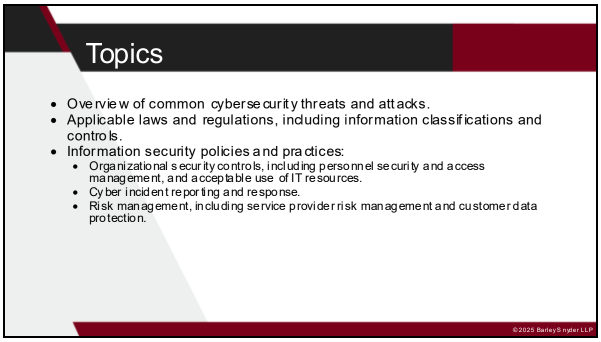
Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

LANCASTER · YORK · READING · HARRISBURG · HANOVER · LEBANON · MALVERN · GETTYSBURG · SCHUYLKILL HAVEN · HUNT VALLEY,MD · COLUMBIA,MD



Disclaimer

The information in this presentation is for general informational purposes only. It should not be construed as legal or financial advice, or a substitute for legal counsel. The views expressed in this presentation are those of each individual presenter and do not necessarily reflect the views of the presenter's organization or the views of the other presenters or their respective organizations. If you have questions about your situation or about how to apply information contained in this presentation to your situation, you should reach out to an attorney or a financial advisor. We assume no responsibility for the accuracy or timeliness of any information provided herein or by any linked site. As information changes rapidly, users are strongly advised to verify any information before relying upon it.



Topics

- Overview of common cybersecurity threats and attacks.
- Applicable laws and regulations, including information classifications and controls.
- Information security policies and practices:
  - Organizational security controls, including personnel security and access management, and acceptable use of IT resources.
  - Cyber incident reporting and response.
  - Risk management, including service provider risk management and customer data protection.

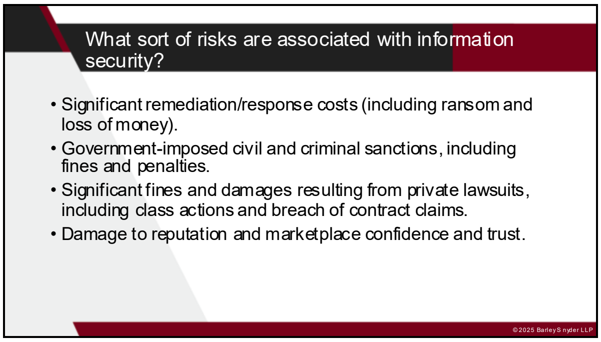
Common Cybersecurity Threats and Attacks

Let's understand the current threat landscape…

- Ransomware
- Theft of money – including BEC
- Phishing Attack
- Data Breach
- Denial of Service Attack
- Lost or Stolen Device/Files
- Disclosure of Private Information
- Hacking
- Malware
- Vendor Error or Negligence
- Physical Security Breach
- Artificial Intelligence
- The Unknown…

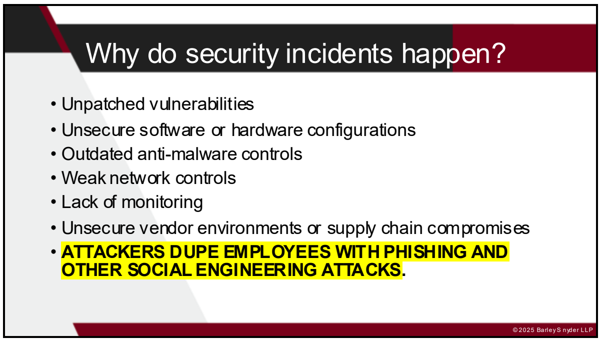
Cyber Crime

It is estimated more than 50 billion devices and processes are now connected to the internet
Cybercrime is projected to cost the world $10.5 trillion annually in 2025 *(Cybercrime Magazine)*



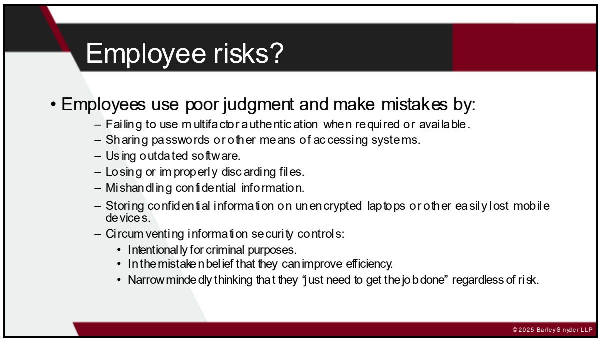
What sort of risks are associated with information security?

- Significant remediation/response costs (including ransom and loss of money).
- Government-imposed civil and criminal sanctions, including fines and penalties.
- Significant fines and damages resulting from private lawsuits, including class actions and breach of contract claims.
- Damage to reputation and marketplace confidence and trust.



Why do security incidents happen?

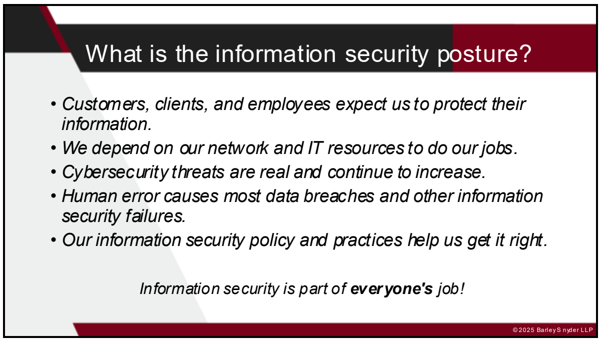
- Unpatched vulnerabilities
- Unsecure software or hardware configurations
- Outdated anti-malware controls
- Weak network controls
- Lack of monitoring
- Unsecure vendor environments or supply chain compromises
- **ATTACKERS DUPE EMPLOYEES WITH PHISHING AND OTHER SOCIAL ENGINEERING ATTACKS.**



Employee risks?

- Employees use poor judgment and make mistakes by:
  - Failing to use multifactor authentication when required or available.
  - Sharing passwords or other means of accessing systems.
  - Using outdated software.
  - Losing or improperly discarding files.
  - Mishandling confidential information.
  - Storing confidential information on unencrypted laptops or other easily lost mobile devices.
  - Circumventing information security controls:
    - Intentionally for criminal purposes.
    - In the mistaken belief that they can improve efficiency.
    - Narrow mindedly thinking that they 'just need to get the job done" regardless of risk.

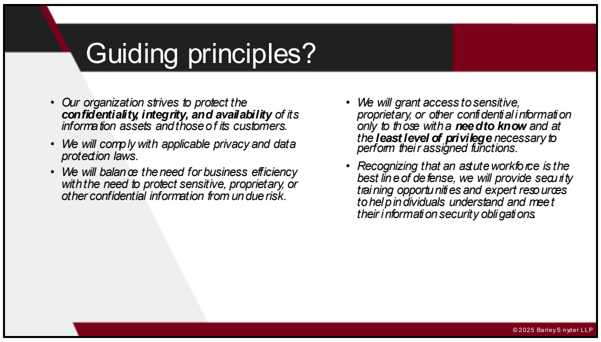
Information Security



What is the information security posture?

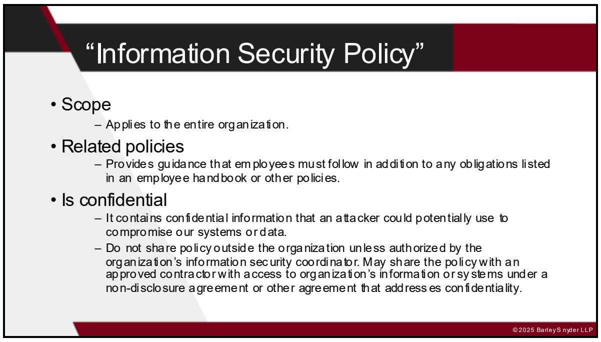
- *Customers, clients, and employees expect us to protect their information.*
- *We depend on our network and IT resources to do our jobs.*
- *Cybersecurity threats are real and continue to increase.*
- *Human error causes most data breaches and other information security failures.*
- *Our information security policy and practices help us get it right.*

Information security is part of ***everyone's*** *job!*



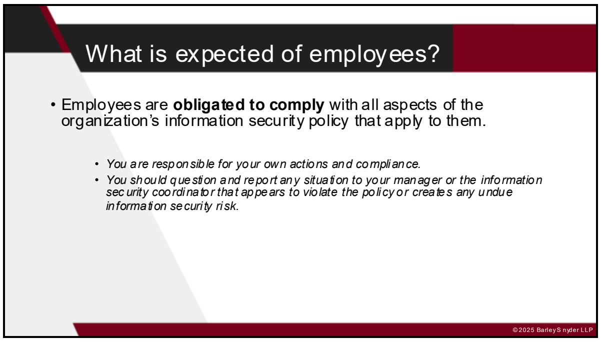
Guiding principles?

- *Our organization strives to protect the* ***confidentiality, integrity, and availability*** *of its information assets and those of its customers.*
- *We will comply with applicable privacy and data protection laws.*
- *We will balance the need for business efficiency with the need to protect sensitive, proprietary, or other confidential information from undue risk.*
- *We will grant access to sensitive, proprietary, or other confidential information only to those with a* ***need to know*** *and at the* ***least level of privilege*** *necessary to perform their assigned functions.*
- *Recognizing that an astute workforce is the best line of defense, we will provide security training opportunities and expert resources to help individuals understand and meet their information security obligations.*



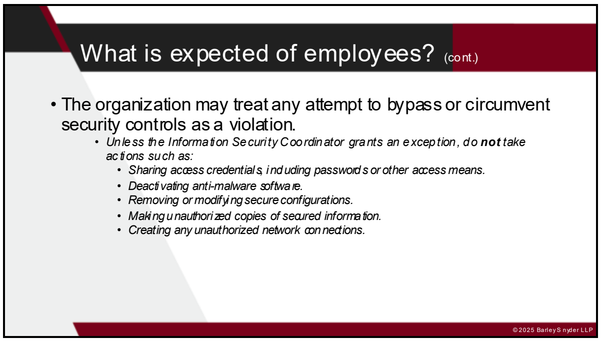
“Information Security Policy”

- Scope
  - Applies to the entire organization.
- Related policies
  - Provides guidance that employees must follow in addition to any obligations listed in an employee handbook or other policies.
- Is confidential
  - It contains confidential information that an attacker could potentially use to compromise our systems or data.
  - Do not share policy outside the organization unless authorized by the organization’s information security coordinator. May share the policy with an approved contractor with access to organization’s information or systems under a non-disclosure agreement or other agreement that addresses confidentiality.



What is expected of employees?

- Employees are **obligated to comply** with all aspects of the organization’s information security policy that apply to them.
  - *You are responsible for your own actions and compliance.*
  - *You should question and report any situation to your manager or the information security coordinator that appears to violate the policy or creates any undue information security risk.*



What is expected of employees? (cont.)

- The organization may treat any attempt to bypass or circumvent security controls as a violation.
  - *Unless the Information Security Coordinator grants an exception, do **not** take actions such as:*
    - *Sharing access credentials, including passwords or other access means.*
    - *Deactivating anti-malware software.*
    - *Removing or modifying secure configurations.*
    - *Making unauthorized copies of secured information.*
    - *Creating any unauthorized network connections.*

Applicable Laws and Regulations

Applicable laws and regulations

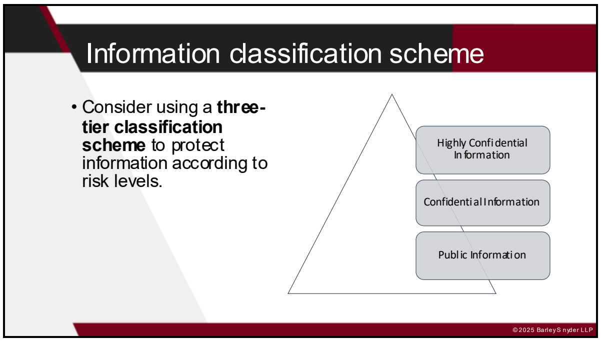
- Body of law is not systematic.
- State laws (generally applicable); Federal Laws (industry and activity specific); international law (i.e., GDPR)
- It is implemented through criminal prosecutions, regulatory enforcement actions, executive orders, contracts, and civil litigation between private parties. It includes both federal and state elements.
- The result is a patchwork—worse, a crazy quilt, with substantial gaps, showing signs of wear even as it is being stitched together.

FTC Safeguards Rule

- Who is in charge and who do they report to?
- Data audit/risk assessment?
- What safeguards are in place (mix of tech and people)?
- Are safeguards being monitored and tested?
- Is staff being trained?
- How are vendors being managed?
- Is program updated and current?
- What are your written policies?

Source: https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Information Classification and Controls



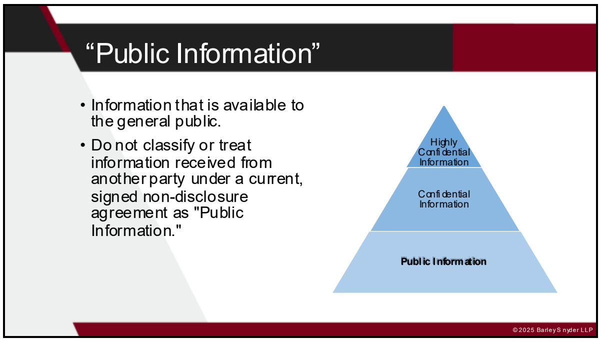
Information classification scheme

- Consider using a **three-tier classification scheme** to protect information according to risk levels.

Highly Confidential Information

Confidential Information

Public Information



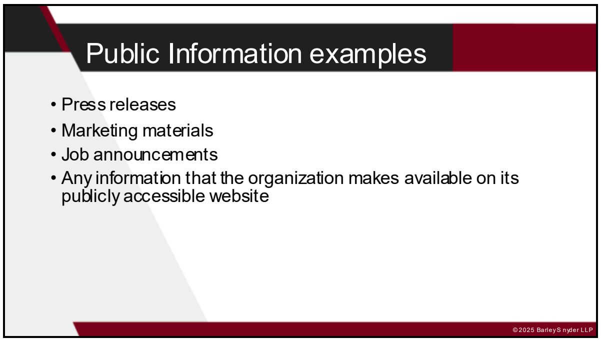
“Public Information”

- Information that is available to the general public.
- Do not classify or treat information received from another party under a current, signed non-disclosure agreement as "Public Information."

Highly Confidential Information

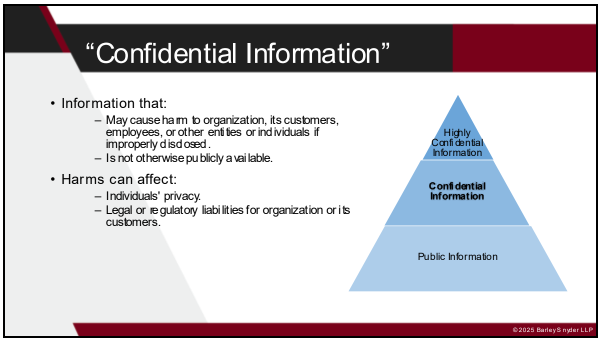
Confidential Information

Public Information



Public Information examples

- Press releases
- Marketing materials
- Job announcements
- Any information that the organization makes available on its publicly accessible website



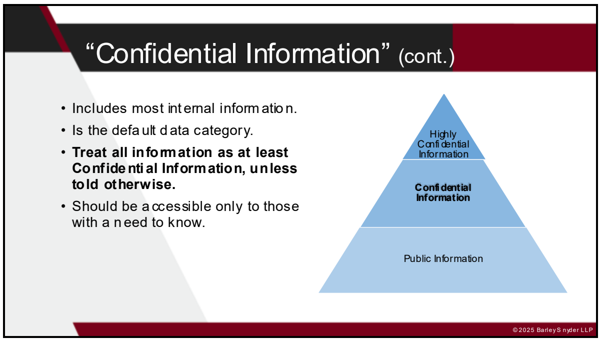
"Confidential Information"

- Information that:
  - May cause harm to organization, its customers, employees, or other entities or individuals if improperly disclosed.
  - Is not otherwise publicly available.
- Harms can affect:
  - Individuals' privacy.
  - Legal or regulatory liabilities for organization or its customers.

Highly Confidential Information

Confidential Information

Public Information



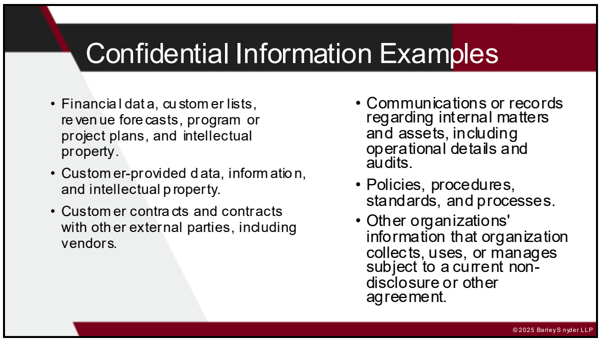
"Confidential Information" (cont.)

- Includes most internal information.
- Is the default data category.
- **Treat all information as at least Confidential Information, unless told otherwise.**
- Should be accessible only to those with a need to know.

Highly Confidential Information

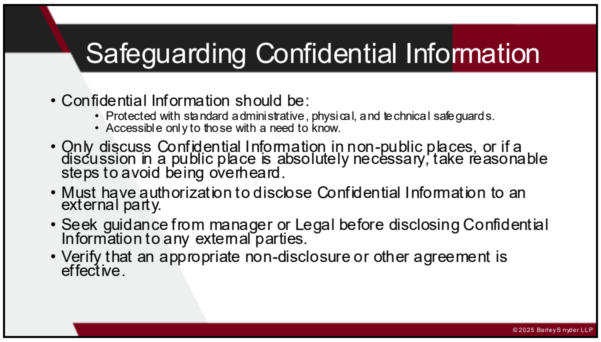
Confidential Information

Public Information



Confidential Information Examples

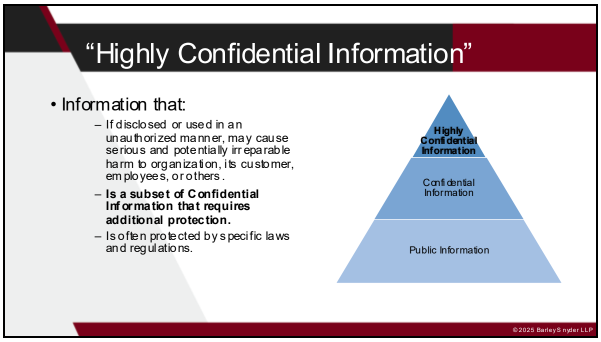
- Financial data, customer lists, revenue forecasts, program or project plans, and intellectual property.
- Customer-provided data, information, and intellectual property.
- Customer contracts and contracts with other external parties, including vendors.
- Communications or records regarding internal matters and assets, including operational details and audits.
- Policies, procedures, standards, and processes.
- Other organizations' information that organization collects, uses, or manages subject to a current non-disclosure or other agreement.



Safeguarding Confidential Information

- Confidential Information should be:
  - Protected with standard administrative, physical, and technical safeguards.
  - Accessible only to those with a need to know.
- Only discuss Confidential Information in non-public places, or if a discussion in a public place is absolutely necessary, take reasonable steps to avoid being overheard.
- Must have authorization to disclose Confidential Information to an external party.
- Seek guidance from manager or Legal before disclosing Confidential Information to any external parties.
- Verify that an appropriate non-disclosure or other agreement is effective.

©2025 BarleySnyder LLP

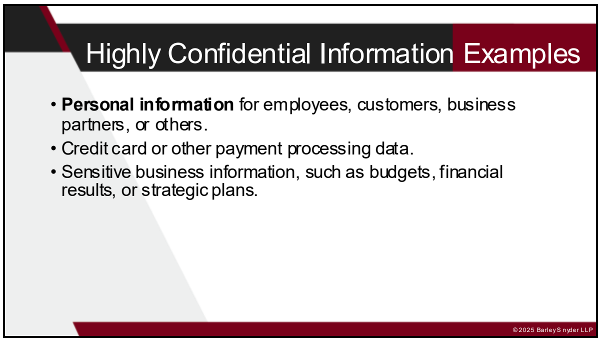


“Highly Confidential Information”

- Information that:
  - If disclosed or used in an unauthorized manner, may cause serious and potentially irreparable harm to organization, its customer, employees, or others.
  - **Is a subset of Confidential Information that requires additional protection.**
  - Is often protected by specific laws and regulations.

Highly Confidential Information
Confidential Information
Public Information

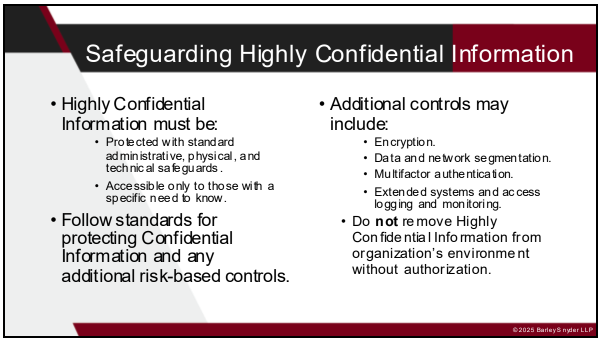
©2025 BarleySnyder LLP



Highly Confidential Information Examples

- **Personal information** for employees, customers, business partners, or others.
- Credit card or other payment processing data.
- Sensitive business information, such as budgets, financial results, or strategic plans.

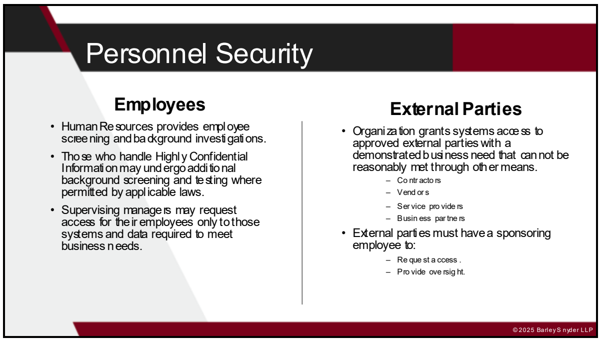
©2025 BarleySnyder LLP



Safeguarding Highly Confidential Information

- Highly Confidential Information must be:
  - Protected with standard administrative, physical, and technical safeguards.
  - Accessible only to those with a specific need to know.
- Follow standards for protecting Confidential Information and any additional risk-based controls.
- Additional controls may include:
  - Encryption.
  - Data and network segmentation.
  - Multifactor authentication.
  - Extended systems and access logging and monitoring.
  - Do **not** remove Highly Confidential Information from organization's environment without authorization.

Personnel Security and Access Management



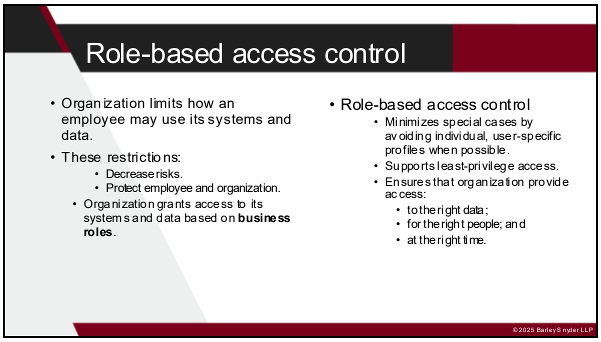
Personnel Security

Employees

- Human Resources provides employee screening and background investigations.
- Those who handle Highly Confidential Information may undergo additional background screening and testing where permitted by applicable laws.
- Supervising managers may request access for their employees only to those systems and data required to meet business needs.

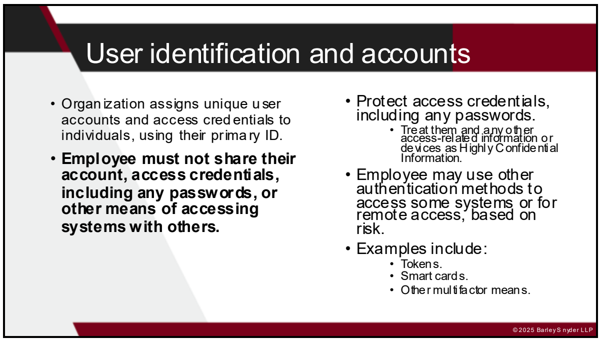
External Parties

- Organization grants systems access to approved external parties with a demonstrated business need that cannot be reasonably met through other means.
  - Contractors
  - Vendors
  - Service providers
  - Business partners
- External parties must have a sponsoring employee to:
  - Request access.
  - Provide oversight.



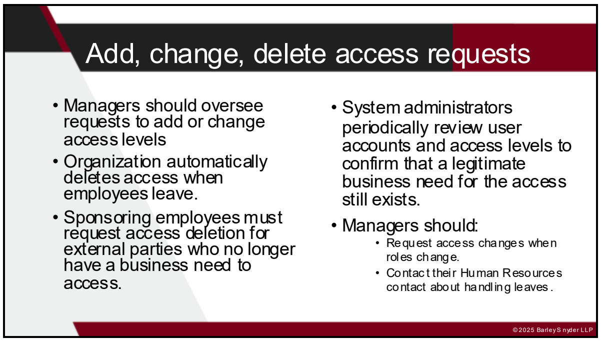
Role-based access control

- Organization limits how an employee may use its systems and data.
- These restrictions:
  - Decrease risks.
  - Protect employee and organization.
  - Organization grants access to its systems and data based on **business roles**.
- Role-based access control
  - Minimizes special cases by avoiding individual, user-specific profiles when possible.
  - Supports least-privilege access.
  - Ensures that organization provide access:
    - to the right data;
    - for the right people; and
    - at the right time.



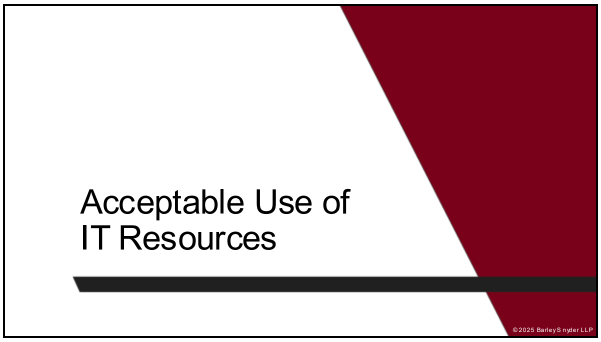
User identification and accounts

- Organization assigns unique user accounts and access credentials to individuals, using their primary ID.
- **Employee must not share their account, access credentials, including any passwords, or other means of accessing systems with others.**
- Protect access credentials, including any passwords.
  - Treat them and any other access-related information or devices as Highly Confidential Information.
- Employee may use other authentication methods to access some systems or for remote access, based on risk.
- Examples include:
  - Tokens.
  - Smart cards.
  - Other multifactor means.

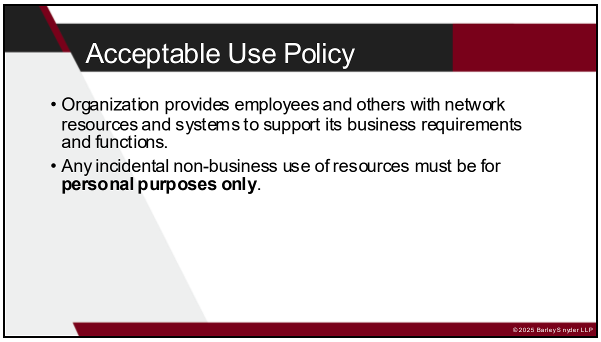


Add, change, delete access requests

- Managers should oversee requests to add or change access levels
- Organization automatically deletes access when employees leave.
- Sponsoring employees must request access deletion for external parties who no longer have a business need to access.
- System administrators periodically review user accounts and access levels to confirm that a legitimate business need for the access still exists.
- Managers should:
  - Request access changes when roles change.
  - Contact their Human Resources contact about handling leaves.

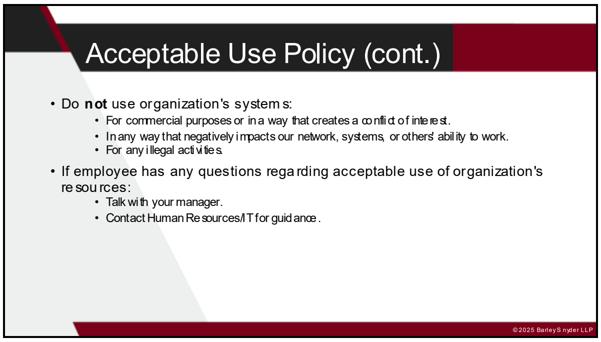


Acceptable Use of IT Resources



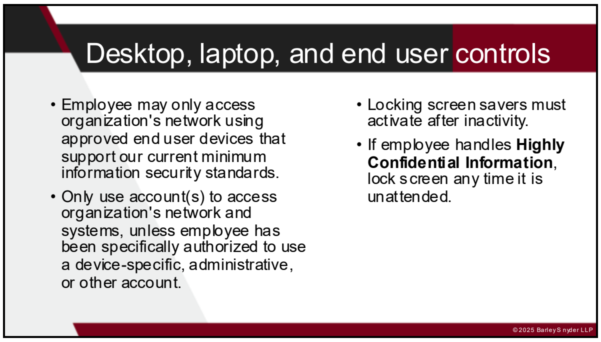
Acceptable Use Policy

- Organization provides employees and others with network resources and systems to support its business requirements and functions.
- Any incidental non-business use of resources must be for **personal purposes only**.



Acceptable Use Policy (cont.)

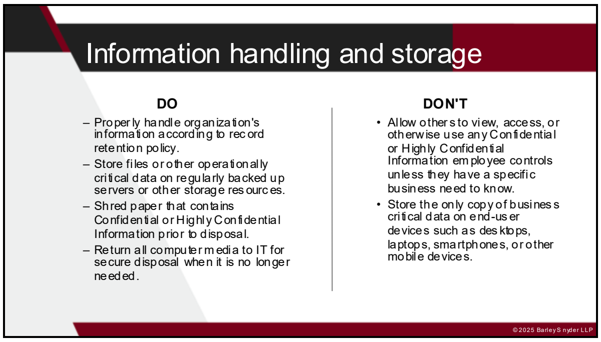
- Do **not** use organization's systems:
  - For commercial purposes or in a way that creates a conflict of interest.
  - In any way that negatively impacts our network, systems, or others' ability to work.
  - For any illegal activities.
- If employee has any questions regarding acceptable use of organization's resources:
  - Talk with your manager.
  - Contact Human Resources/IT for guidance.



Desktop, laptop, and end user controls

- Employee may only access organization's network using approved end user devices that support our current minimum information security standards.
- Only use account(s) to access organization's network and systems, unless employee has been specifically authorized to use a device-specific, administrative, or other account.
- Locking screen savers must activate after inactivity.
- If employee handles **Highly Confidential Information**, lock screen any time it is unattended.

©2025 BarleySnyder LLP



Information handling and storage

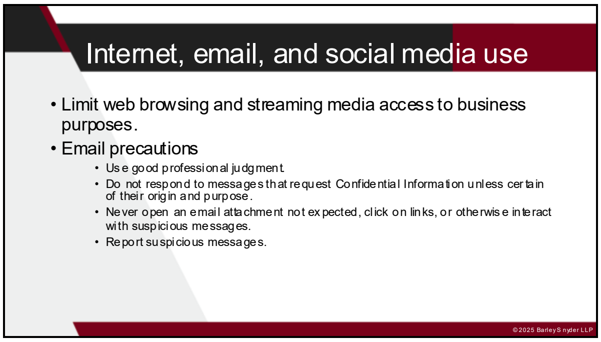
DO

- Properly handle organization's information according to record retention policy.
- Store files or other operationally critical data on regularly backed up servers or other storage resources.
- Shred paper that contains Confidential or Highly Confidential Information prior to disposal.
- Return all computer media to IT for secure disposal when it is no longer needed.

DON'T

- Allow others to view, access, or otherwise use any Confidential or Highly Confidential Information employee controls unless they have a specific business need to know.
- Store the only copy of business critical data on end-user devices such as desktops, laptops, smartphones, or other mobile devices.

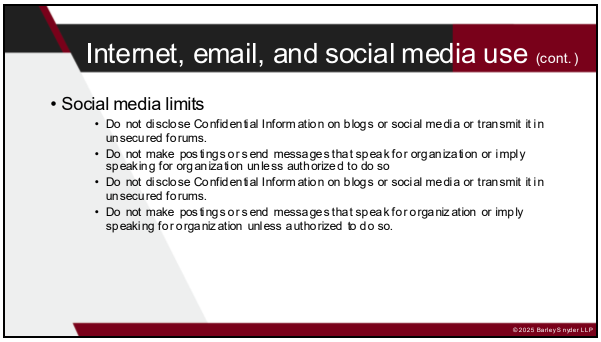
©2025 BarleySnyder LLP



Internet, email, and social media use

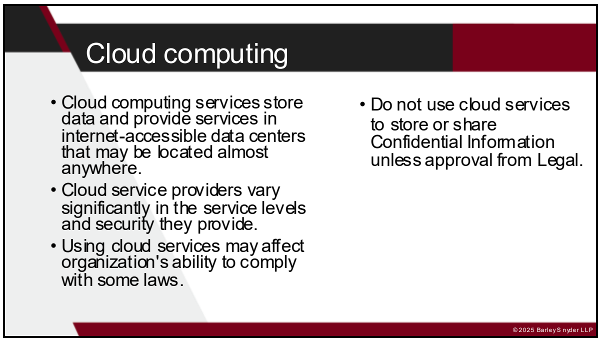
- Limit web browsing and streaming media access to business purposes.
- Email precautions
  - Use good professional judgment.
  - Do not respond to messages that request Confidential Information unless certain of their origin and purpose.
  - Never open an email attachment not expected, click on links, or otherwise interact with suspicious messages.
  - Report suspicious messages.

©2025 BarleySnyder LLP



Internet, email, and social media use (cont.)

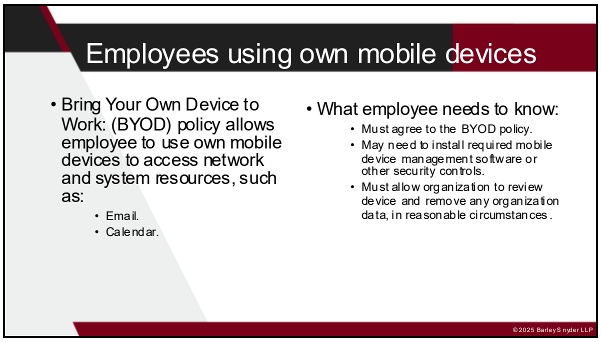
- Social media limits
  - Do not disclose Confidential Information on blogs or social media or transmit it in unsecured forums.
  - Do not make postings or send messages that speak for organization or imply speaking for organization unless authorized to do so
  - Do not disclose Confidential Information on blogs or social media or transmit it in unsecured forums.
  - Do not make postings or send messages that speak for organization or imply speaking for organization unless authorized to do so.



Cloud computing

- Cloud computing services store data and provide services in internet-accessible data centers that may be located almost anywhere.
- Cloud service providers vary significantly in the service levels and security they provide.
- Using cloud services may affect organization's ability to comply with some laws.

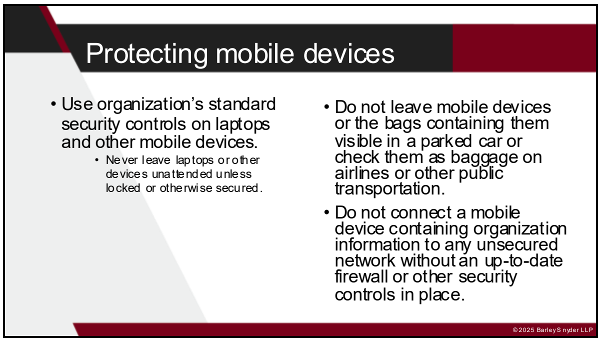
- Do not use cloud services to store or share Confidential Information unless approval from Legal.



Employees using own mobile devices

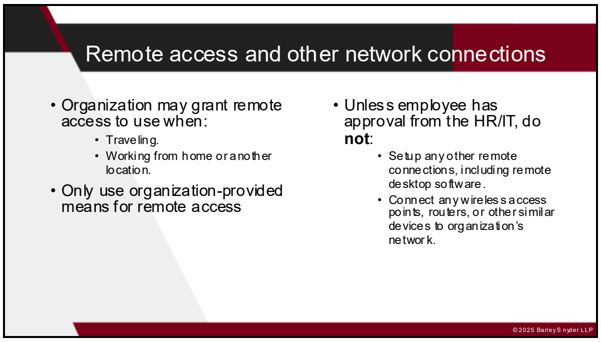
- Bring Your Own Device to Work: (BYOD) policy allows employee to use own mobile devices to access network and system resources, such as:
  - Email.
  - Calendar.

- What employee needs to know:
  - Must agree to the BYOD policy.
  - May need to install required mobile device management software or other security controls.
  - Must allow organization to review device and remove any organization data, in reasonable circumstances.



Protecting mobile devices

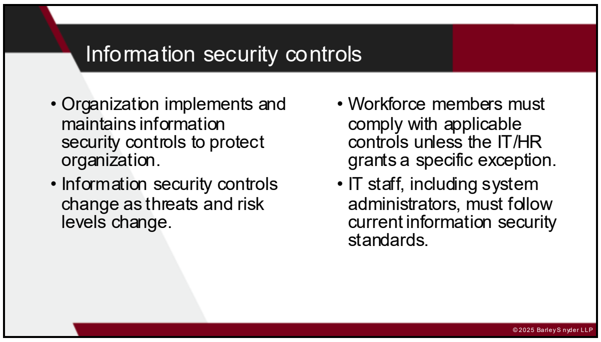
- Use organization's standard security controls on laptops and other mobile devices.
  - Never leave laptops or other devices unattended unless locked or otherwise secured.
- Do not leave mobile devices or the bags containing them visible in a parked car or check them as baggage on airlines or other public transportation.
- Do not connect a mobile device containing organization information to any unsecured network without an up-to-date firewall or other security controls in place.



Remote access and other network connections

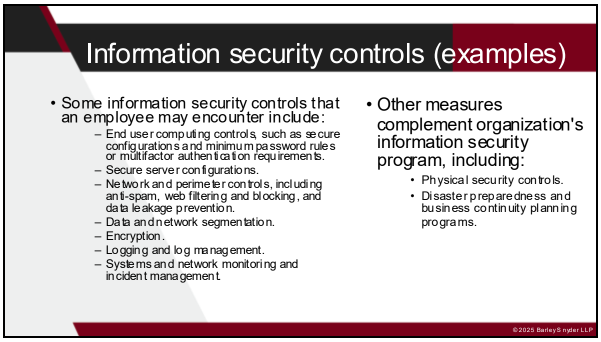
- Organization may grant remote access to use when:
  - Traveling.
  - Working from home or another location.
- Only use organization-provided means for remote access
- Unless employee has approval from the HR/IT, do **not**:
  - Setup any other remote connections, including remote desktop software.
  - Connect any wireless access points, routers, or other similar devices to organization's network.

Information Security Controls



Information security controls

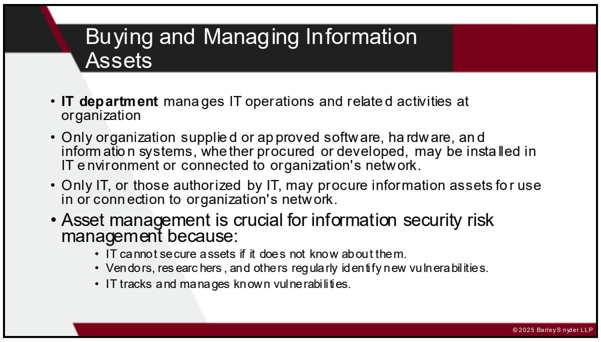
- Organization implements and maintains information security controls to protect organization.
- Information security controls change as threats and risk levels change.
- Workforce members must comply with applicable controls unless the IT/HR grants a specific exception.
- IT staff, including system administrators, must follow current information security standards.



Information security controls (examples)

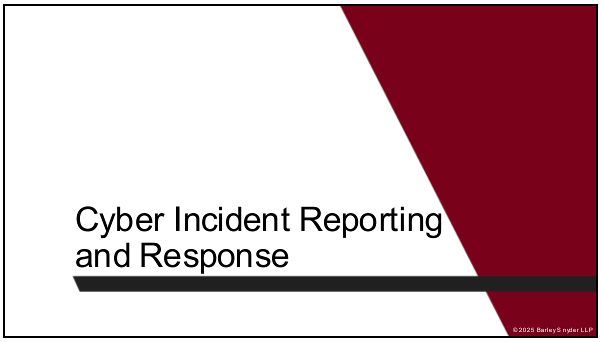
- Some information security controls that an employee may encounter include:
  - End user computing controls, such as secure configurations and minimum password rules or multifactor authentication requirements.
  - Secure server configurations.
  - Network and perimeter controls, including anti-spam, web filtering and blocking, and data leakage prevention.
  - Data and network segmentation.
  - Encryption.
  - Logging and log management.
  - Systems and network monitoring and incident management.
- Other measures complement organization's information security program, including:
  - Physical security controls.
  - Disaster preparedness and business continuity planning programs.

Buying and Managing Information Assets

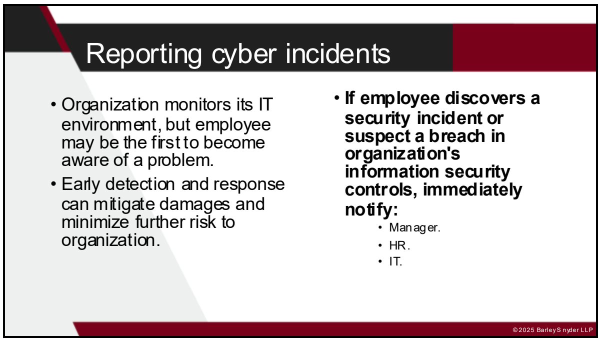


Buying and Managing Information Assets

- **IT department** manages IT operations and related activities at organization
- Only organization supplied or approved software, hardware, and information systems, whether procured or developed, may be installed in IT environment or connected to organization's network.
- Only IT, or those authorized by IT, may procure information assets for use in or connection to organization's network.
- Asset management is crucial for information security risk management because:
  - IT cannot secure assets if it does not know about them.
  - Vendors, researchers, and others regularly identify new vulnerabilities.
  - IT tracks and manages known vulnerabilities.



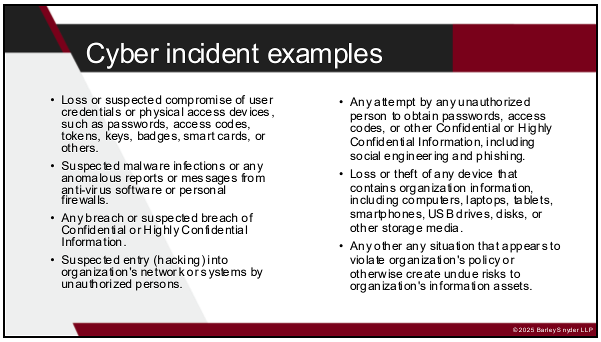
Cyber Incident Reporting and Response



Reporting cyber incidents

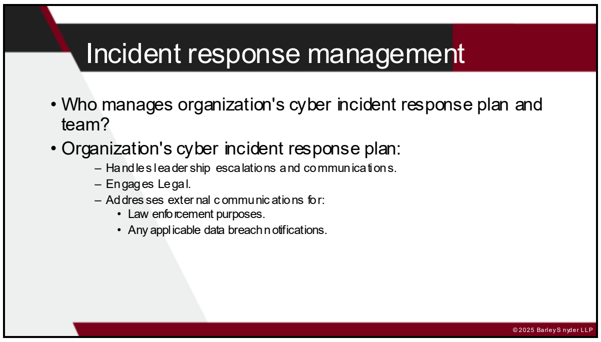
- Organization monitors its IT environment, but employee may be the first to become aware of a problem.
- Early detection and response can mitigate damages and minimize further risk to organization.

- **If employee discovers a security incident or suspect a breach in organization's information security controls, immediately notify:**
  - Manager.
  - HR.
  - IT.



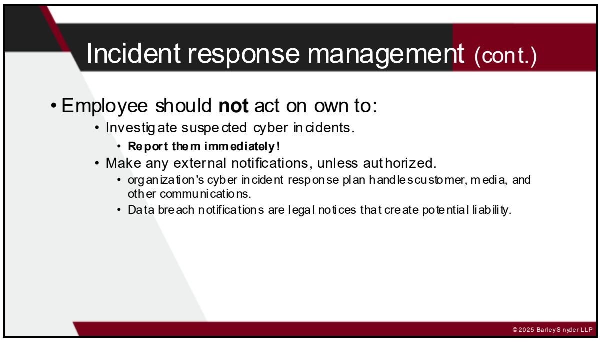
Cyber incident examples

- Loss or suspected compromise of user credentials or physical access devices, such as passwords, access codes, tokens, keys, badges, smart cards, or others.
- Suspected malware infections or any anomalous reports or messages from anti-virus software or personal firewalls.
- Any breach or suspected breach of Confidential or Highly Confidential Information.
- Suspected entry (hacking) into organization's network or systems by unauthorized persons.
- Any attempt by any unauthorized person to obtain passwords, access codes, or other Confidential or Highly Confidential Information, including social engineering and phishing.
- Loss or theft of any device that contains organization information, including computers, laptops, tablets, smartphones, USB drives, disks, or other storage media.
- Any other any situation that appears to violate organization's policy or otherwise create undue risks to organization's information assets.



Incident response management

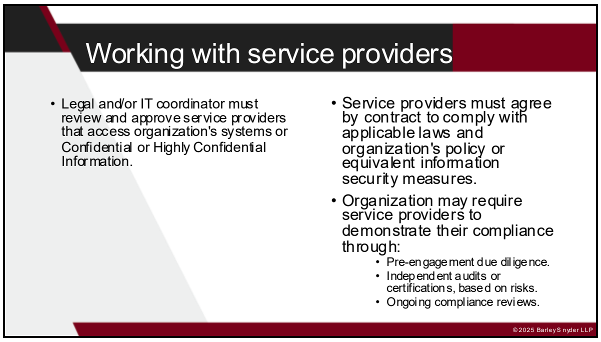
- Who manages organization's cyber incident response plan and team?
- Organization's cyber incident response plan:
  - Handles leadership escalations and communications.
  - Engages Legal.
  - Addresses external communications for:
    - Law enforcement purposes.
    - Any applicable data breach notifications.



Incident response management (cont.)

- Employee should **not** act on own to:
  - Investigate suspected cyber incidents.
    - **Report them immediately!**
  - Make any external notifications, unless authorized.
    - organization's cyber incident response plan handles customer, media, and other communications.
    - Data breach notifications are legal notices that create potential liability.

Service Provider Risk Management

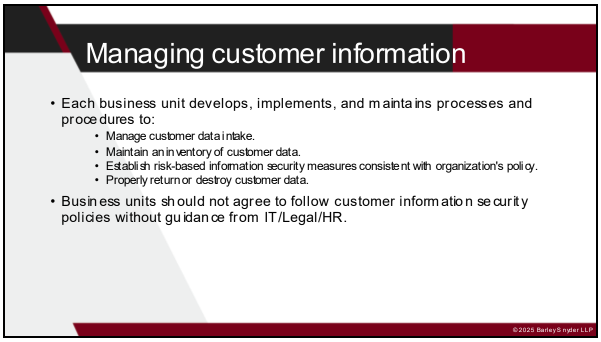


Working with service providers

- Legal and/or IT coordinator must review and approve service providers that access organization's systems or Confidential or Highly Confidential Information.

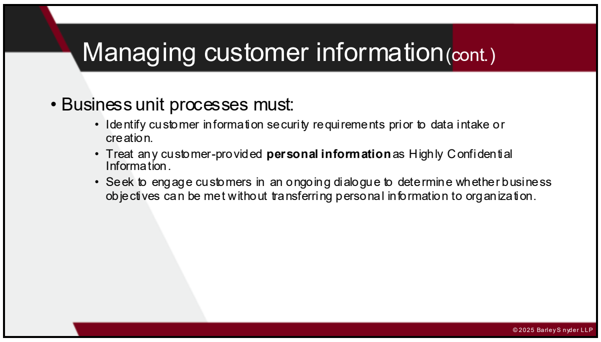
- Service providers must agree by contract to comply with applicable laws and organization's policy or equivalent information security measures.
- Organization may require service providers to demonstrate their compliance through:
  - Pre-engagement due diligence.
  - Independent audits or certifications, based on risks.
  - Ongoing compliance reviews.

Customer Data Protection



Managing customer information

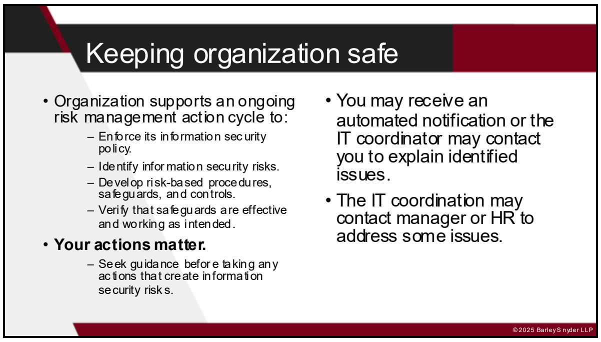
- Each business unit develops, implements, and maintains processes and procedures to:
  - Manage customer data intake.
  - Maintain an inventory of customer data.
  - Establish risk-based information security measures consistent with organization's policy.
  - Properly return or destroy customer data.
- Business units should not agree to follow customer information security policies without guidance from IT/Legal/HR.



Managing customer information (cont.)

- Business unit processes must:
  - Identify customer information security requirements prior to data intake or creation.
  - Treat any customer-provided **personal information** as Highly Confidential Information.
  - Seek to engage customers in an ongoing dialogue to determine whether business objectives can be met without transferring personal information to organization.

Risk and Compliance Management



Keeping organization safe

- Organization supports an ongoing risk management action cycle to:
  - Enforce its information security policy.
  - Identify information security risks.
  - Develop risk-based procedures, safeguards, and controls.
  - Verify that safeguards are effective and working as intended.
- **Your actions matter.**
  - Seek guidance before taking any actions that create information security risks.
- You may receive an automated notification or the IT coordinator may contact you to explain identified issues.
- The IT coordination may contact manager or HR to address some issues.

Questions?