Preparing for a Post-COVID Future:
Privacy and Cybersecurity Risk Management

Lillian Russell, Esq., CIPP-US, CIPM – Chief Privacy Officer
Office of Privacy – Risk Management - Chief Executive Office
Los Angeles County Management Council

Overview

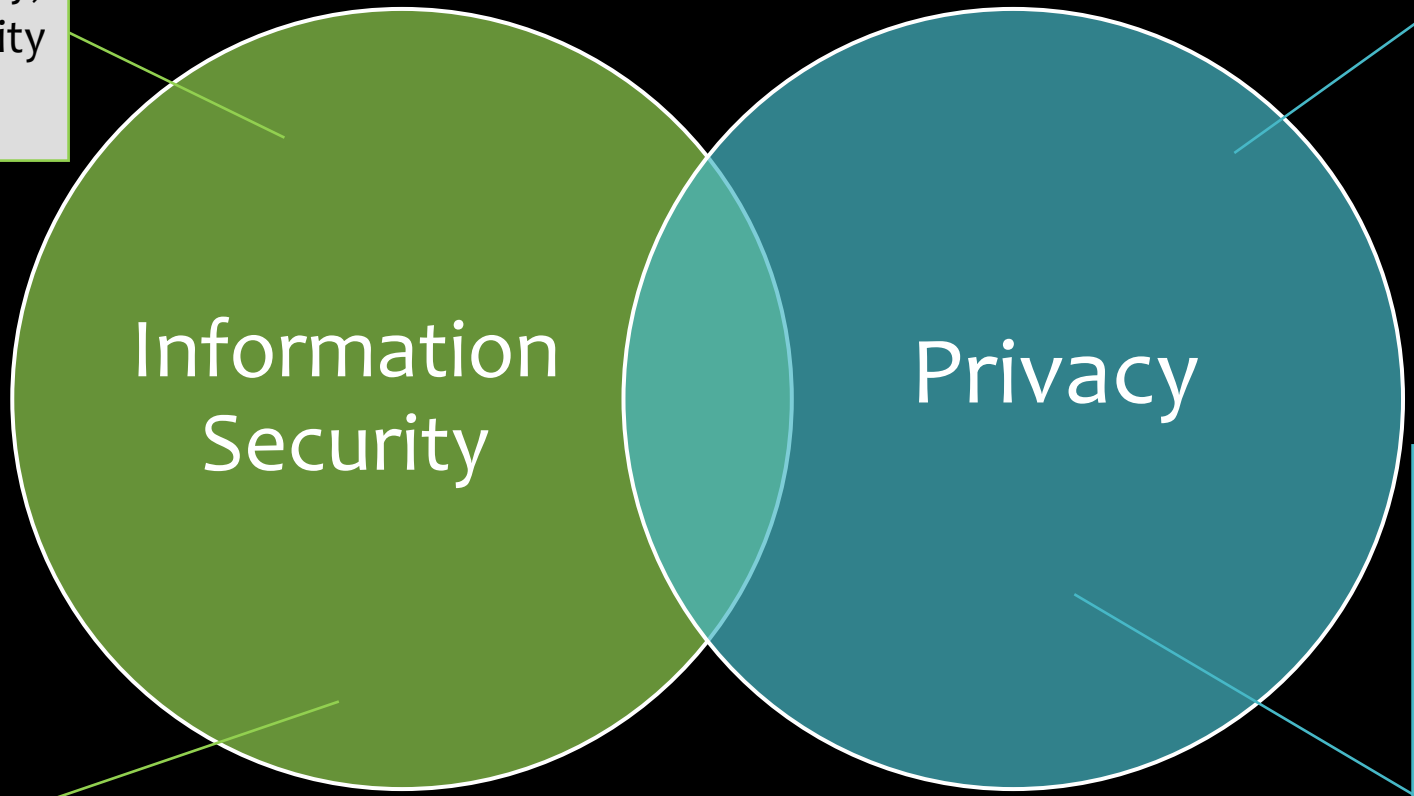
- **Introduction: Key Concepts**
  - Information Security and Privacy
  - Cybersecurity & Common Risks
  - Event Classification: Incidents vs. Breaches
- **Cyber Threats**
  - Recent Global & U.S. Events
- **Privacy & Cybersecurity in LA County**
  - **Risk Considerations**
  - **Risk Management Protocols**
    - Countywide Employee Education and Policies
    - Cybersecurity and Privacy Incident Response
- **Questions and Comments**

Introduction: Key Concepts

Information Security, Privacy, and Cybersecurity

Intro: Information Security and Privacy

Ensuring confidentiality, integrity, and availability of information

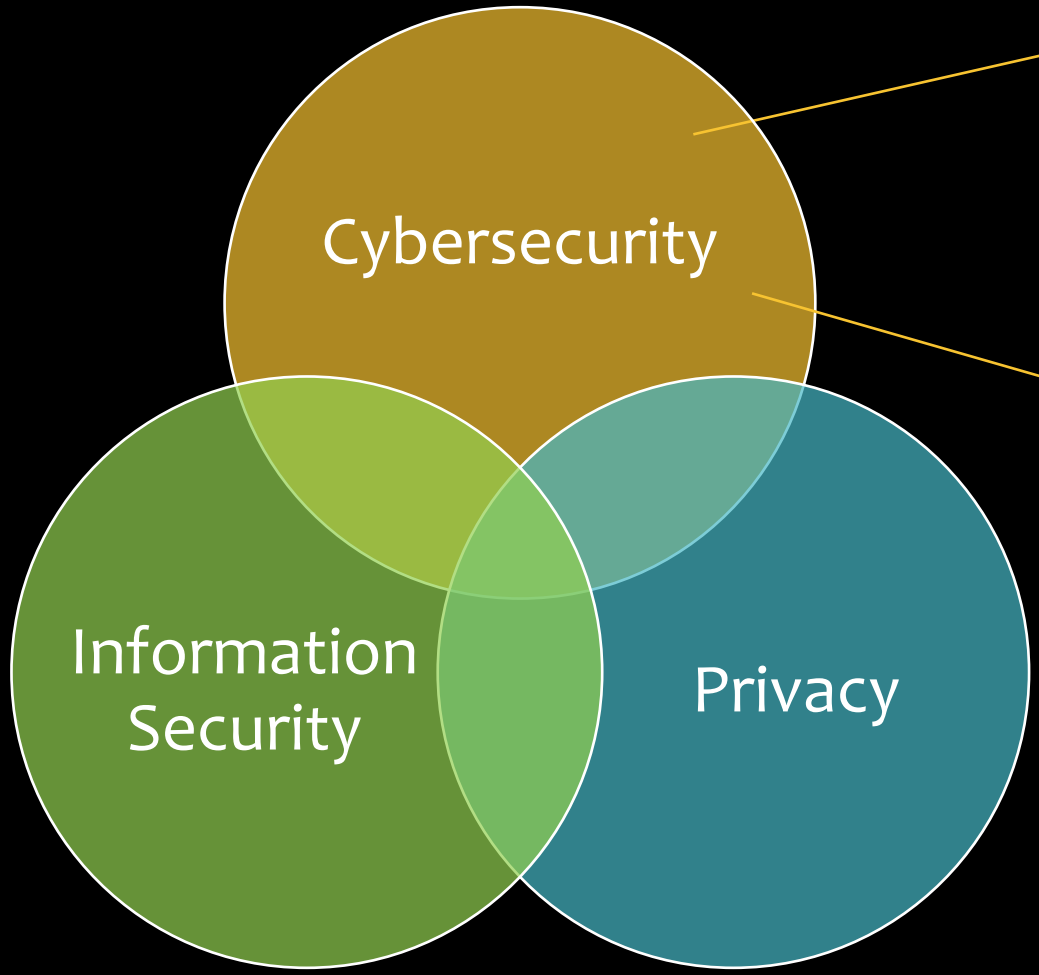


Focuses on how information is collected, used, stored and shared

Implement Security Controls:
Procedural,
Access,
Technical,
Compliance

Implement Privacy Controls:
Collection/ purpose,
Risk assessments,
Risk management,
Data quality,
Data minimization & retention

Intro: Cybersecurity



Protecting networks, devices, and data from unauthorized access, attack or misuse

Focuses on protecting servers, endpoints, databases, and networks by finding security gaps

Common Cybersecurity Risks

Malware

Malicious software such as computer viruses, spyware, Trojan horses, and keyloggers

Viruses can replicate and attach to another computer file, while keyloggers can spy on users

Ransomware

Type of malware that locks or encrypts data until a ransom is paid

May occur through malicious email attachments or links in compromised websites

Phishing

Misleading victims into providing personal or sensitive information (e.g., passwords, credit card information, login credentials)

May occur through fraudulent communication such as emails, phone calls, or text messages

Bad Actors

External Individuals/ Hackers

Employees/ Contractors

Event Classification: Incidents vs. Breaches

Security Incident

Actual or possible jeopardy to the **confidentiality, integrity, or availability** of an information system, or a violation or imminent threat of violation of security policies/procedures, or acceptable use policies.

Privacy Incident

Loss of control, compromise, or **unauthorized disclosure, acquisition, or access** of information, by **unauthorized persons** for an **unauthorized purpose** (whether physical or electronic).

Investigation & Determination by the Incident Response Team

Security Breach

Confirmation of unauthorized access to, or compromise of an information system.

Privacy Breach

Confirmation of unauthorized access or compromise of information, and/or meets certain legal and regulatory definitions of a breach.

Cyber Threats: Global & U.S.

Russia–Ukraine Crisis

Global & U.S. Cyber Threats - 2022

- **CISA Warnings**
  - U.S. Cybersecurity & Infrastructure Security Agency (CISA) has issued warnings to US businesses and governments about preparation to defend against cyber attacks, including potential:
    - Ransomware attacks
    - Malware attacks
    - Distributed Denial of Service (DDoS) attacks
    - Disinformation campaigns
    - Disruption to critical infrastructure
- **Global Impact:**
  - Cyber threats and attacks in this region may extend to organizations in other countries.
- **Consequences**
  - Cyber attacks can threaten an organization's daily operations and impact the availability of critical assets and data.
- **Defense**
  - Organizations should increase vigilance and evaluate their capabilities with planning, preparation, detection, and response for such an event.
  - Organizations are advised to ensure they are equipped to detect, prevent, and mitigate cyberattacks.

- **What happened**
  - Hackers broke into SolarWind's systems and added malicious code into the company's software system, called "Orion" which is used by 33,000 customers around the world. This went undetected for months.
  - At least 18,000 SolarWinds customers downloaded software updates that included the hacked code.
    - The code created a backdoor to customer's information technology systems, which hackers then used to install even more malware.
  - US agencies and private companies were attacked, including parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, the Treasury, along with Microsoft, Cisco, Intel, and Deloitte.

SolarWinds

Supply Chain Attack –December 2020
Global & U.S. Cyber Threats

Colonial Pipeline

Ransomware Attack –May 2021
Global & U.S. Cyber Threats

- **What happened**
  - Colonial Pipeline suffered a ransomware attack after hackers accessed its system by stealing a single password.
    - No multi-factor authentication was in place, so the system could be accessed through a password without a second later or validation.
  - Colonial Pipeline provides roughly 45% of the East Coast's fuel, including gasoline, diesel, home heating oil, jet fuel, and military supplies.

  - This cyber attacked disrupted fuel supplies to the U.S. Southweast after Colonial Pipeline shut down the pipeline to prevent the ransomware from spreading.
  - Colonial Pipeline paid a ransom of $5 million in cryptocurrency.

Privacy & Cybersecurity in LA County: Risk Considerations

Where are the threats?

Cyber Insurance: 2022 and Beyond

- Shifts in the Insurance Markets
  - Increases seen in:
    - Premiums and SIRs (self insured retentions)
    - Scrutiny in cybersecurity and privacy controls and internal procedures
    - Loss ratios-
- Understand whether certain risks are covered… or not
  - Ransomware
  - Privacy regulations & legislative changes
  - War exclusions
  - Data breaches
- Cyber risk management maturity
  - Cybersecurity and data protection architecture
- Adapting to 2022 threats
  - Changing motivations of threat actors
  - Extent of business disruption

Information Security and Privacy Contract Requirements

Incident Response Protocols

Cybersecurity and Privacy Risk Assessments

Data Inventory & Business Processes

Vendor Risk Management

- Vendor Management Policies
- Identify and classify vendor risk
- Compliance assessments and monitoring
- Understand services and business processes

Teleworking

Risks

- File Sharing & Management
- Unsecured Wi-fi
- Inexperienced users & non-compliance
- Sudden shift to virtual environments

Milestones

- Multi-Factor / 2-Factor Authentication
- Electronic Signatures
- Paper → Digital
- Digital efficiency

Teleworking

Lessons

- Employee Training
- Enhanced Incident Response protocols
- Access Management

Passwords

The first line of defense against unauthorized access to IT systems and information.

High Risk:

- Re-used passwords
- Weak/ easily guessed passwords

Risk Mitigation:

- Strong & unique passwords
- 2FA – Two-Factor Authentication
- SSO – Single Sign-On

+1 (323) 378-7[redacted]

Text Message
Today 3:28 PM

CITI: Your account has locked and requires verification, to restore please visit http://citi01online.com

Text Message
Today 2:43 PM

We qualified you for 15,000 in student debt forgiveness. It expires today so call me @ 412-274-[redacted]. Just need 5 mins.

Text Message
Today 9:34 AM

APPLICATI0N BACKGR0UND

https://bit.ly/37r[redacted]

Reply stop to opt out

GMAIL 4m ago

service@intl.paypal.com
Bill Hatzidiakos sent you 20,00 USD via PayPal
Create an account to accept it. Hello! [redacted]@gmail.com Bill Hatzidiakos sent you a payment Accept your 20,00 USD today Transaction Details Transaction ID 9AG49554...

Phishing

A form of social engineering that attempts to steal personal information through a fraudulent solicitation via email, text or website.

Victims unknowingly volunteer their personal information to bad actors who are pretending to be a legitimate business or reputable person.

Privacy & Cybersecurity in LA County: Risk Management Protocols

Education, Policies, and Incident Response

LA County: Privacy & Cybersecurity Risk Management Protocols

Countywide Employee Education

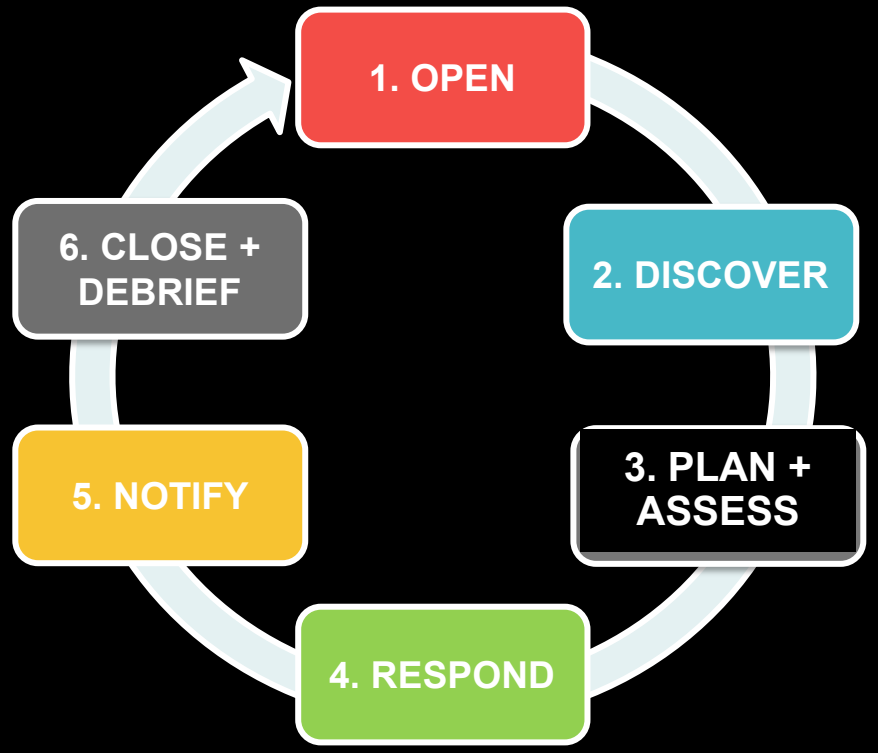
- Privacy Awareness Training
- HIPAA Training
- Cybersecurity Awareness Training
- IR Tabletop Exercises

Countywide Policies & Practices

- Updated Information Security Policies
- New Privacy Policies
- New HIPAA Policies

LA County: Privacy & Cybersecurity Risk Management Protocols

Incident Response Stages



Incident Response: Key Stakeholders

ISD – Cybersecurity Governance Operations	CEO Teams: Privacy & CIO	BOS
PIO	County Counsel	DHR
OCI	Law Enforcement	Impacted Departments

Questions & Comments

Contact privacy@ceo.lacounty.gov
or
Lillian Russell lrussell@ceo.lacounty.gov