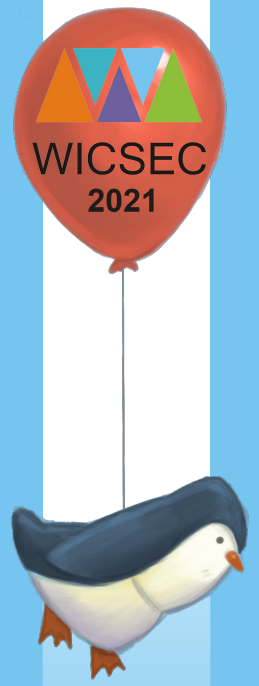
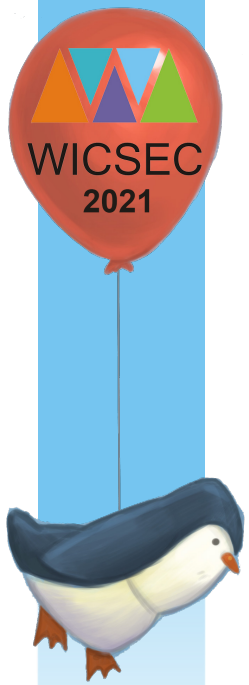


IT Security
Now and in the Future

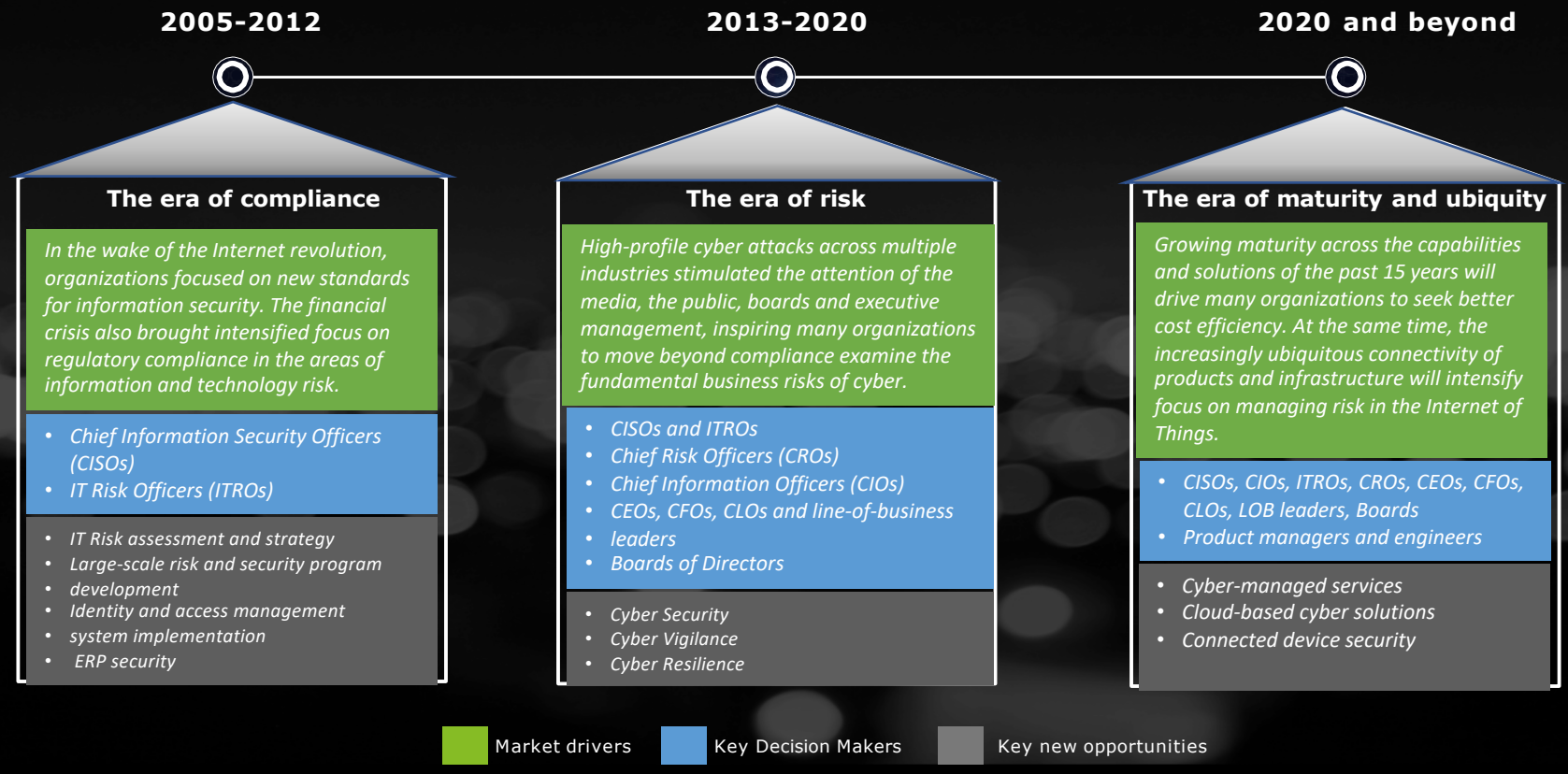
David Kilgore, Director of California Child Support Services
Piyush Pandey, Advisory Managing Director, Deloitte Consulting LLP



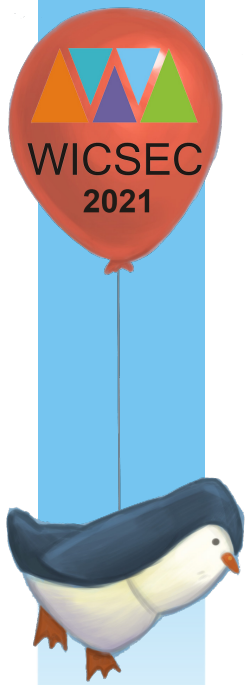
How do you see cyber has evolved over the years? Discuss the evolution of cyber from a function of compliance to risk to the enabler of business transformation in the current era of hyperconnectivity…

The evolution of cybersecurity

The evolution of cyber risk is generally cumulative. That is, the drivers and opportunities in one era do not replace those of the preceding era. Rather, they expand the horizon.

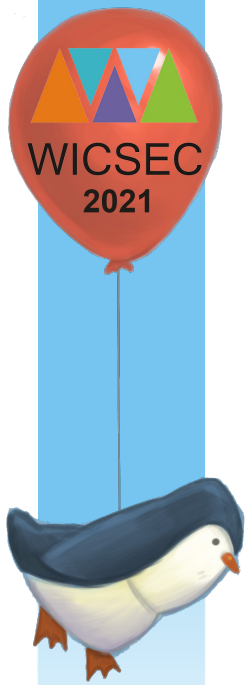


2



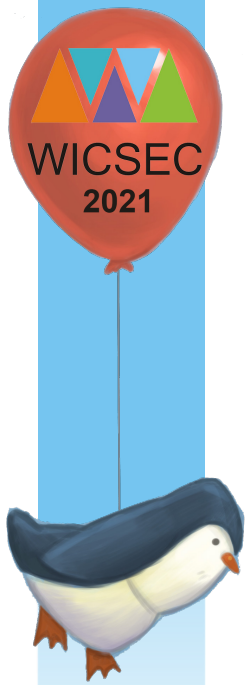
What are the cyber trends – both global and local…what are specific risks organizations, especially government organizations, are dealing with from a cyber threat perspective?

Zoom Questions



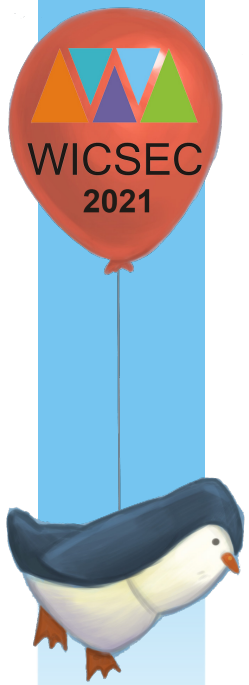
How is your organization addressing cybersecurity:

1. Strictly following regulatory requirements to make sure I am complaint
2.I evaluate risk to determine the necessary level of cyber controls.
3. I work with business to help them enable business processes using cyber



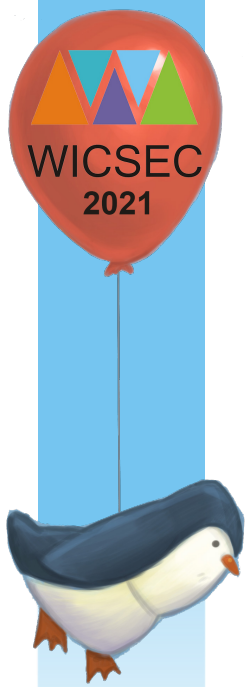
What are specific considerations for child support agencies – discuss the state of cyber maturity, workforce challenges, regulatory requirements (IRS) etc.?

DCSS Compliance Regulations



- IRS Publication 1075
- Internal Revenue Code section 6103, 7431, 7213(a), 7213A
- 42 United States Code section 454
- California Welfare and Institutions Code sections 11478.1
- California Family Law Code section 17212
- 22 California Code of Regulations sections 111430
- National Institute of Standards and Technology (NIST 800-53)

What is PII & FTI



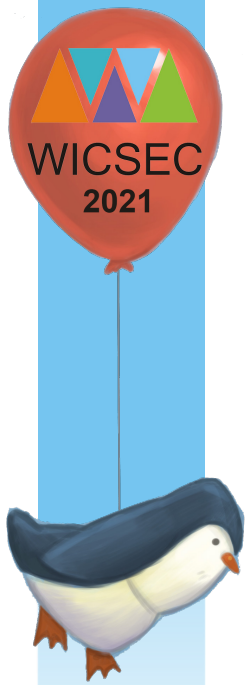
Personally Identifiable information (PII) – any information that can be used to distinguish an individual's identity

Example: a first name or first initial and last name in combination with any of the following elements:

- SSN, Driver's license, Bank account, Passport, Email

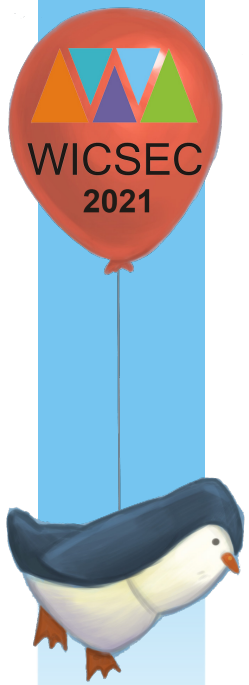
- **Federal Tax Information (FTI)** – tax return information received directly from the IRS or through an authorized secondary source (SSA, OCSE, etc.)

Protecting PII and FTI – wherever you are



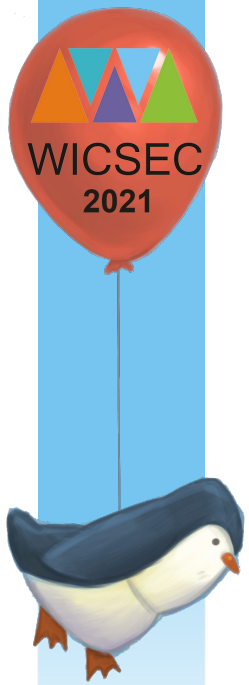
- Must have an “official need to know”
- Only access from work devices (laptop, etc.) NEVER personal
- Use Multifactor Authentication whenever available
- Encrypt emails intended for an external authorized recipient
- Get their address right
- Phishing is on the rise. Open/respond only to legitimate emails
- Delete confidential information when no longer required
- Follow your organization’s records management policy regarding retention and disposal requirements

How does DCSS protect PII & FTI?



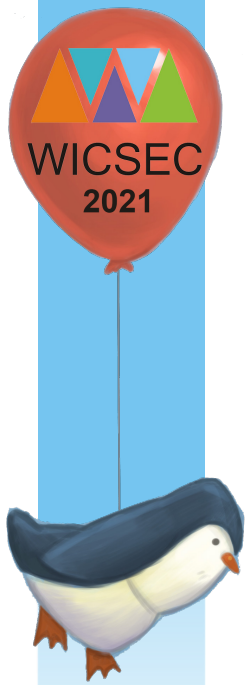
- Data Loss Prevention software on all emails managed by DCSS
- Encryption for all emails with sensitive information
- VPN or VDI to ensure a more secure connection
- Encrypted work devices
- Policies, trainings, guidelines, tips, techniques

PII & FTI Protection (continued)



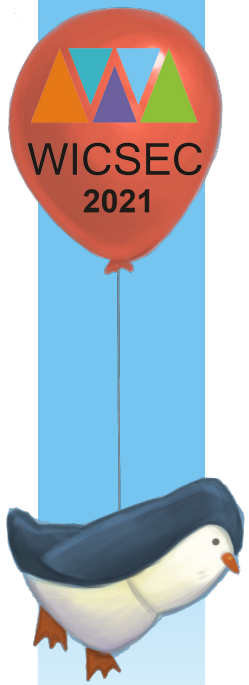
- Information security training for ALL staff:
  - Identification, reporting and handling of “phishing” emails
- Compliance with oversight agencies policies and regulations
  - IRS Publication 1075, Section AC-17 Remote Access
  - Multifactor Identification required for remote access
- Safeguard Reviews conducted
- Critical system vulnerabilities patched right away

Zoom Questions



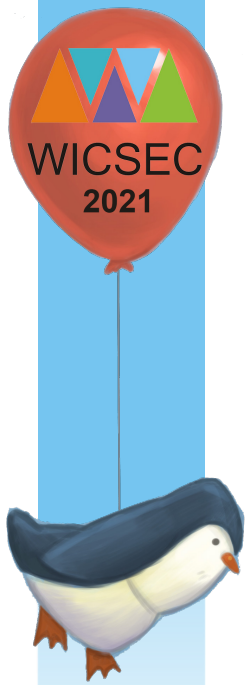
What does IRS 1075 entail?

1. cybersecurity controls
2. Implementation guide
3. compliance guidelines



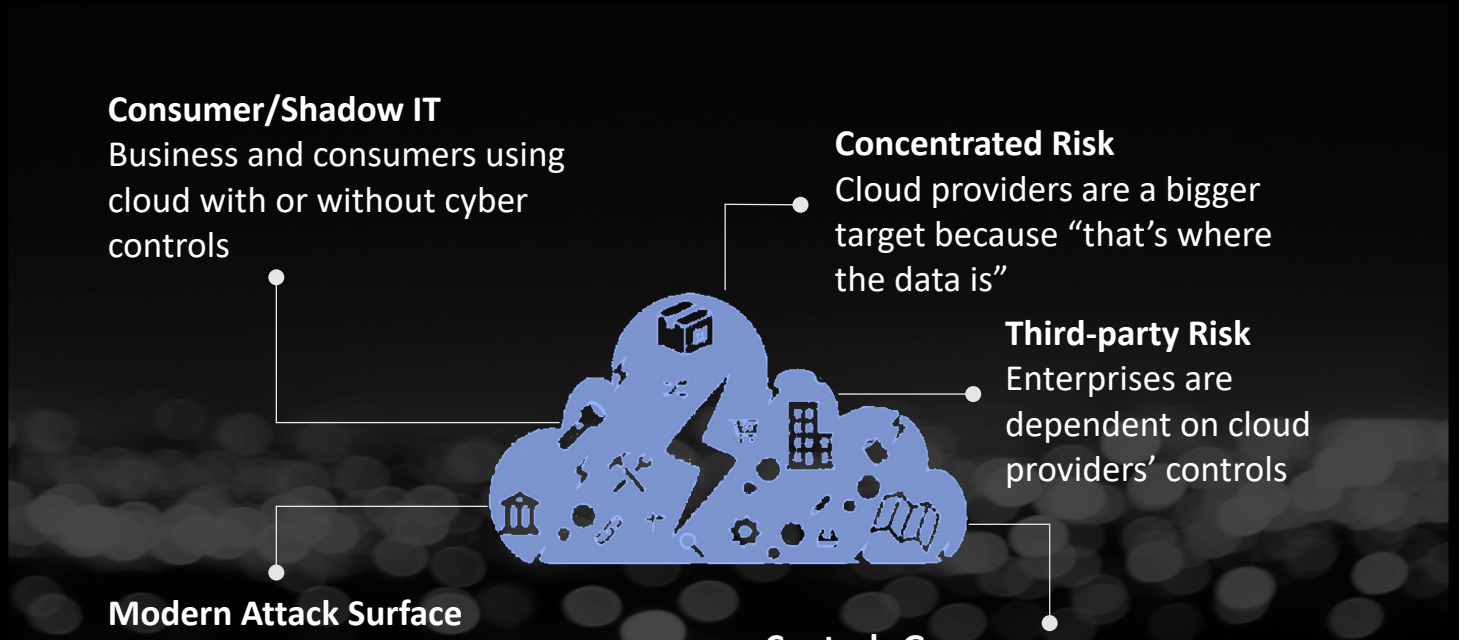
Discuss trends of cloud adoption and special considerations for cyber to protect data in the cloud and alignment with IRS requirements.

Future Considerations for CA



- Move to the cloud to Improve infrastructure resilience & security
- Prepare to manage security incidents, such as ransomware scenarios
- Passwordless and Multi-factor Authentication for all
  - Replace complex passwords with combination of one or more of the following: biometric, physical devices, MFA
- Maintain single user identity
  - Single-Sign-On improves security, simplifies monitoring, and enhances user experience
- Information Security Customer Service Web Portal
  - Source of accurate information and self-service capability for security

There are a variety of cyber risks associated with moving to the cloud, yet there is also an opportunity



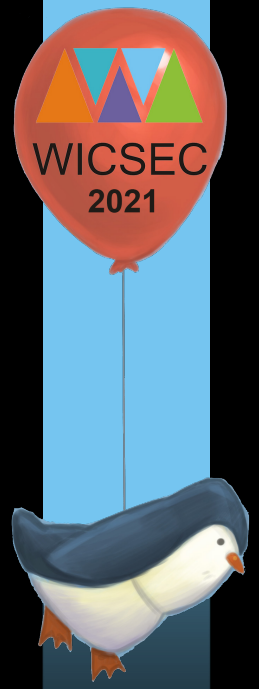
Consumer/Shadow IT
Business and consumers using cloud with or without cyber controls

Concentrated Risk
Cloud providers are a bigger target because “that’s where the data is”

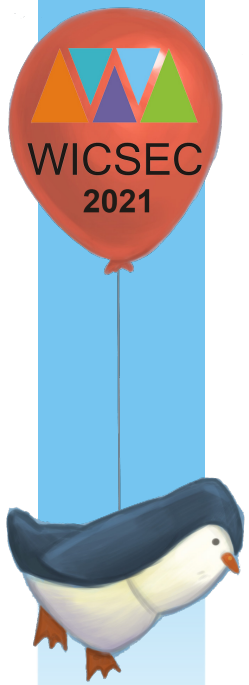
Third-party Risk
Enterprises are dependent on cloud providers’ controls

Modern Attack Surface
The walled enterprise is replaced by a hybrid, more complicated technology environment

Controls Gap
Traditional cyber risk controls need to extend to the cloud at a time when many enterprises are barely keeping up with existing threats

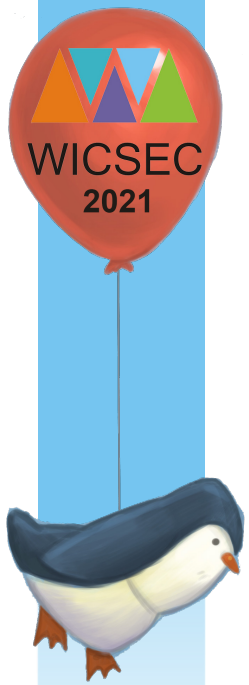


Zoom Questions



Who is responsible for cybersecurity in the cloud?

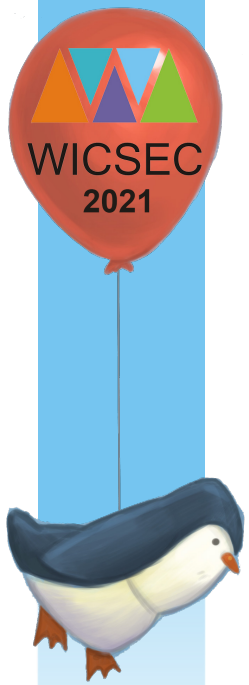
1. Cloud provider
2. System Integrator
3. Customer
4. Depends



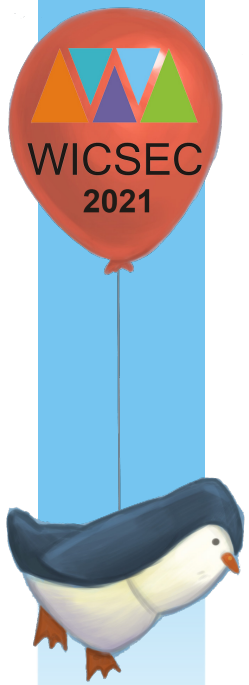
Discuss a holistic approach for cyber risk management – a programmatic approach to integrate cyber as part of the organizational culture and cyber by design as part of a system lifecycle.

CA Telework Guidelines

- Establish Good Boundaries
  - The IRS requires two barriers to prevent unauthorized access to FTI.
  - In a telework location, a locked front door and a locked room
  - Use VPN or VDI for a secure connection
  - Secure your Wi-Fi with supported protections
  - When available, use guest Wi-Fi in your house for visitors
- Best Practices for your Monitor
  - Be mindful that your monitor does not face a window
  - Family and friends may not view confidential information
  - Use a privacy screen

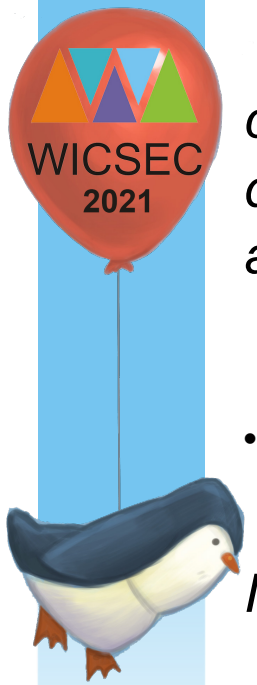


CA Telework Guidelines (continued)



- Secure All Documents
  - File cabinets must be kept closed, locked, and in a secure location
- Computer Workstations
  - Secure when not in use with a cable or in a locked drawer
  - Use only your work computer to access sensitive information
- Key Access
  - Securely maintain any keys to locations containing work equipment, folders or files

IRS Audit Requirements Telework and Site Inspections



- IRS Publication 1075 Section 4.7 Telework Locations:

  "…*If the confidentiality of FTI can be adequately protected…non-traditional work sites can be used… The agency must conduct periodic inspections of alternative work sites during the year to ensure that safeguards are adequate… IRS reserves the right to visit alternative work sites while conducting safeguard reviews…*"

- DCSS' telework policy:

  "DCSS may require an inspection of a home office space to ensure the security of FTI. If warranted, employees will be notified."

- DCSS requires remotely working staff to self-certify by signing a Safety Checklist-Acknowledgement Form

The way forward – evolving cyber

Evolve the approach

Consider the end-to-end process, build in cyber risk by design, think more mobile-centric, focus on driving business outcomes

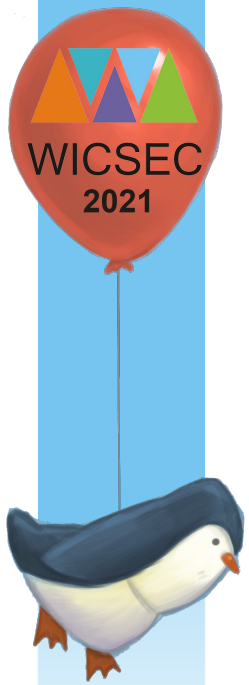
Robotics, cognitive automation and **artificial intelligence**

to increase the velocity and scale of detection and response for managing cyber risk

Use **Digital identity** to manage human and machine **credentials**

Cyber Resilience

goes beyond recovery of systems and processes to incorporate business recovery in the wake of a "digital scorched earth" event



Questions?