isc2.org/Events | #ISC2Events

ISC2 Spotlight

Data access and its critical role in Incident Response

Dennis Ludena Ph.D.

Contents

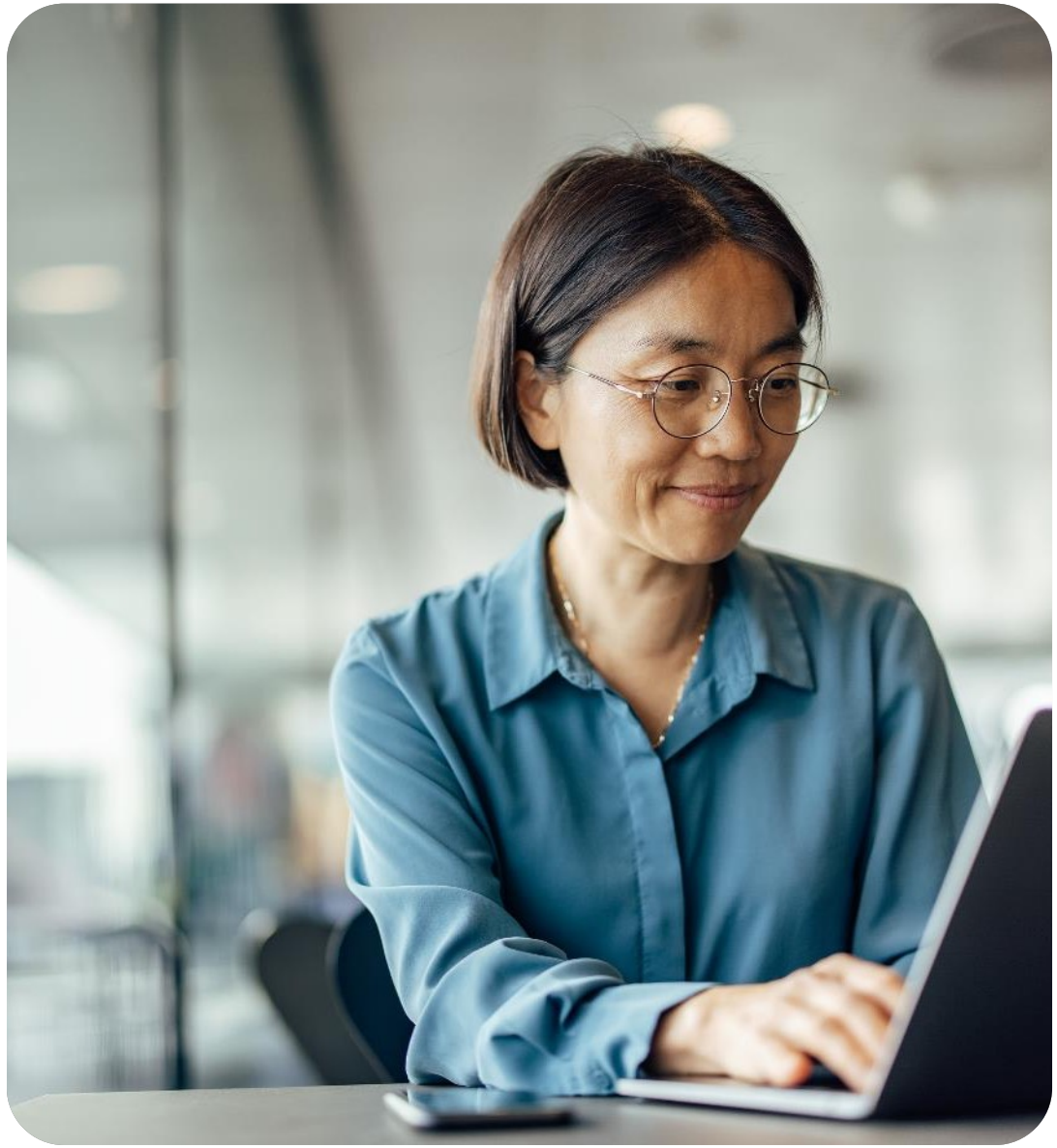
Today's contents:

- Summary
- Cost of a Data breach
- Incident Response (IR)
- Data Access Management
- Putting things together
- Conclusions

Summary

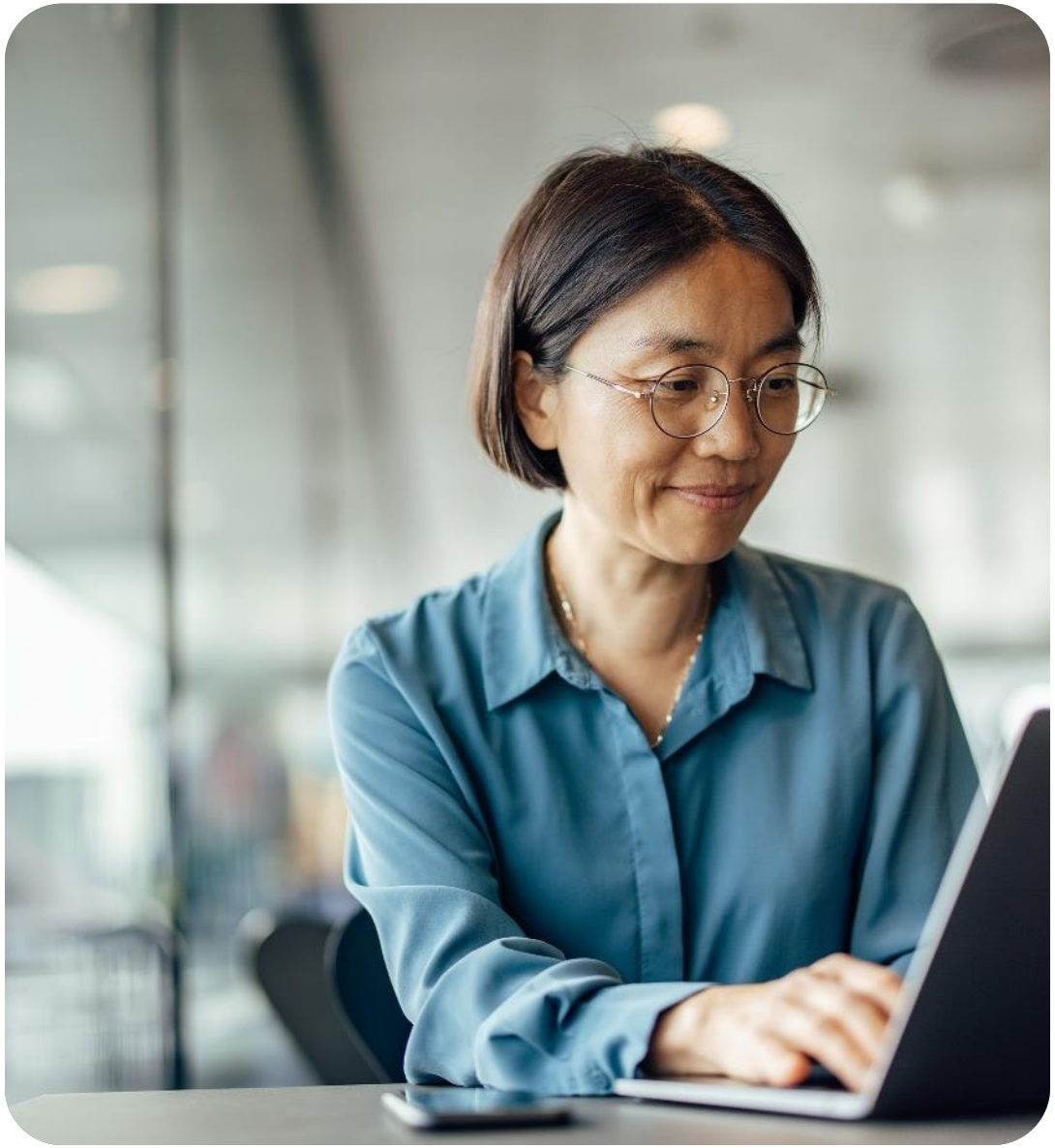
Summary

Incident Response is a complex process that touches all IT disciplines and business applications when its activation is required. In this scenario, Data Access, if well structured, protected and documented, could represent the last hope when it comes to protecting organizations' critical data. Both processes need to work together to strengthen organizations posture and evolve in time according to non-on-premise infrastructure adoptions.



Cost of a Data breach

Cost of a Data breach



Cost of a Data breach by country or region [1]

Incident Response

Incident Response (IR)

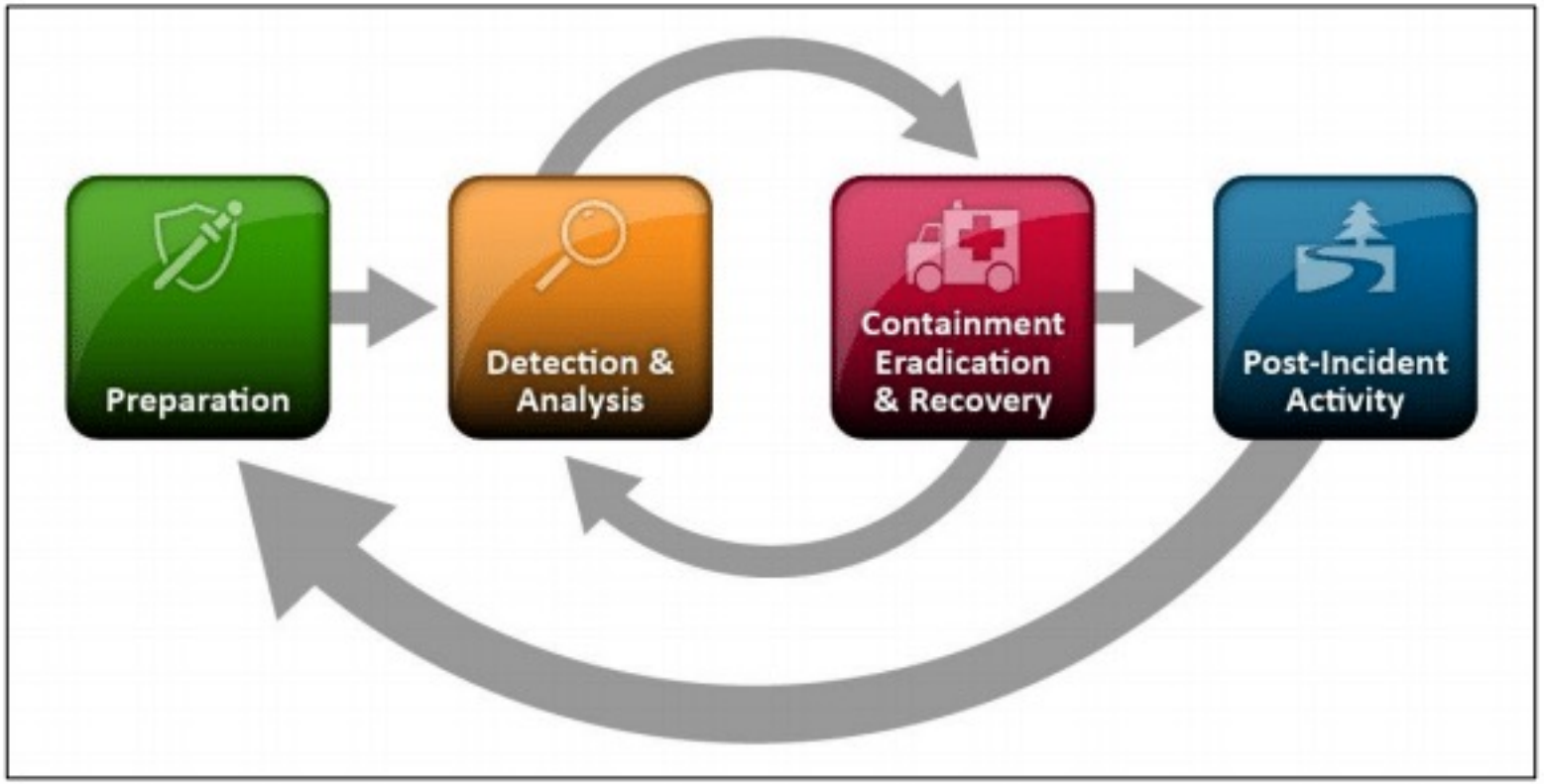


Figure 1. NIST Incident Response Life Cycle [1]

Incident Response (IR)

- When is the IR process activated?
  - Organization's senior management decided to declare a Security Incident when there is proving evidence of an attack
  - Organization's third party (business partner) has been infected
  - Global operating organizations' HQ, or a branch is under attack
  - SOC found evidence of data leaked in the dark web, etc.
- What behaviors can we expect when a Security Incident occurs?
  - Increased nervousness
  - Unclear understanding of specific deliverables
  - No visibility on the data required to act upon

Incident Response (IR)

- What attacks could damage organizations' data?
  - Accidental exposure
  - Phishing and other social engineering attacks
  - Insider Threats
  - Ransomware
  - Data Loss in the Cloud
  - SQL injection
- What attackers are they looking for?
  - Illegal collection of critical organizations' data
  - Customer information to be used in further attacks

Incident Response (IR)

- What attackers are they looking for? (Cont'd)
  - Economic revenue through ransom
  - Organization financial data
  - Persistence to execute future payloads

Data Access Management

Data Access Management

- What are the possible solutions to protect data?
  - Understand where critical data (crown jewels) are located
  - Decide a Data Access Management framework/method
  - Put into effect the decided solution
  - Document the process
  - Review/audit the process in a frequent basis (bi-annual, quarterly, etc.)
  - Decide on a data masking solution

Data Access Management

- Available frameworks
  - Authentication (e.g. username and password, PINs, X.509 digital certificates, one-time passwords, biometrics, smart cards, electronic passports, hardware tokens, etc.)
  - Single Sign-on
    - Particularly important due to its ability to provide access to multiple protected resources across domains
    - Transparent to the user, only one password required to remember
  - Authorization
    - Various models and mechanisms available: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC)

Data Access Management

- Available frameworks (cont.)
  - Federation and Trust
  - Security Auditing
    - Auditing is key in any process
    - Below logs should be analyzed
      - Authentication events
      - Authorization events
      - Directory objects modification
    - Centralizing these logs according to organization's' retention periods could help auditors to create reports, etc.

Putting things together

Putting things together

- Once the data access management is adopted
  - Log centralization is key for SOC's:
    - Data correlation
    - Alert generation
    - Use case creation
    - Data retention periods (>36 months)
  - Process creation:
    - Document the process
    - Establish a frequency to review/update the process
  - Audit:
    - Audit established process looking for improvements
    - Establish a frequency to review/update the process
  - Repeat

Putting things together

- Strategies and technology:
  - Strategies
    - Network Isolation – especially the one where crown jewels DBs reside
    - Network behavior analysis
      - Done in a yearly basis
      - Network traffic storage for 36 months
      - Metadata analysis
      - Data correlation, use case creation
      - Repeat
    - DR/BCM environment ready to switch
  - Technology
    - EDR/XDR/MDR
    - Data masking
    - Backup in place (either by delta/batch update)

Putting things together

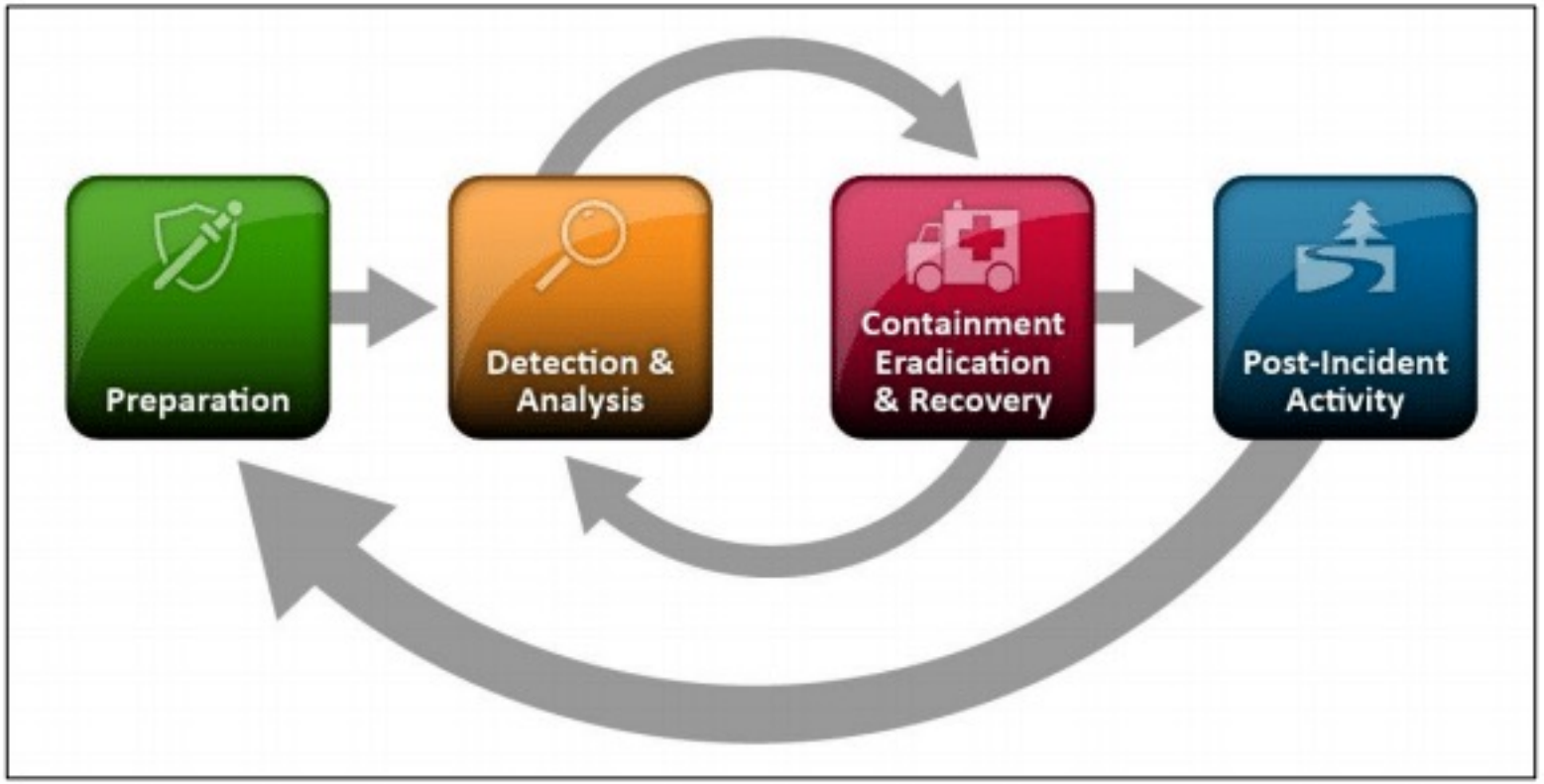
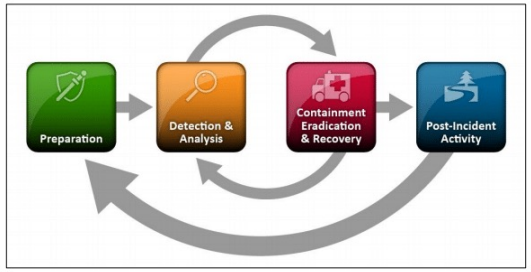


Figure 1. NIST Incident Response Life Cycle [1]

Putting things together

Preparation

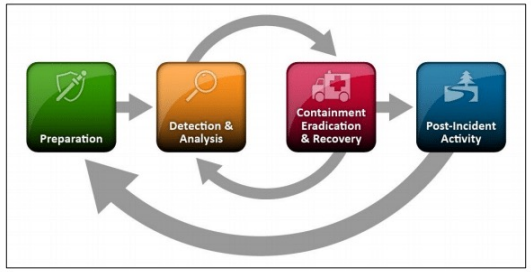
- CI Identification
- Segmentation if possible
- Security Controls
  - Logging and Monitoring
  - Data retention
  - Data correlation and alert generation
  - SOC use case
  - Automation
  - Crown Jewels Data backup solution
  - DR/BCM



Putting things together

Detection and Analysis

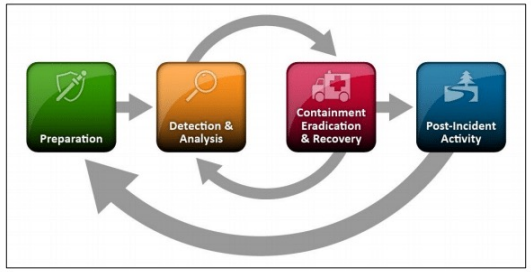
- Alerts
- SOC use case
- Triage
- Automation
- AI?



Putting things together

Containment Eradication and Recovery

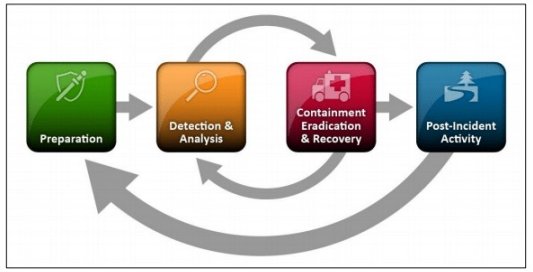
- Network isolation
- Crown Jewels Backup use (Delta/batch, etc.)
- DR/BCP use



Putting things together

Post Incident Activity

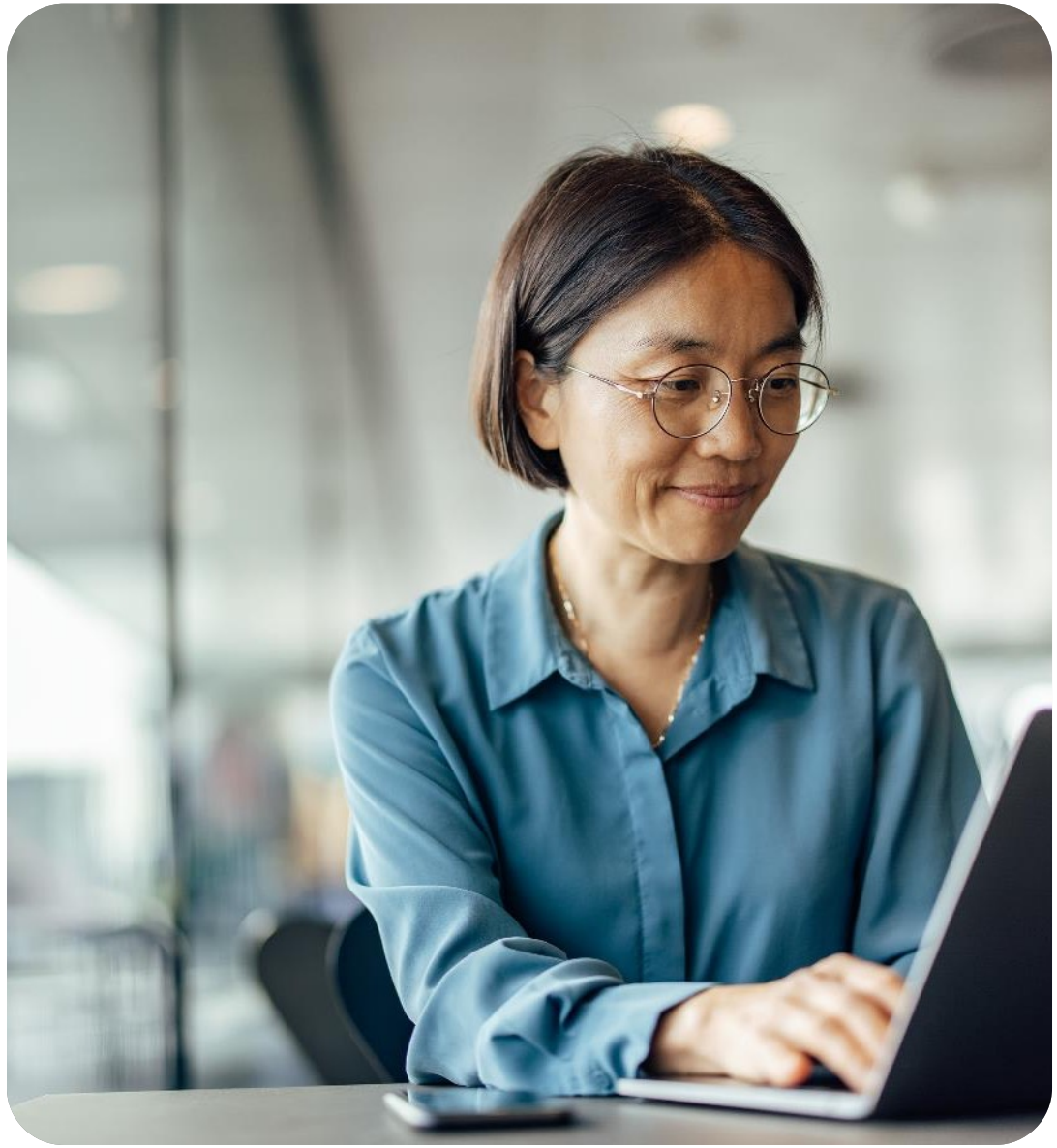
- Lessons learned
- Problem Management
- Root Cause Analysis



Conclusions

Conclusions

- Preparation is key
- Incident Response document is a must
- Visibility on Crown Jewel Data is critical – “You can not defend what you can’t see”
- Process documentation is a must
- Technology is just a part of the solution – NOT THE SOLUTION
- Practice, tabletop exercises are key to create muscle memory
- Review documented process
- Repeat



Thank You!

ISC2 Spotlight