Proposed Incident Response Methodology For Data Leakage

Presenting the best processes and procedures to safeguard
your business while preventing data leakage

Alex Rabello, Junior Goulart, Marcelo Karam, Marcos Pitanga, Reinaldo Gomes Baldoino Filho and Ronaldo Ricioni

IESB University Center – Brasilia, Brazil

alex.rabello@privamax.com.br, jgoulart@vidalink.com.br, karam@unb.br, marcos.pitanga@talkcomm.com.br, reinaldo.baldoino@iesb.edu.br and ronaldo@r3force.com

The Sixteenth International Conference on Software Engineering Advances
ICSEA 2021
October 03, 2021 to October 07, 2021 - Barcelona, Spain

Ronaldo Roberto Ricioni

Cybersecurity | Data Protection | Privacy | IT Governance

Sao Paulo, Brazil

MBA in Data Protection - IESB University Center - Brazil, 2021

CISO & RM IT Security Certification - EC-Council - USA, 2021

Executive Certification - SLOAN MIT and Bentley University - USA, 2012

MBA in Technology Innovation & Operations - FIA USP - Brazil, 2011

Telecommunication & Network Engineering - FEI - Brazil, 2000

Career development in Information Security, Risk Management and IT Governance with +20 years of work experience managing IT infrastructure and Cybersecurity services for large organizations in the financial and telecommunications market, such as, Neon, Afinz, Stone Pagamentos, Rede and Convergys Corporation.

ronaldo@r3force.com

Proposed Incident Response Methodology For Data Leakage

Purpose

Provide insights responding properly to any security and privacy incidents in order to safeguard organizations while preventing data leakage

Outline

- Purpose
- Introduction to incident response management
- Challenges & scenarios of data leakage
- Proposed methodology for data leakage approach
- Final considerations

- Purpose
- Introduction to incident response management
- Challenges & scenarios of data leakage
- Proposed methodology for data leakage approach
- Final considerations

Introduction

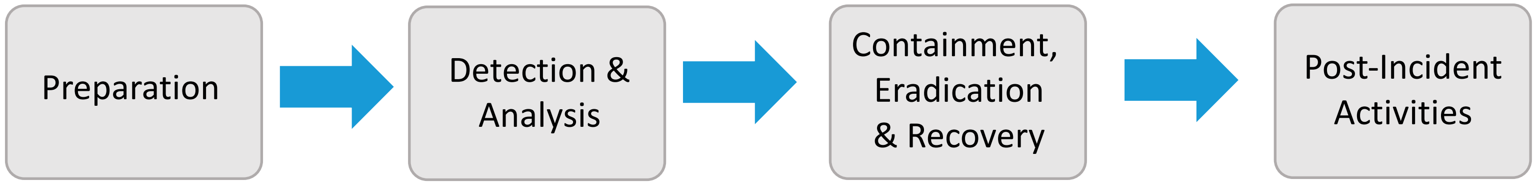
Overview of Incident Response

- ✓ Incident Response Management for security and privacy
- ✓ Risk analysis mapping possible data breaches scenarios
- ✓ Preferred way to handle the security incident lifecycle
- ✓ Frameworks with best practices of Incident Response Management
- ✓ Appropriate communication and notification with transparency

Introduction

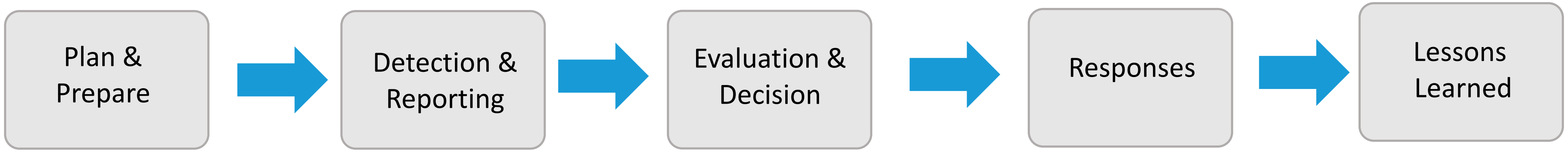
Incident Response Processes

NIST 800-61 - Computer Security Incident Handling Guide



Preparation → Detection & Analysis → Containment, Eradication & Recovery → Post-Incident Activities

ISO 27035 - Information security incident management



Plan & Prepare → Detection & Reporting → Evaluation & Decision → Responses → Lessons Learned

- Purpose
- Introduction to incident response management
- Challenges & scenarios of data leakage
- Proposed methodology for data leakage approach
- Final considerations

Challenges & scenarios of data leakage

Breach Type of Data Exposed

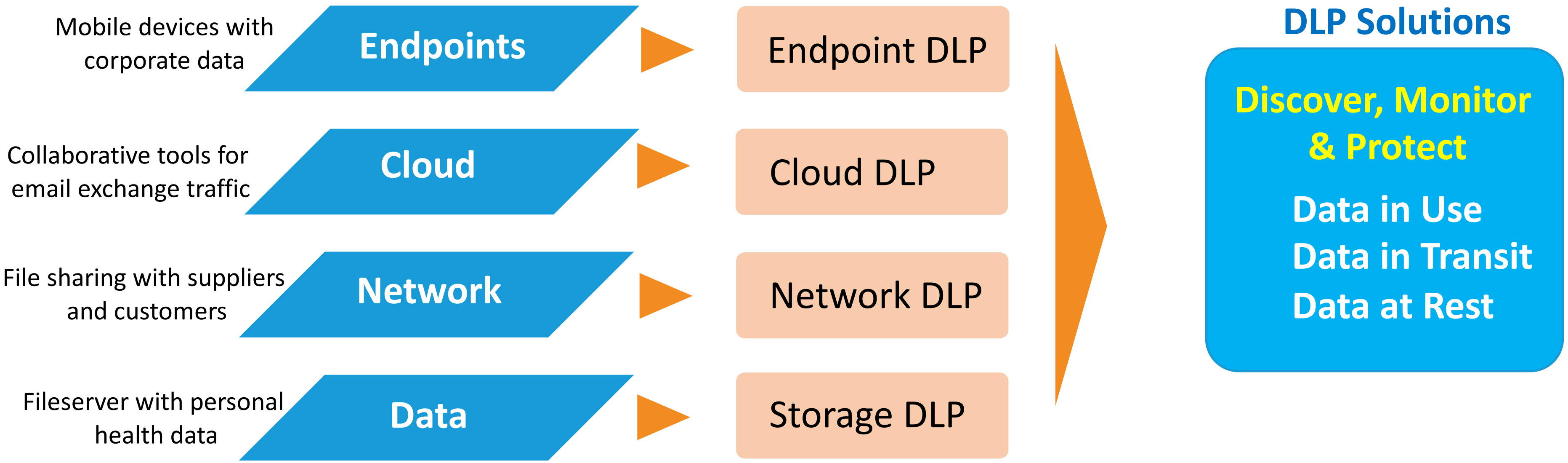
- ✓ Contact & Location information
- ✓ Personal Health Information
- ✓ Financial Identification Number
- ✓ Banking & Payment Information
- ✓ Username & Password

Reasons for Data Loss

- ✓ Software Failure
- ✓ Virus/malware
- ✓ Hardware Failure
- ✓ Human Error
- ✓ Theft/Malicious Employees

Challenges & scenarios of data leakage

Data Loss Prevention



Mobile devices with corporate data

Collaborative tools for email exchange traffic

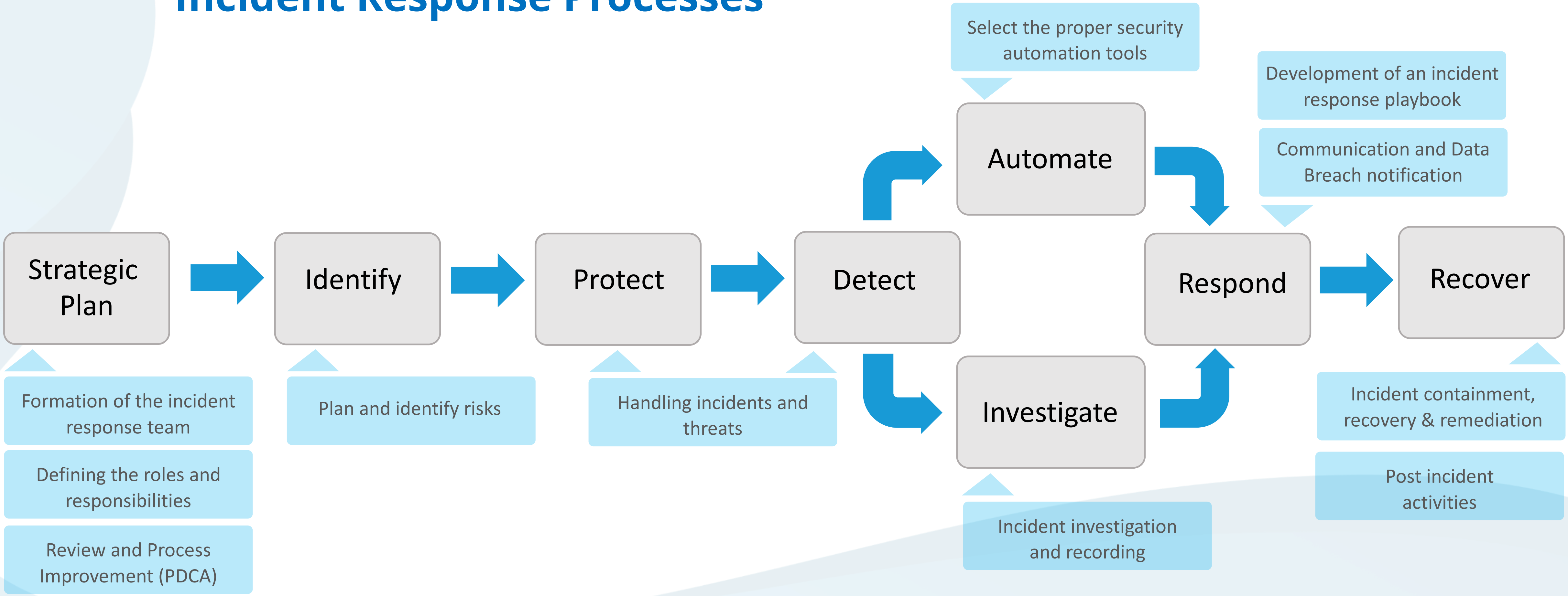
File sharing with suppliers and customers

Fileserver with personal health data

- Purpose
- Introduction to incident response management
- Challenges & scenarios of data leakage
- Proposed methodology for data leakage approach
- Final considerations

Proposed methodology for data leakage approach

Incident Response Processes



Select the proper security automation tools
Development of an incident response playbook
Communication and Data Breach notification
Automate
Strategic Plan
Identify
Protect
Detect
Respond
Recover
Investigate
Formation of the incident response team
Defining the roles and responsibilities
Review and Process Improvement (PDCA)
Plan and identify risks
Handling incidents and threats
Incident investigation and recording
Incident containment, recovery & remediation
Post incident activities

- Purpose
- Introduction to incident response management
- Challenges & scenarios of data leakage
- Proposed methodology for data leakage approach
- Final considerations

Final considerations

Key points

- ✓ Develop a team with diverse abilities (security, privacy, legal, public relations)
- ✓ Proper documentation and chain of custody for the entire incident timeline
- ✓ Use of security automation tools applied to short deadlines for notification
- ✓ Lessons Learned & Continuous Improvement
- ✓ Decision plan for public notification

Thank You for your time

ronaldo@r3force.com