Conferencia Anual Latinoamericana Sobre Delitos Financieros de la ACFCS

13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis

CIBERDELITO y CIBERINVESTIGACIÓN

Shahryar Shaghaghi

National Leader, Technology Advisory Services

Head of International BDO Cybersecurity

BDO USA, LLP

Los Estados Unidos

ACFCS | ASOCIACIÓN DE ESPECIALISTAS CERTIFICADOS EN DELITOS FINANCIEROS

BDO

With You Today

SHAHRYAR SHAGHAGHI

National Leader, Technology Advisory Services

Head of International BDO Cybersecurity

+1 212-885-8453

sshaghaghi@bdo.com

Conferencia Anual Latinoamericana Sobre Delitos Financieros de la ACFCS

13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis

BDO

Today's Landscape

Today's Landscape

Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.

This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was $4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of $13.1 million.

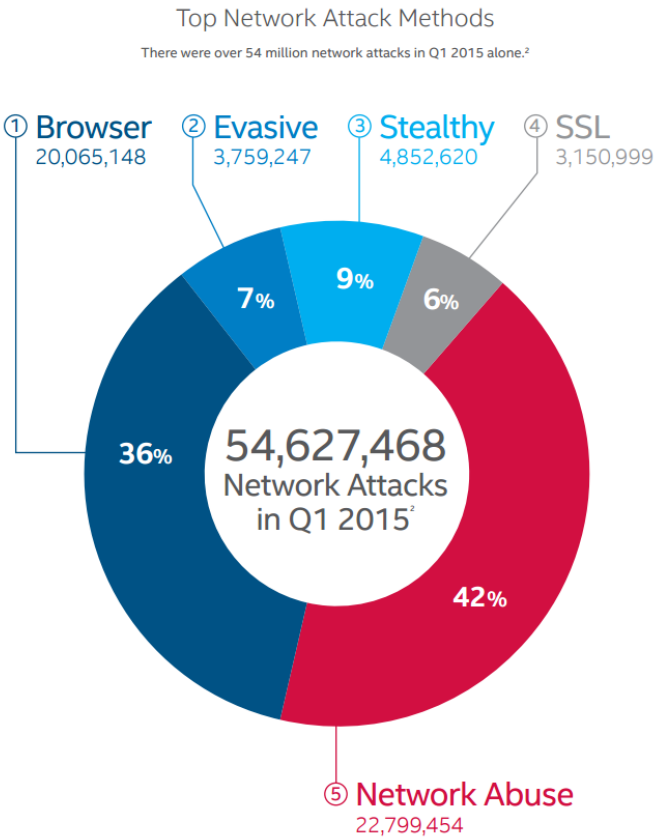
Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection

2016 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC June 2016

Today's Landscape

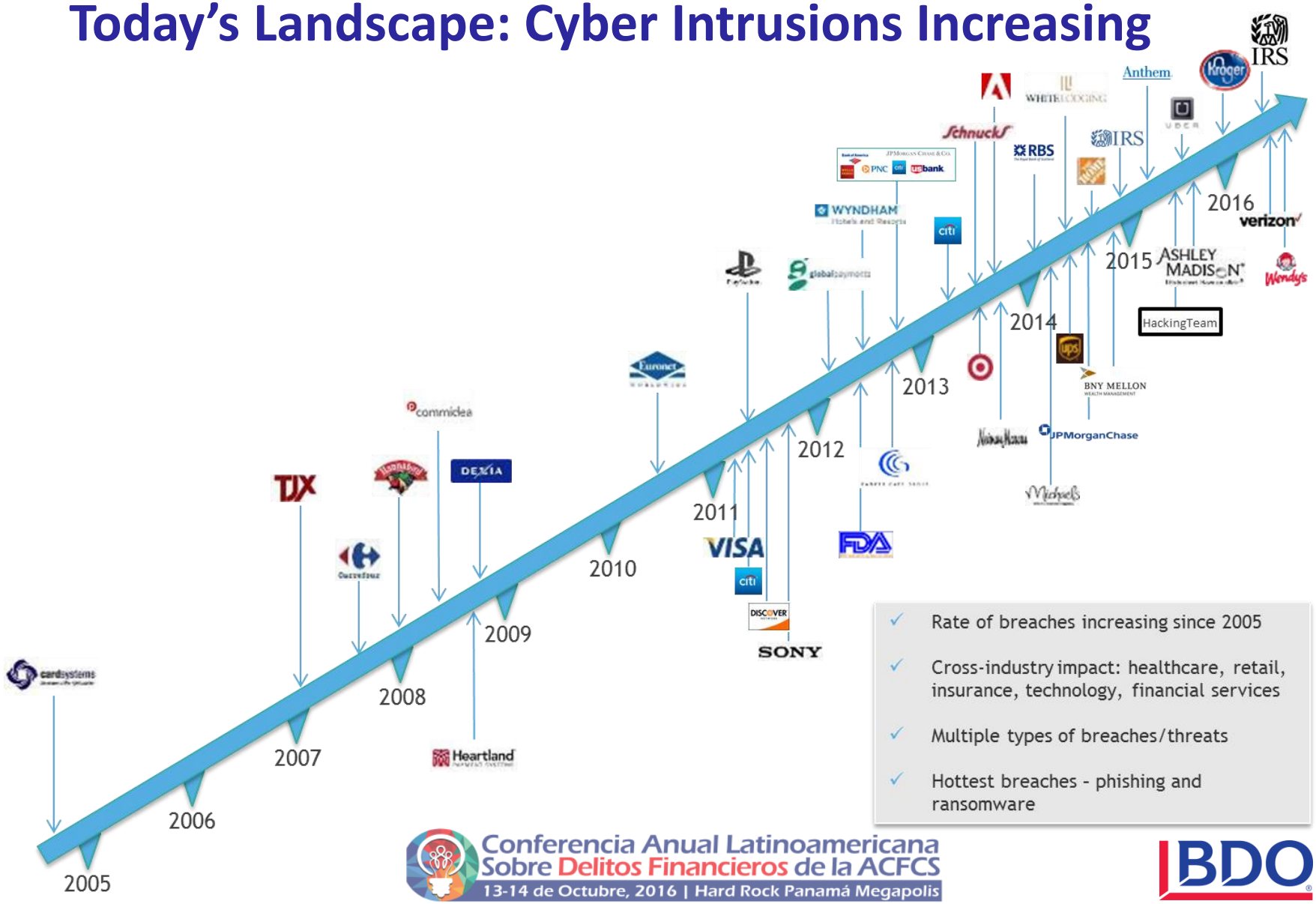
What Data Are They Taking?

Data types	Internal Actors	External Actors
Customer Information	27%	32%
Employee Information	33%	28%
Intellectual Property	15%	14%
Payment Card Information	11%	15%
Other Financial Information	14%	11%



Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection
Intel Security Report, Dissecting the Top Five Network Attack Methods: A Thief's Perspective

Today's Landscape: Cyber Intrusions Increasing



- ✓ Rate of breaches increasing since 2005
- ✓ Cross-industry impact: healthcare, retail, insurance, technology, financial services
- ✓ Multiple types of breaches/threats
- ✓ Hottest breaches - phishing and ransomware

Conferencia Anual Latinoamericana Sobre Delitos Financieros de la ACFCS
13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis

BDO

Today's Landscape

1.5 million
Cyber attacks each year
(approx. 4,000 per day)

16,856
Cyber attacks on
businesses each year

500 million
Yahoo user
accounts hacked

$2.1 trillion
Predicted global cost of data breaches by 2019

$74 billion
Current annual spending on
cybersecurity

▶

$1 trillion+
Predicted global spending on
cybersecurity 2017-2021

AGC New York, "Keeping Your Transactions Safe"

Doing Business in the Digital Age

What is the Internet of Things?

The Internet of Things (IoT) by other names:

- Industry 4.0
- M2M (machine to machine)
- Connected Enterprise

Network of physical objects or "things" embedded with smart electronics, sensors, controls or software that allow them to collect data, communicate and react to data.

The IoT is moving from smart objects to smart locations/plants to smart companies to smart grids to smart cities.

If this is all new to you… you're not alone!

The Four Forces Driving IoT

Cloud Computing

Sensors

Data Analytics

Expanded Internet Connectivity

IoT Offers Fortune and Fear

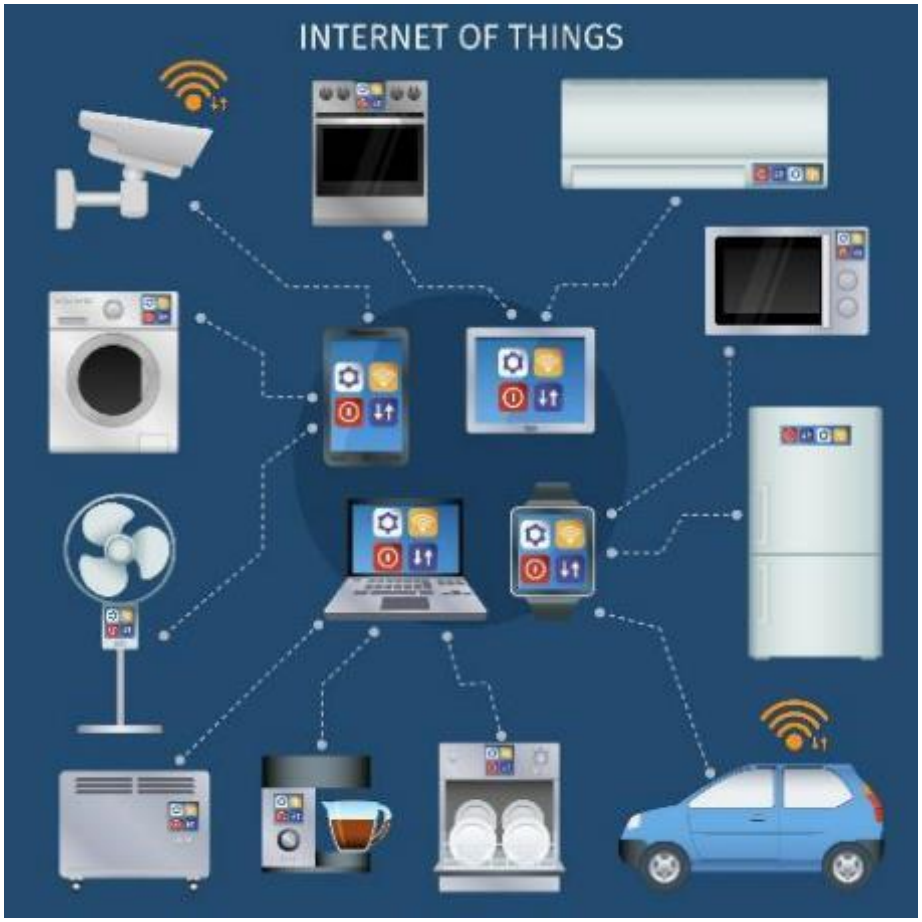
Fortune

- Add value to existing products
- Create new products designed for IoT
- Automate processes in plants and offices

Fear

- Potential security breaches
- Invasion of privacy
- Growth of electronics waste

IoT in Practice



Security Concerns Related to IoT

Current known security concerns relate to:

- Security of the device itself
- Risk to enterprise systems

Security challenges difficult for IoT devices:

- Companies making IoT devices, particularly with wearables, have inadequate experience in dealing with security issues
  - Not dominated by large tech companies as in computer market
  - Designed instead by companies in various industries, from fashion to home goods where security is an afterthought
- Inexpensive nature of most IoT devices - economically impractical to provide security patches or notification upon discovery of vulnerability after the sale
- Typically utilize unencrypted means to transmit information

Understanding Your Risk

Risk Overview

ASSETS

Processes, Information, and Systems with varying degrees of value to the organization

THREATS

Actors that are motivated to attack or misuse your assets

VULNERABILITIES

Flaws, control weaknesses or exposures of an asset to compromise

Digital Assets Valuation

Three Principles of Digital Asset Valuation

1. Consider **who gets value** from the asset
2. Understand the role your digital assets play in **creating economic value / generating revenue**
3. **Look forward** – valuing your digital assets requires an outward view (previously invested costs to create the asset are "sunk")

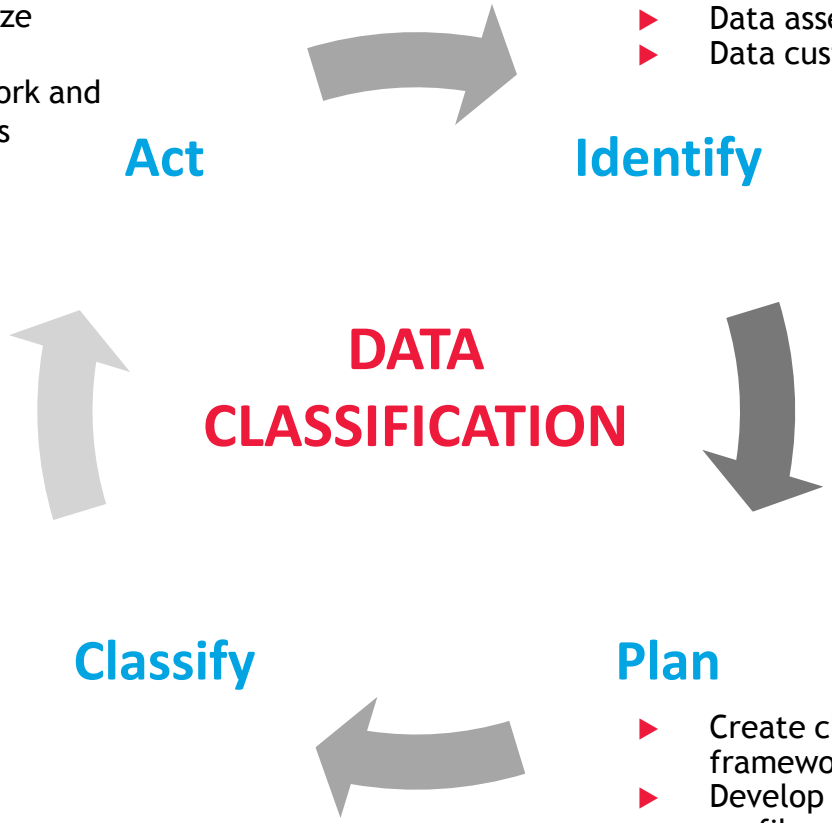
Understanding the Value of Digital Assets

- **Intrinsic** – Critical element that allows the digital asset to exist in the first place (e.g. the person, binary data, physical object, legal contract etc.)
- **Extrinsic** – Opportunities to leverage the digital asset making it more useful to prospective users
- **Sum it up** – Metadata defines the extrinsic value of your digital assets, informing their value

Data Classification

- Review and analyze report(s)
- Readjust framework and re-classify data as needed

Act



Identify

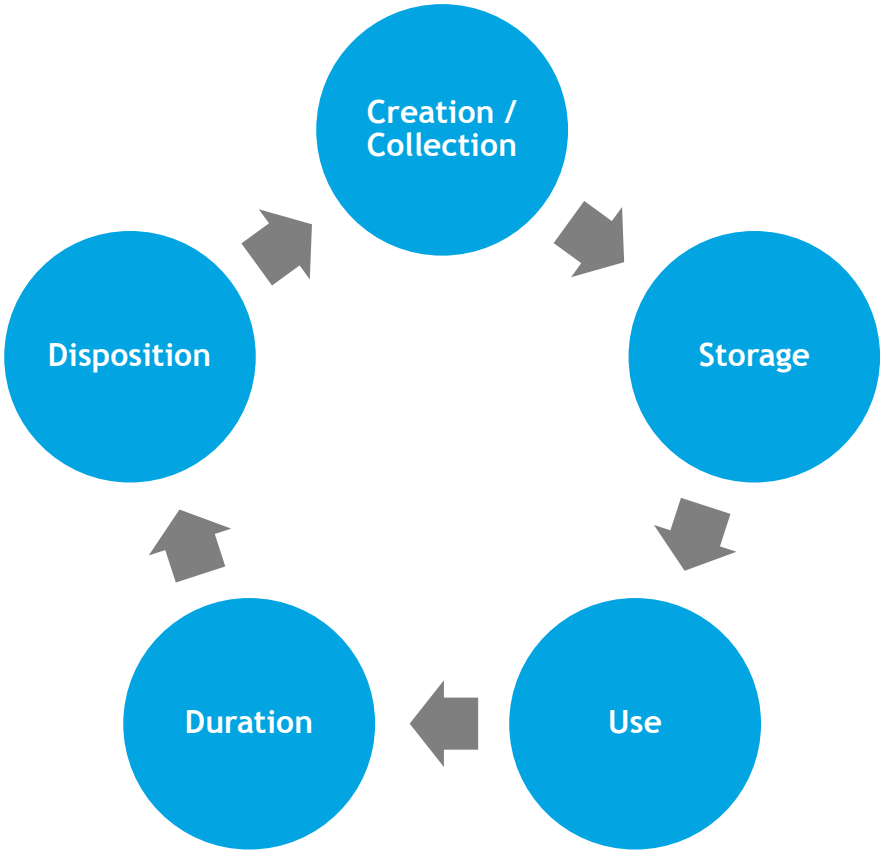
- Data assets
- Data custodians

Plan

- Create classification framework
- Develop protection profiles

Classify

Lifecycle of Data Privacy & Protection



Strategies to Minimize Risk

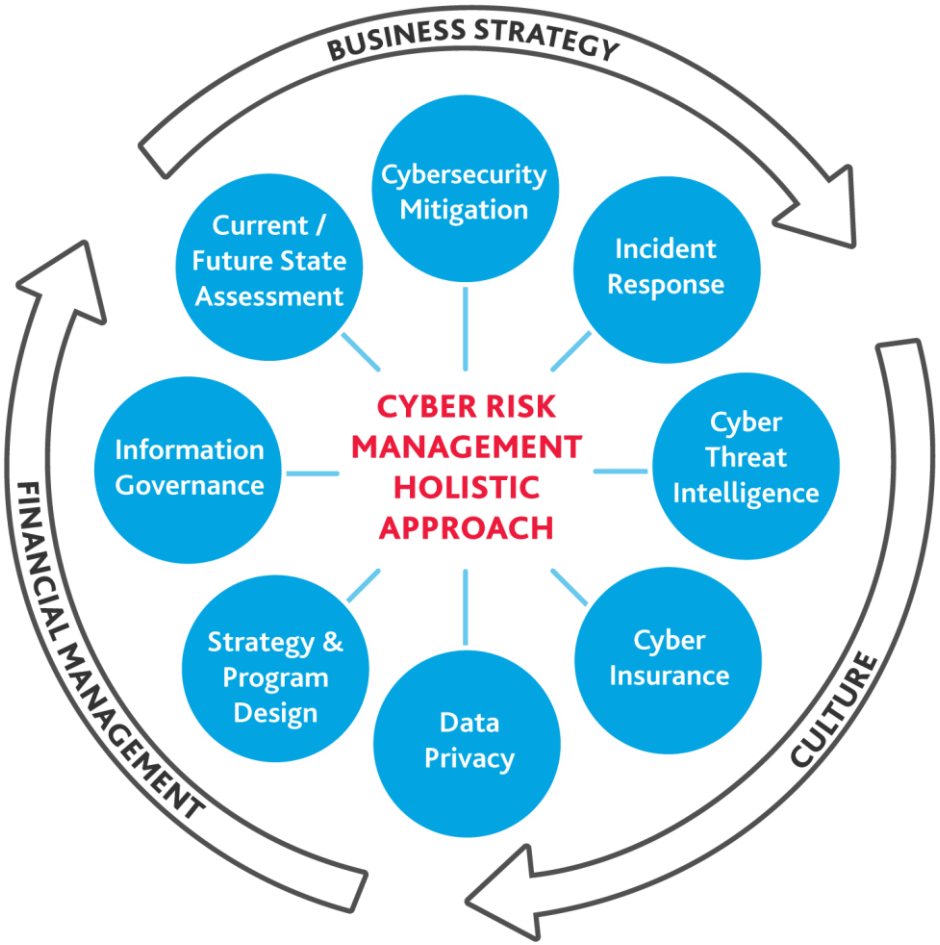
- Digital transformation
- Cloud strategy
- Context computing / Internet of Things
- Holistic view of a comprehensive Cybersecurity Risk Management Program
- Implementation of global and local security and privacy requirements

Cybersecurity Overview

What is a "Cybersecurity Risk Management Program"?

Cybersecurity is the process of designing, implementing and operating controls and other risk management activities to (a) protect information and systems from security events that could compromise the achievement of the entity's objectives and (b) to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented.

Cyber Risk Management Holistic Approach



BDO Cybersecurity Framework

Key Policy & Process Domains

- Data privacy / protection
- Identity & access management
- Threat & risk intelligence
- Third party / vendor management
- Incident response & planning
- Asset inventories
- Metrics / reporting
- Training / awareness

Cybersecurity Lifecycle

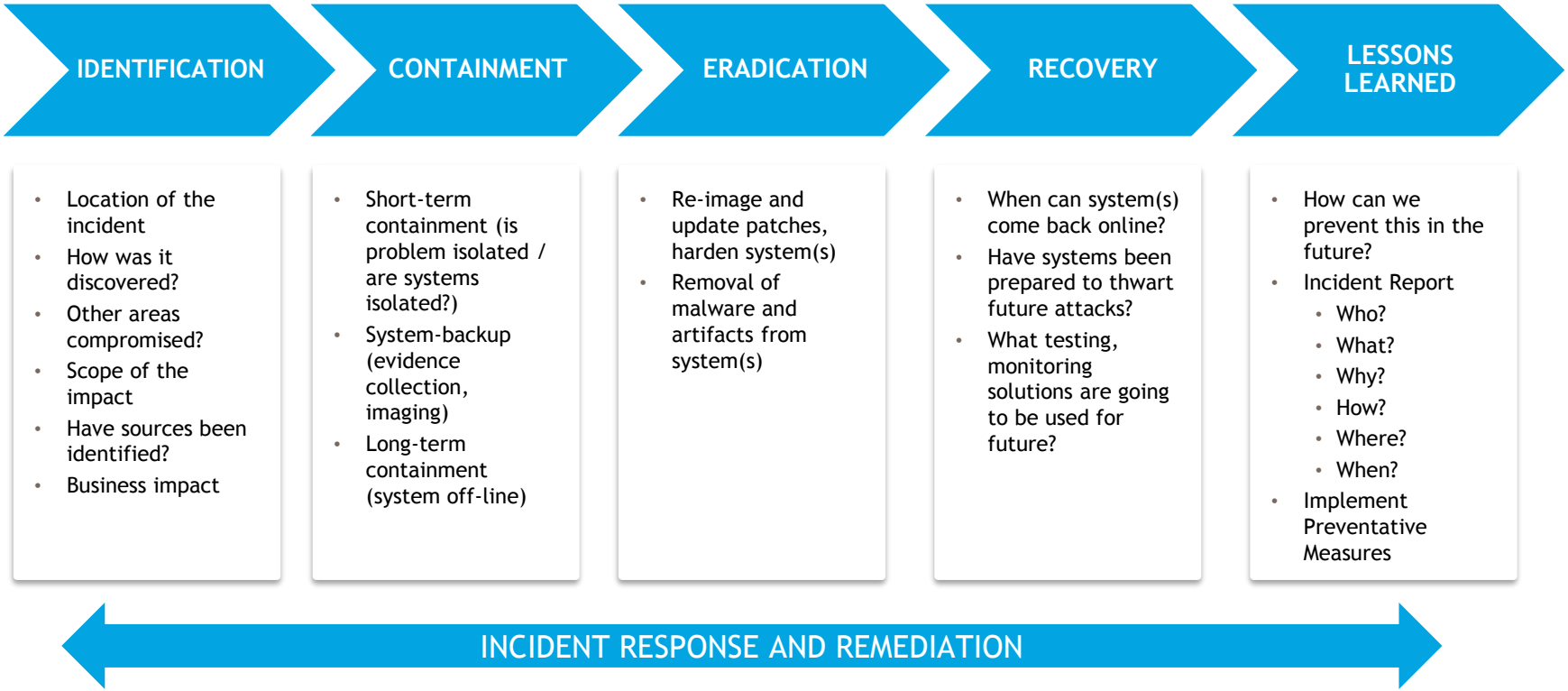
Governance & Strategy

- Cybersecurity risk profile management
- Cybersecurity risk management program
- Organization roles and responsibilities (Board of Directors, Executive Management, etc.)
- Investment optimization
- Legal & compliance
- Cyber insurance

Conferencia Anual Latinoamericana Sobre Delitos Financieros de la ACFCS
13-14 de Octubre, 2016 | Hard Rock Panamá Megapolis

BDO

Sample Approach to Incident Response/Cyber Investigations



Cyber Insurance

- What is “cyber insurance”?
- What it covers: legal fees, forensics/ investigation costs, response costs, crisis management/PR, business interruption, credit monitoring, extortion claims
- No standard form policies
- First wave of insurance coverage disputes
- Other types of available coverage
  - Older claims under GL
  - E&O/Professional Services
  - Crime
  - D&O

Threat Intelligence and Information Sharing

Private Sector Collaboration

Private Sector
Threat Information

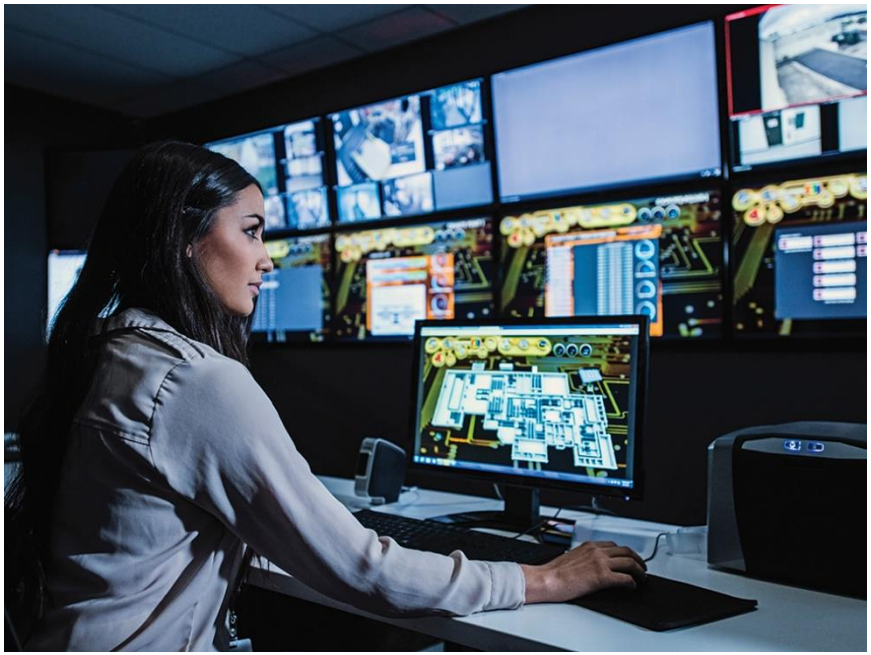
Government Classified and
Unclassified Evidence and
Intelligence

Cyber Threat
Intelligence

Information Sharing Channels

BDO's Cybersecurity Services

BDO's Cybersecurity Services



- Cyber Risk Management Strategy & Program Design
- Cyber Risk Assessment & Security Testing
- Data Privacy & Protection
- Security Architecture & Transformation
- Incident Response Planning
- Business Continuity Planning & Disaster Recovery
- Digital Forensics & Cyber Investigations
- Cyber Insurance Claim Preparation & Coverage Adequacy Evaluation

¿PREGUNTAS?