

# Cyber Risks on Natural Disasters

## Case: Huracán María



Eduardo Cardín, CISA, CISM

Eduardo@CardinPR.com

787.444.1166

# Cyber exposure is growing as Organizations are becoming more dependent on technology

Business  
Goals

- Used to enable business initiatives
- Critical dependence of many business processes on information technology
- Has moved from providing largely back-office support to becoming the prime facilitator and enabler of the total business

Risks

- Are vulnerable to a variety of risks

# María Hurricane Impact



# María Hurricane Impact

Business Continuity

Information Assets  
Protection

María Hurricane  
Impact

Business Continuity

## Scenario of Main Threats

No availability or destruction of locations /  
facilities

Failures of electricity generation backup  
systems

Electricity and telecommunications not  
available

Limited fuel supply

Failure or destruction of equipment

Key personnel were not available for  
operations or could not be contacted

Failures or non-accessibility of critical  
systems

Third-party services not available

María Hurricane  
Impact

Information Assets Protection

## Scenario of Main Threats

Emergency changes  
being implemented  
without adequate  
security configuration

Temporary Internet services

Connected services

Routers, Access Points, Switches

María Hurricane  
Impact

Information Assets Protection

## Scenario of Main Threats

Allowing temporary /  
extraordinary access  
to the network

Other entities

Internet of Things devices

Unsecure remote access

Unchallenged wireless access to the  
network in the physical vicinity

María Hurricane  
Impact

Information Assets Protection

## Scenario of Main Threats

Rogue access points /  
devices not sanctioned

By employees

By third party / provider

By nearby entities



María Hurricane  
Impact

Information Assets Protection

## Scenario of Main Threats

Cyber scams  
(new and recycled  
scams)

eMail Spoofing

Malicious phishing emails

Links to malicious websites

María Hurricane  
Impact

Information Assets Protection

## Scenario of Main Threats

Poor data management  
practices

Poor data retention, transmission  
and disposal practices

Hurricane literally blew away  
sensitive personal information

María Hurricane  
Impact

Information Assets Protection

## Scenario of Main Threats

## Planning Issues

Lack of disaster preparedness

Lack of Disaster Recovery Plans tests

Lack of incident response plans

# The perfect storm:

## Cyber-Attacks During Natural Disasters

- When a natural disaster hits, surges in cybercrime may rise.
- When disasters hit, people immediately shifted away

SECURITY MODE



SURVIVAL MODE



# The perfect storm:

## Cyber-Attacks During Natural Disasters

- When a natural disaster hits, surges in cybercrime may rise.
- When disasters hit, people immediately shifted away from **security mode** into **survival mode**.
- When physical assets have been compromised, IT staff priority is business continuity—times like that make cyber assets easy prey for an attacker. After a disaster strikes cyber attackers are likely to make their move when a company's IT staff and resources are consumed in post-incident recovery.

# Natural Disasters are Magnets for Cyber Criminals

eMail scams

Push malicious websites to the  
top of search results

Break into business data while  
people work remotely

# Course of Action

Natural Disasters

Business Continuity

Contingency Planning

Disruption

Coordinated Strategy

Plans

Procedures

Technical Measures

Enable the Recovery

Information Systems

Data

Operations

# Course of Action

Natural Disasters

Business Continuity

Business Continuity Planning

Disaster Recovery Planning

**Purpose**

Provides procedures for sustaining mission/business operations while recovering from a significant disruption.

Provides procedures and capabilities for recovering information systems.

**Scope**

Addresses mission/business processes

Addresses information systems recovery



# Contingency Planning Process

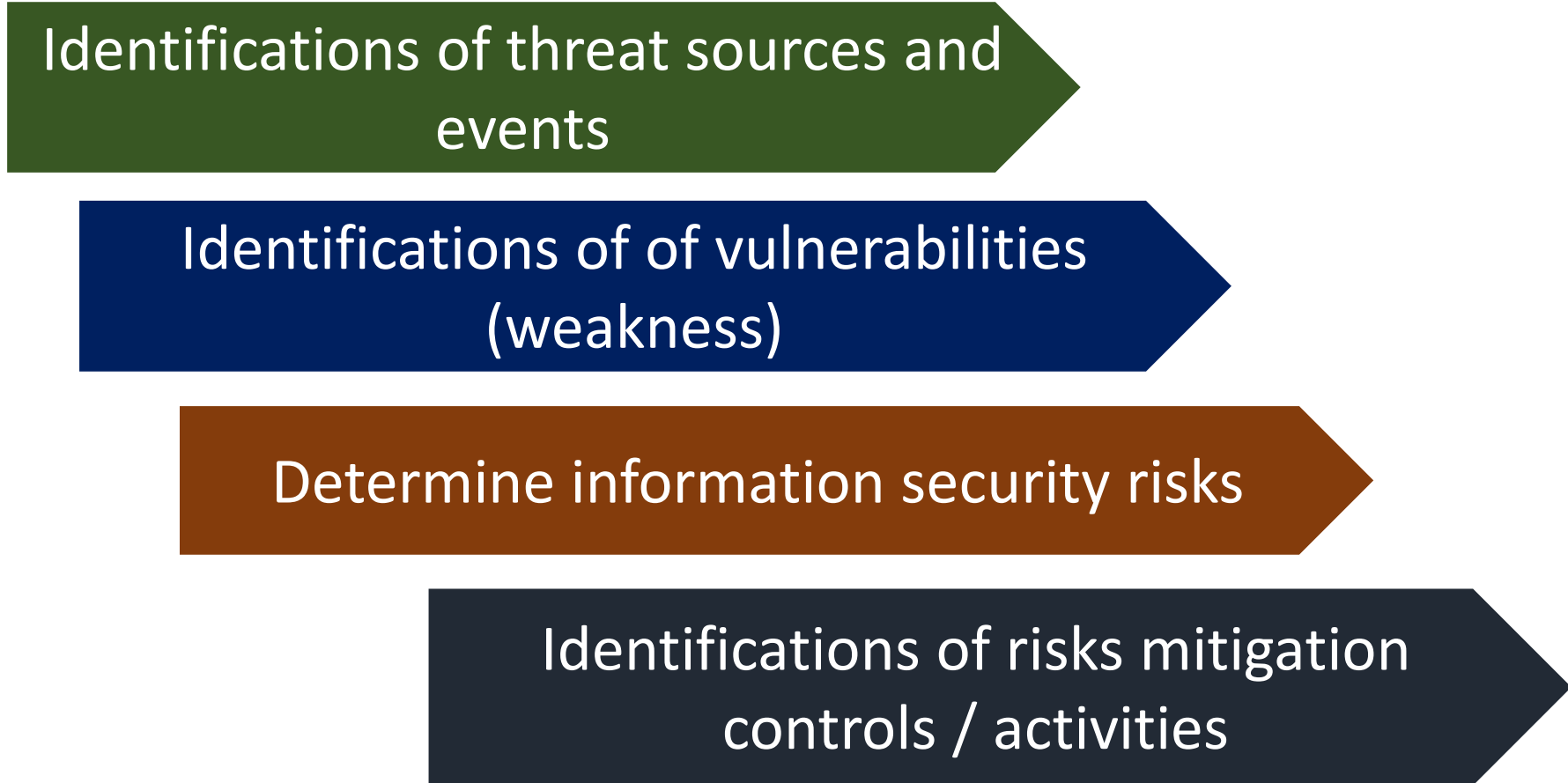
Develop Contingency Planning Policy	Conduct Business Impact Analysis	Identify Preventive Controls	Create Contingency Strategies	Develop Contingency Planning	Plan Testing, Training, and Exercises	Plan Maintenance
<p>Identify statutory or regulatory requirements</p> <p>Develop contingency planning policy statement</p> <p>Publish policy</p>	<p>Determine business processes and recovery criticality</p> <p>Identify outage impacts and estimated downtime</p> <p>Identify recovery priorities</p>	<p>Identify controls</p> <p>Implement controls</p> <p>Maintain controls</p>	<p>Mitigate the risks arising from use of information systems in the execution of mission/business processes</p>	<p>Business continuity planning</p> <p>Disaster recovery planning</p>	<p>Plans testing</p> <p>Train personnel</p> <p>Plans exercises</p>	<p>Review and update plans</p> <p>Document changes</p>



# Course of Action



## Risk Assessment



# Course of Action

Natural  
Disasters

Information Assets Protection

## Threats

Emergency changes  
being implemented  
without adequate  
security configuration

## Controls

Change Management

Configuration Management

# Course of Action

Natural  
Disasters

Information Assets Protection

## Threats

Allowing temporary /  
extraordinary access  
to the network

## Controls

Logical and physical security controls  
over IT assets in the following layers

Networks

Applications

Platforms (OS)

Databases

Network Access Control (NAC) tools

# Course of Action

Natural  
Disasters

Information Assets Protection

## Threats

Rogue access points /  
devices not sanctioned

## Controls

Network Access Control (NAC)  
tools to implement policies for  
controlling devices and user  
access to the network

# Course of Action

Natural  
Disasters

Information Assets Protection

## Threats

Cyber scams  
(new and recycled  
scams)

## Controls

Periodic personnel information  
security awareness



**RESPONSIBILITY**

No single drop of water thinks it is  
responsible for the flood.

# Course of Action

Natural  
Disasters

Information Assets Protection

## Threats

Cyber scams  
(new and recycled  
scams)

## Controls

Periodic personnel information  
security awareness

eMail / Spam filtering

Domain-based Message  
Authentication Reporting and  
Conformance (DMARC)  
Implementation

# Course of Action

Natural  
Disasters

Information Assets Protection

## Threats

Poor data management  
practices

## Controls

Strong cryptography and security  
protocols

Data retention and disposal  
controls

Physical security controls for  
sensitive personal information



# Course of Action

Natural  
Disasters

Information Assets Protection

**Threats**

**Controls**

Planning Issues

Contingency Planning

What critical operational or security controls require implementation prior to recovery?

Determine threats and vulnerabilities to the organization's contingency planning process.

- Technological and security vulnerabilities;
- Internally identified threats; and
- Externally identified threats

# Course of Action

Natural  
Disasters

Information Assets Protection

**Threats**

**Controls**

Planning Issues

Incident Response Planning

In the event of a security incident, management must decide how to properly protect information systems and confidential data while also maintaining business continuity.

# Thank you!



Eduardo Cardín, CISA, CISM

Eduardo@CardinPR.com

787.444.1166