Incident Response Training

North Central Texas Council of Governments

Incident Response Training

Part 3 –

Communication and Reporting

Agenda

1. Third Party Communication during IR
2. Regulatory requirements
3. The Media
4. Clients and Customers
5. Tracking, Reporting and KPIs

Agenda

1. **Third Party Communication during IR**
2. Regulatory requirements
3. The Media
4. Clients and Customers
5. Tracking, Reporting and KPIs

Third Party Communication

Important is to have a plan for the:

- **How**
- **When**
- **Why**
- **What**
- **Who** and
- **Security and Privacy**

Other Incident Response Teams

For Reporting Purposes:

- Internet Service Providers
- Software Vendors
- Incident Response Teams (TX DIR, US-CERT, GFIRST)
- Affected External Parties

For Collaboration and Information Sharing:

Issues to address:

- Incident Coordination (incident commander, centralized IR team, established processes)
- Sharing agreements (contracts, NDAs etc.)
- Information sharing Techniques (automated, secure email)
- Technical information (network designs, IP addresses, logs)

Agenda

1. Third Party Communication during IR
2. **Regulatory requirements**
3. The Media
4. Clients and Customers
5. Tracking, Reporting and KPIs

Regulatory Requirements

- Personal Identifiable Information (PII)
- PCI-DSS (Credit Cards)
- HIPAA (Healthcare)
- Annual Risk Assessments and Audits
- Breach Notifications
- Disaster Recovery Testing

Microsoft Word Document

Agenda

1. Third Party Communication during IR
2. Regulatory requirements
3. **The Media**
4. Clients and Customers
5. Tracking, Reporting and KPIs

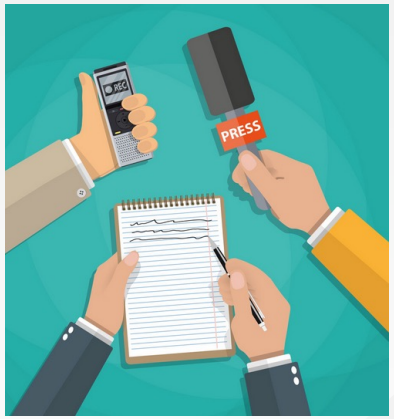
Media Reporting

Know:

- Who is authorized to report
- What can be reported
- How to report it

For larger incidents:

- Media releases with other CERTs/vendors, etc.
- Integration with Federal Support and Public Affairs



Microsoft Word Document

Agenda

1. Third Party Communication during IR
2. Regulatory requirements
3. The Media
4. **Clients and Customers**
5. Tracking, Reporting and KPIs

Customer Reporting

Know:

- Who is authorized to report
- What can be reported
- How to report it

Note: Refer to *Regulatory Notification Requirements*

Statement Tips:

- Check the script examples
- Honesty – admit and express regret if needed
- Context – broadening context to isolate incident (e.g., negative incident is “very rare”)
- Framing Effect – use positive statements
- Partnerships – no blame, focus on collaboration
- Action –being passive will not help
- Positives – pointing out positive areas/success
- Express Empathy
- Be Concise
- Statement – avoid confrontation

Microsoft Word Document

Assigned Responsibilities

This matrix provides a guideline that highlights the responsibility for communicating status and decisions during the response to an incident.

Personnel	VP	Senior Leaders	Response Mgmt.	Extended Support BALs, Legal, Partners	Directors	Depts.	Media	Clients	Enterprise
Incident Commander	P / B		A / B, V, E	P / B, V, E	P / V, E				
CIRT			P / B, V, E	A / B, V, E	A / V, E	A / B, V, E			
Communication							P / B, V, E	P / B, V, E	
IT Management/CTO/CEO/CISO		P / B, V, E				P / B, V, E			P / B, V, E

Responsibility	Type	
P = Primary Responsibility A = Alternate Responsibility	B = Briefing E = Email V = Voice Mail	Communication frequency shall be established based on the nature of the incident and SLAs.

Agenda

1. Third Party Communication during IR
2. Regulatory requirements
3. The Media
4. Clients and Customers
5. **Tracking, Reporting and KPIs**

Tracking, Reporting and KPIs

Why:

- Improvement in IR
- Remediation of Risks
- Targeted training
- Identification of most vulnerable systems
- Budget and resource planning
- Decrease in Cyber Insurance

IR Metrics		
Category	Measurement	Description
SLAs	# SLA adherence	Total percentage of incidents where SLAs were adhered to
Incidents	# Total Incidents / Year	Total amount of incidents responded to per year
	# Incidents by Type / Year	Total number of incidents by category responded to per year
Time	# Personnel Hours / Incident	Total amount of labor spent resolving incident
	# Days / Incident	Total amount of days spent resolving incident
	# System Down-Time Hours / Incident	Total hours of system down-time until incident resolved
Cost	Estimated Monetary Cost / Incident	Estimated total monetary cost per incidence, including containment, eradication, and recovery, as well as data collecting and analysis (this may include labor costs, external entity assistance, tool procurements, travel, etc.)
Damage	# Systems Affected / Incident	Total number of systems affected per incident
	# Records Compromised / Incident	Total number of records compromised per incident
Forensics	# Total Forensics Leveraged Incidents / Year	Total number of incidents requiring forensics (collection & analysis) per year
	# System Images Analyzed / Incident	Total number of system images analyzed per incident
	# System Memory Dumps Examined / Incident	Total number of system physical memory dumps examined per incident

Microsoft Word Document

Questions?

Where to find documents and information?

https://nctcog.org/ep/resources/cyber-security-incident-response-planning-system

THANK YOU

HQ – ARLINGTON, VIRGINIA

4601 North Fairfax Drive, Suite 1200
Arlington, VA 22203

OFFICE LOCATIONS

Las Vegas, Nevada

London, England

Dubai, United Arab Emirates

Bratislava, Slovakia

www.stealth-iss.com