



Industry Consortium for Advancement of Security on the Internet

# Managing a Global Industry Unified Security Incident Response Program

*Case Study and Lessons Learned*

# Agenda

- Background
- ICASI's Unified Incident Response Process
- Case Studies
- Lessons Learned
- Q&A



## What Is ICASI?

- Non-profit organization founded by industry-leading global vendors dedicated to improving incident response
- Relatively small organization that thrives on relationships of trust and collaboration (5-10 core members)
- Members work together using an innovated approach to improve response procedures across the ecosystem

# Assessing the Threat Landscape

- **Situation**

- Vulnerabilities and exploits are commoditized by a lucrative, highly profitable, and sophisticated underground economy
- Threats are becoming more complex and future exploits may simultaneously target multiple vendors

- **Challenges**

- Currently government-based SIRTs, FIRST, and other incident-related response forums are not structured to coordinate complex multi-vendor vulnerabilities and lack the intellectual property to fully participate or action a solution
- Industry lacked an agile and innovative multi-vendor response mechanism capable of collectively responding to global public/private sector customers outside of ICASI



## What Is the USIRP?

The Unified Security Incident Response Plan is a process designed to facilitate *Joint* collaboration amongst Members' SIRTs under certain conditions.

The USIRP is not meant to replace members' individual SIRTs; rather, it provides:

- **A process** that enables ICASI members to securely and effectively address range of multi-vendor threats
- **Overlays and runs in parallel** to current vendors response processes
- **Customization** to cover each of three major categories
  - **Vulnerabilities** – which may take weeks to months to resolve
  - **Incidents that impact 3 or more members** – urgent/emergent
  - **Strategic response (persistent problems)** – ongoing or long-term

# Laying the Foundation

## Framework of Trust

- Strong Multi-lateral NDA's between Members
- Track Record of maintaining confidentiality
- Secure Communications



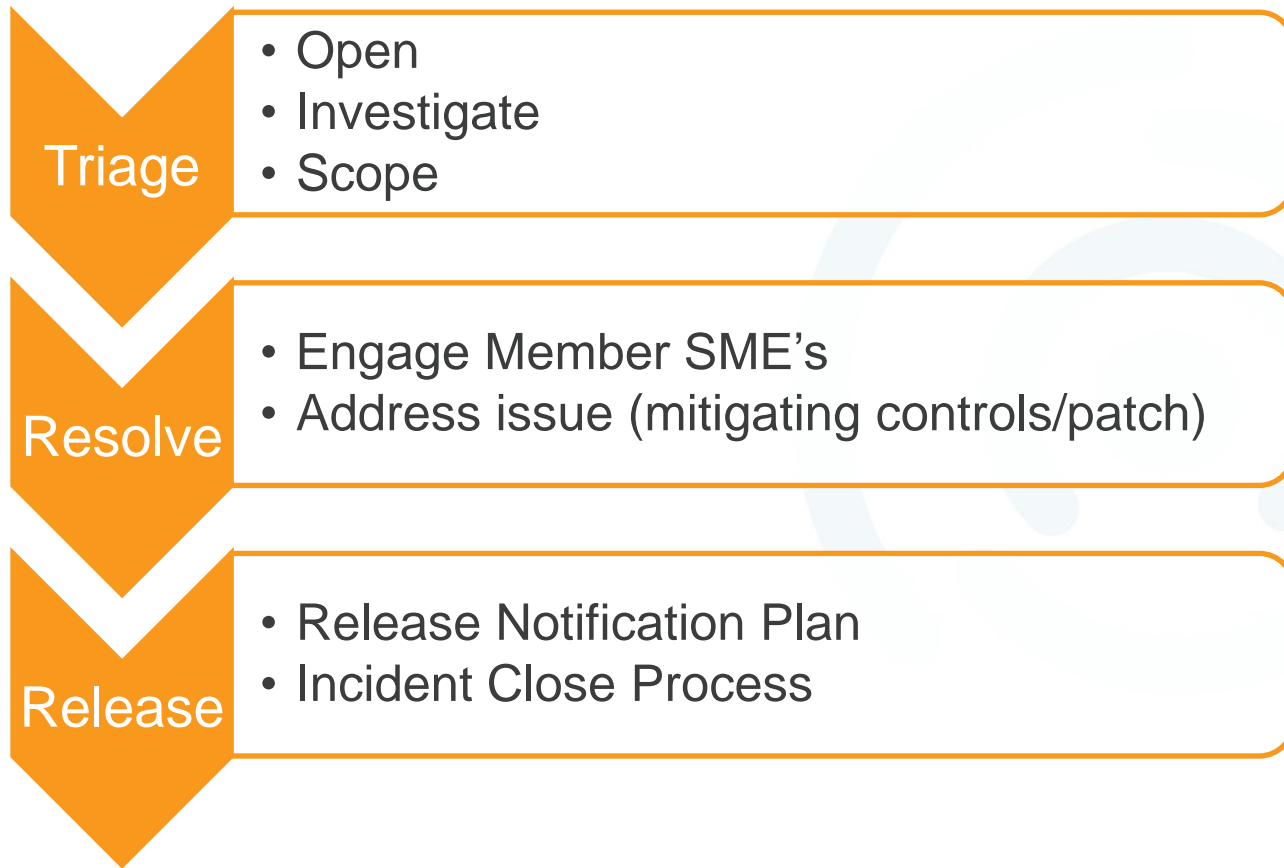
## Defined Process and Protocol

- Established and documented common response process
- Response plans are exercised
- Support groups (PR/Legal/etc) pre-defined

## Organizational Commitment

- Senior Leadership of Member SIRTs committed
- Technical Leads of Member SIRTs engaged

# USIRP Incident Process Abstract



# Triage

## Triggering an Event

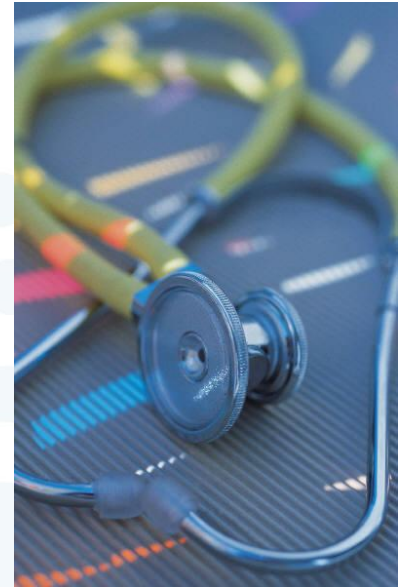
- Variety of Sources
- Thresholds

## Investigate and Verify

- Technical Verification of Vulnerability
- Survey of potential impacts to products or services

## Define Your Scope

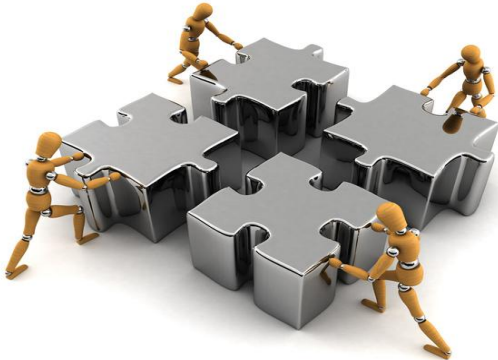
- What problem/issue is to be resolved?
- What products/services are impacted?
- Who should be involved in USIRP response?



# Resolving the Issue

## Work Best and Worst Case

- Level set on upper and lower bound of solutions sets and timelines
- Err on the side of over communicating
- Prepare for leaks



## Run Parallel Work Streams

Run Legal, Communications work streams in parallel to technical work streams

## Expand your Trust Circle as Needed

You may need to pull in other stakeholders or SME's to work the issue.

# Releasing the Solution

Communications and PR

Unified versus Individual  
Messaging

Coordination with Global SIRTs

Reaching Critical Infrastructure  
Owners and Operators



# Case Study A

- Protocol-level Vulnerability reported by researcher
- ICASI Triage Issue
  - ICASI Response Team Members meet with researcher for technical dialogue
  - ICASI Members meet to discuss impacted products/services
- USIRP Triggered
  - Member Company SME's meet to discuss venues to work temporary and permanent solution. (patch the vuln/update the protocol spec)
  - Establish dialogue with researcher related to public release timing
  - Ongoing collaborative work to coordinate release timelines
- Researcher Goes Public w/o ICASI Coordination

## Case Study B

- ICASI Member reports pervasive vulnerability
- ICASI Triage Issue
  - ICASI Response Team Members meet for technical dialogue and discuss impacted products/services
- USIRP Triggered
  - Member Company SME's meet to discuss venues to work temporary and permanent solution.
  - Timeline dictated by planned publicity of researcher
  - Ongoing collaborative work to coordinate release timelines
- ICASI provides briefing to SIRTs/CI Community coinciding with public disclosure of vulnerability

## Lessons Learned

- ✓ Trust is an investment – the foundation must be laid before the incident occurs
- ✓ Coordinating incident response across multiple companies globally is inherently difficult
- ✓ Keep it simple
- ✓ Continuous communication between Members and leadership is key.
- ✓ Build flexible capabilities that can be morphed to meet the next incident requirements

# Q&A



