Using Cybersecurity Metrics to Inform Stakeholders
Why Present Cybersecurity Metrics?

- Provide updates on cybersecurity program risks and vulnerabilities
- Set and manage expectations
- Determine where to direct resources
- Plan your strategy and develop organizational roadmaps
- Create a security awareness organizational culture
Initial Internal Questions

• **Initial Questions to Ask Before Collecting Metrics**
  – What is the goal?
    • Show activities we are performing well
    • Show areas for improvement
    • Show comparisons to similar organizations
  – What should I measure to help my organization do better?
  – What will the audience find most relevant?
  – How should data and information be presented?
Evaluate How to Measure Activities

• Measuring can be time based or “snapshots”.
  • Time-Series: Provides insight over a period, such as a week or month
  • Snapshot: Provide insight at a specific time or summary of total events in a period
Knowing Your Audience

• According to Gartner, there are two stakeholder groups for security metrics:
  – Security Managers & Practitioners (Operations)
    • Tasked with operating security controls and procedures
  – Business Stakeholders (Management)
    • Tasked with budgets and resources needed to meet risk management and business goals

• The guidance in this document can be used for either Operations or Management groups

• Local level organizations will likely have different environments to present metrics, compared to state level organizations.
  – Example: A county contact presenting to a local Board of Supervisors
    • Evaluate the audience, and tailor the messaging for them.
Presentation Tips

• Utilize actionable summaries and avoid overly specific technical language
• Keep the presentation and summaries concise
• Utilize past success stories
  – Provide examples of risks averted after certain processes or capabilities were previously implemented
• Discuss the organizational risks if resources or processes are not implemented
  – Financial Risk, Reputation Loss
Presentation Tips

• Review and discuss potential risks of not addressing current gap or weakness areas
  – Examples:
    • “Risk of Exposure” or “Risk of Being in the News”
      – Utilize past real world examples
    • Evaluate tying the risk to the average cost of a breach
    • Review the potential work loss that could occur, as well as the impact on public safety and critical infrastructure processes
Examples of Activity Areas to Present

- **What Activity Areas Should be Emphasized?**
  - Preventative Controls
    - Example Areas: Anti-Malware, Vulnerability Scanning
  - Detective Controls
    - Example Areas: Security Information & Event Management (SIEM)
  - Processes
    - Example Areas: Updates to User Education, Incident Detection & Response Times, Patching Activity, Risk Assessment Results (NCSR)
Activity Examples

• **Potential Activities of Focus:**
  – Security Training Stats
  – Phishing Exercises & Testing Results
  – Patching Activity & Current Status
  – Anti-Malware Activity
  – Vulnerability Scanning Activity
  – Disaster Recovery Capability to Return to Business Operations
  – NCSR Assessment Results of Your Overall Cybersecurity Program
During the week of 10/11, a total of 11,590 malicious DNS requests were blocked out of 27,464,799 requests, which accounts to less than 1% of all activity.

DNS Activity by Day

- 10/11
- 10/12
- 10/13
- 10/14
- 10/15
- 10/16
- 10/17
Visual Example: Malicious Domain Blocking

Blocked Malicious Domains by Threat Category

Blocked Malicious Domains by Severity

Confidential & Proprietary
Visual Example: Cyber Program Assessment Results

Where Are We Today?

Current NCSR Results:

- Our organization is scoring best within Protect and Recover.
- Improvements can be made in Identify, Detect, and Recover.
- Action Item: Increase Identify score to a 3.00 within 1-2 years.

Visual Example: Vulnerability Management Data

Vulnerability Findings

- High: 6,845
- Medium: 10,495
- Low: 8,732
- No Vulnerabilities: 1,896
Potential Pitfalls

- Inappropriate focus of resources on the wrong priorities
- Excessive expenditure on measuring rather than doing
- Investments in controls and processes that don’t have a relevance to the business priorities
- Overambitious targets
- Under ambitious targets being met and leading to a false sense of security
- Poor communication of outcomes leading to misinterpretation and poor responses
- Lack of transparency leading to lack of trust
Multi-State Information Sharing & Analysis Center (MS-ISAC)

Contact: NCSR@cisecurity.org