Security Metrics: Can They Be Effectively Measured Across The Enterprise?

SESSION ID: CISO-W01

Moderator: Alan Shimel
Managing Partner, The CISO Group
CEO, DevOps.com

Panelists: Jody Brazil
President, CTO Firemon

Ivana Cojbasic
VP Security FIS

Andrew McCullough
ESS Expert Hewlett Packard Enterprise
Security Services
Lies, Damn Lies and Metrics

- We can measure just about anything that we seek to.
- We can use resulting metrics to show us many different things.
- Just because we can measure something doesn’t mean we should!
- So, which metrics are truly meaningful and to whom should we show them?

Everything that can be counted does not necessarily count; everything that counts cannot necessarily be counted.

- Albert Einstein

www.quotesworthrepeating.com
What Metrics to Measure
Meaningful Security Metrics?

- The Value of Good Metrics
  - Convey a Clear Picture (Point-in-Time or Historically)
  - Signify Valuable & Actionable Information
  - Provide Support for Business Objective(s)
The *Usual Suspects*…

The *Hard Questions*…

- How can Security Effectively Communicate to the Company and Executive Stakeholders?
- Where does Security have a ‘Real’ relation and potential to Impact the Business Objectives?
- Are we aligning the Information Security Program Objectives to the Business Needs?

The *Easy Answers*…. 

- Demonstrate Effective Management of Prioritized Risks
- Provide a picture of how Business Critical Assets are Impacted
- Provide Accountability for Decisions and help to Justify Security Spend
Metrics that Matter

Stakeholders define objectives, processes, assets, and linkages

Security identifies risk component linkages, finds data sources and sets data connectors

- Effect on business processes
- Effect on business assets
- Security risk component (incident, threat and vulnerability) information layer

- Compliance data
- Financial data
- Resource data
- Incident data
- Vulnerability data
- Threat data

Effect on business 1 objectives
Effect on business 2 objectives
Effect on business 3 objectives
Effect on business 4 objectives
What Metrics Matter to Others
C-Levels and Board Members

- Current State of Security
- Current Risk Posture and Changes Over Time
  - (Previous 4 Quarters at Minimum)
- Security Initiative Performance
- Regulatory Compliance Reports/Updates
  - (PCI DSS, SSAE16, FFIEC, HIPPA, FISMA)
- Benchmark Reports
- Budget Performance
Management Metrics

- Trend Analysis Data (Periodic), Security Posture Trends
- Vulnerability Management/Patch Reporting, Vulnerabilities By Severity Levels (High, Medium, Low, Informational), Emerging Network Threats
- Incident Response Times, Associates/Contractors That Have Completed Information Security Policy Training, Asset Criticality & Sensitivity,
- Total $ Invested in Security Initiatives and Current Status, Audit Compliance and Findings
- Total % of Systems Patched, % Compliance with Security Policies (Patch/Password/Vulnerability), % of Risk Accepted Threats
Engineers/Support Teams

- Detail info on Threats, Top/Emerging Exploits, Top Present Vulnerabilities, Top Source Attackers (Egress -> Ingress), Top Destinations Attacked (Egress -> Ingress), Top Source Attackers (Ingress -> Egress), Top Destinations Attacked (Ingress -> Egress)

- Potential Virus Outbreaks, # Accounts Created (Unix and Windows), Accounts Deleted (Unix and Windows), # Successful / Failed Logins, # Incidents Investigated, # Failed Use of Privilege, # Files Accessed on Servers, # Security Event Logs, # Severe Security Events, % Time Devices Were Actively Logging by Day, Type and Severity of Security Incidents, Analyzed vs. Validated Incidents,

- Top 4 Devices by Log Activity, Vulnerability External (Highs/Mediums/Lows), Vulnerability Internal (Highs/Mediums/Lows),

- # Potential Malware Infected Clients (IPs), # Requests to Malware sites, # Blocked Requests to Known Malware Sites, % Servers Patched to Current Patch Level, % Servers Patched w/All Service Packs, AntiVirus Workstation, AntiVirus Server, Availability Security Hardware/Services

- # Accounts Inactive ( => 90 <120), # Accounts w/Passwords That Can't Be Changed, # Accounts Inactive ( > 120), # Accounts w/Non-Expiring Passwords, # Locked Out Accounts, # Disable Accounts, # Rogue Aps, SPAM Email
What Matters to Jody as President and a Security Person
What’s wrong with security metrics?

- There is No Industry Agreement on What to Measure
  - Where is the MBA of Security?
- We Measure the Wrong Things
  - We tend to Measure Our “Successes”.
    - Drop logs, IPS Block Events, Failed Logins
- We Measure What We Can’t Control
  - Threats
  - Vulnerabilities
New Ponemon Metrics Survey – Initial Results

- Over half of all organizations surveyed only report to senior management on security risk when there is serious issue, or never at all!
- > 50% feel that current metrics provide limited value for:
  - Security change
  - IT risk
  - Threat prevention
  - Effectiveness of people/process/tech
- 69% feel current metrics do not align with business objectives
Measure Security Posture

Don’t just measure what’s happening or has happened. **Measure current security posture of what you can control.**
Measure Your Failures

Measure incidents. By **Severity**, **Policy** and **Category**. Trend your incidents.
What You Should Take Away
As Soon As You Get Back (0-3 Months)

- Like Ivana did, decide which things you want to measure and report and to which audience (just because you can, doesn’t mean you should)
- Meet with various constituents and understand what intelligence is most important to them
- Assess what your current capabilities to measure are
- What tools, services and solutions are you lacking to measure what you need?
Where You Should Be In 6-12 Months

- Practical security metrics program in place
- Delivering whatever intelligence you can now
- Budgeting and implementation approved for solutions
- Quarterly feedback from various teams on metrics
  - Meaningful enough for them?
  - What else they need?
  - What they don’t need.
Questions?
Metrics Can Be Your Best Friend

Contact: ashimmy@devops.com