ASIS NY

April 28, 2016

Security Metrics: Communicating Value to the C-Suite

Session 2104

Richard Weaver
Chief Security Officer
Johns Hopkins Applied
Physics Laboratory

Peter Ohlhausen
President
Ohlhausen Research, Inc.

DEFENSE AND
INTELLIGENCE
COUNCIL

Background on Metrics Research

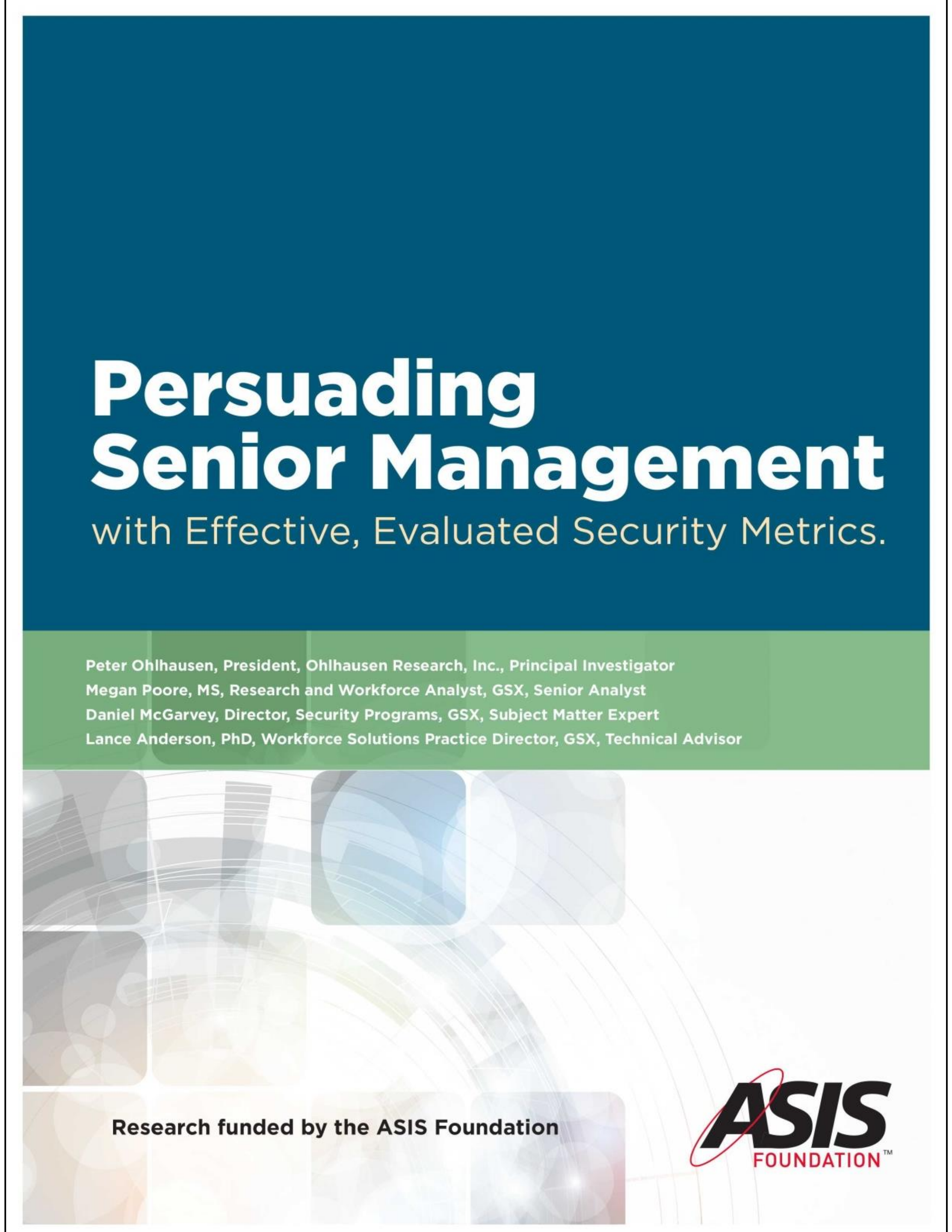
Persuading Senior Management with Effective, Evaluated Security Metrics (2014)

- **Nine criteria for evaluating metrics**

  Technical: Reliability, Validity, Generalizability
  Operational: Cost, Timeliness, Manipulation
  Strategic: ROI, Organizational Relevance, Communication

- **Library of evaluated metrics**

  Please contribute your metric at
  https://www.surveymonkey.com/r/metrics-survey



Persuading Senior Management

with Effective, Evaluated Security Metrics.

Peter Ohlhausen, President, Ohlhausen Research, Inc., Principal Investigator
Megan Poore, MS, Research and Workforce Analyst, GSX, Senior Analyst
Daniel McGarvey, Director, Security Programs, GSX, Subject Matter Expert
Lance Anderson, PhD, Workforce Solutions Practice Director, GSX, Technical Advisor

Research funded by the ASIS Foundation

Strategic Criteria

ROI

Communication

Organizational Relevance

Return on Investment

Extent to which the metric can be used to demonstrate cost savings or loss prevention in relation to relevant security spending.

The causal relation between the security measure and the benefits gained is **not clear**; the cost of the security measure is **hard to isolate**; the benefits of the security measure are **hard to calculate**; the security action being measured has **negative consequences** that are significant but not measureable.		The metric **theoretically** captures the benefits of a security action in relation to the costs of the measure; however, it is **sometimes** difficult to measure the benefits, or it may **sometimes** be difficult to isolate the cost of the security actions.		The metric **very clearly** shows the relation between a security action, policy, or system and the benefits or returns it provides; both the benefits and the costs **are readily measureable**, not vague or theoretical; the relation between the security measure and the benefit gained is **clear and direct**.
1	2	3	4	5

Return on Investment

Question: Are our investigations worthwhile?

- **Metric:** Total cost of investigations compared to the value of money or property recovered.
- **Potentially very clear ROI.** If investigations cost $200,000 over a year but recover $300,000 in money or property, ROI is obvious. If investigations cost more than they recover, but have a preventive effect, this metric might score 2 or 3 because it does not obviously show ROI.

How can you make this a better metric?

Return on Investment

Find other ways to demonstrate ROI when the benefits cannot be quantified easily.

- Look for historical evidence suggesting that when fewer investigations were performed, losses were greater. The current net investigative loss ($100,000) may be small compared to prior-year losses from theft or other offenses.
- Attempt to quantify the benefit of reduced employee turnover—reduced because employees feel protected and defended when they are victimized at or around the workplace.
- Attempt to quantify potential legal penalties that were avoided through good investigations. E.g., fines or liability avoided by background investigations that screened out unsuitable job applicants.

Be creative!

Return on Investment

Question: Is the security officer presence in and around our urban corporate headquarters worthwhile?

- **Metrics:** # of security posts, # of hours worked, # of interactions with employees, and reduction in area crimes.
- **Oblique ROI.** The security officers are not recovering significant amounts of cash or materials.

How can you demonstrate a return on the substantial investment in security officer coverage?

Be creative.

Return on Investment

- If specific reductions in crimes can be measured, attempt to quantify the value of crimes prevented by the security officers' efforts.
  - Use objective data on the costs of various categories of crime.
  - Prevention of vandalism may have a clear ROI.
- Look for subjective returns on investment. Maybe spending on security officers increases employee satisfaction as measured by company surveys. Maybe such spending makes employees more willing to work downtown and improves the quality of the workforce.

Strategic Criteria

ROI

Communication

Organizational Relevance

Communication

Extent to which the metric, metric results, and metric value can be communicated easily, succinctly, and quickly to key stakeholders, especially senior management.

The metric and purpose of the metric are **difficult to explain** to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers); it is **difficult to explain** the value the metric will add to the organization; the results of the metric and implications of the results are difficult to explain.		The metric and purpose of the metric are **somewhat easy to explain** to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers); it is **somewhat easy to explain** the value the metric will add to the organization; the results of the metric and implications of the results are **somewhat easy to explain**.		The metric and purpose of the metric are **easy to explain** to key stakeholders (i.e., C-suite personnel, management, supervisors, subordinates, customers); it is **easy to explain** the value the metric will add to the organization; the results of the metric and implications of the results are **easy to explain**.
1	2	3	4	5

Presenting Metrics to the C-Suite

Communication

Criteria Definition

- Extent to which metrics, metric results, and metric value can be communicated easily, succinctly and convincingly to key stakeholders (especially senior management)

Key Elements

- Style/format
- Organizational alignment
- Credibility
- Use of visual aids
- Tell a story
- Simplicity and clarity
- Logical conclusion

Communication

Style/Format

- Present in a manner that senior management is accustomed to and comfortable with.
- Determine in advance if read-aheads are expected.
- To the extent possible, know the audience (as a group and as individuals) and employ previously successful approaches while avoiding “hot buttons.”

Communication

Organizational Alignment

- Review in advance the organization’s vision, strategic goals, core values and business plans, and attempt to establish linkages wherever possible.
- Most importantly, connect metrics presented to overall organizational objectives and reduction of risks.

Communication

Credibility

- Make sure metrics presented can withstand scrutiny, in terms of validity and reliability.
- Ensure checks and balances are in place to ensure metrics data is not vulnerable to falsification or manipulation.
- Understand and be able to explain the methodologies employed to collect and report metrics data.

Communication

Use of Visual Aids

- Charts, graphs, dashboards, diagrams, tables and illustrations should be used only selectively as a tool to make key points.
- Clarify not confuse.
- Benchmarking can enrich a presentation if it is aligned with strategic organizational goals, and conveys where existing risk levels stand in comparison to others.

Communication

Tell a Story

- Can be a story about the specific risk that security is attempting to mitigate, as well as consequences if the event occurs.
- Be straightforward about risk and uncertainties.
- Part of any compelling story is the unfolding of events over time.

Communication

Simplicity & Clarity

- Keep presentations simple and clear.
- Introductions should be brief, and geared towards quickly setting the stage for substantive discussion.
- Respond to questions promptly and directly, while avoiding longwinded explanations.
- Unless you're really good at it and know your audience well, avoid amateur attempts at humor.
- Similarly, wrap-up, conclusions and recommendations should be crisp.

Communication

Logical Conclusion

- Verbal presentation, visual aids, stories and Q&As should be sequenced in such a way to lead to a high level summary and logical conclusion.
- “Hip pocket” information to include additional metrics and anecdotes should be available to present if needed to amplify a recommendation or to counter a dissenting opinion.
- Above all, convey an unbiased view and objectivity throughout.

Strategic Criteria

ROI

Communication

Organizational Relevance

Organizational Relevance

Extent to which the metric is linked to organizational risk management or a strategic mission, objective, goal, asset, threat, or vulnerability relevant to the organization—in other words, linked to the factors that matter most to senior management.

The metric is **not linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; if linked, the **linkage is weak** and of minimal relevance to the organization; the data derived from this metric is of **little importance** to senior management.		The metric is **somewhat linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the **linkage is moderate** and of some relevance to the organization; the data derived from this metric is of **some importance** to senior management.		The metric is **explicitly linked** to a specific organizational strategic mission, objective, goal, asset, risk, threat, or vulnerability; the **linkage is strong** and of high relevance to the organization; the data derived from this metric is of **great importance** to senior management.
1	2	3	4	5

Organizational Relevance

Question: Is my metric demonstrating success in something that senior management cares about?

- **Metric:** Number of thwarted hacking attempts against company's cloud-based software.
- **Example:** A software company supplies a cloud-based application to its customers. A vital goal of the company is to keep the application properly functioning and available to clients 99.99 percent of the time. Therefore, a metric regarding the number of denial-of-service attacks thwarted through security efforts would be highly relevant to the organization's goals and would be of great interest to senior management.
- **Score:** 5 on the Security MET.

This would be a good metric to present to senior management.

Organizational Relevance

- **Metric:** Number of instances in which employees were robbed of their mobile phones on or around company property.
- **Example:** At a major financial services firm in a high-crime central business district, employees were being robbed of their phones on the sidewalks around the office. Key factor: at this company, the CEO was a major booster of the city and was determined to attract employees to work at the downtown location. Security department focused its efforts and reduced theft to zero.
- **Score:** 5 on the Security MET. This metric is not attempting to prove ROI—it is simply trying to tell senior managers something they care about. In this case, a safe work environment was extremely important to the CEO, so this would be a good metric to share.

Organizational Relevance

- If the metric (reduction in employees being robbed of their phones) is strong in all other criteria (reliability, validity, generalizability, cost, timeliness, manipulation, ROI, and communication), but scores very low on organizational relevance, it may still be worth collecting as feedback on the success of security efforts, but **there may be no reason to present the metric to senior management**.
- **Again, be creative.** Maybe the reduction in phone theft would be more relevant to senior management if you emphasized how it kept unflattering stories about the company out of the news, reduced the risk of premises liability lawsuits, or had other value that senior management strongly cares about.

Case Example

Case Example

Active Shooter Preparedness

Background

Setting

- Established university R&D organization
- 400 acre campus, 30+ buildings, > 5,500 employees
- 5 additional leased buildings nearby

Climate

- Rising concerns over the potential for a workplace violence/active shooter incident have been expressed by employees.
- Senior leadership has directed security to assess and report back as to the organization's readiness posture.

Case Example

Active Shooter Preparedness

Risk Analysis

Threat

- Low probability/high impact
- Frequency of active shooter and workplace violence events on the rise in recent years
- Location/organization unpredictable

Vulnerabilities

- No awareness training or staff involvement in exercises/drills
- Insufficient emergency notification capabilities
- Complex environment, facility layout
- Gaps in video surveillance coverage
- Minimal familiarity of likely first responders
- Absence of a capable on-site armed response

Case Example

Active Shooter Preparedness

Communications Strategy

Challenges

- $$$$
- Staff time away from mission
- Image
- Philosophical resistance

Approach Taken

- Brief executive leadership on threats, vulnerabilities and consequences using metrics, visual displays and anecdotes.
- Keep presentations crisp and compelling.
- Invite open dialogue as to pros/cons to set the stage for decisions to be "owned" by organizational leadership.

Case Example

Active Shooter Preparedness

Numbers (Volume, Velocity, Value) + Stories = Impact

Metrics Used

- FBI statistics: active shooter events have nearly tripled over the last 7 years (volume); most attacks are over in less than 15 minutes (velocity).
- On-site active shooter exercise results highlighted more than 30 minutes transpired before police could locate and engage the threat (velocity).
- On-site armed presence and surveillance enhancements would reduce response time by 66%.

Stories Told

- Theme: "Action taken to expedite law enforcement response while concurrently delaying the perpetrator from locating victims saves lives."
- Columbia Mall shooting (Howard County Police Chief)
- Navy Yard shooting (Senior NCIS Agent)

Case Example

Active Shooter Preparedness

Notable Incidents

- Fort Hood, Texas - April 2, 2014: Suspect killed 4 people, injured 16 others before committing suicide.
- Columbia Mall - January 15, 2014: Suspect entered store with a shotgun, killing 2 persons and injuring 5 others before taking his own life.
- Washington Navy Yard - September 16, 2013: Suspect entered building #197 at the Navy Yard and began firing, killing 12 people and wounding 3 others. Suspect was subsequently killed during a gunfight with police.
- Sandy Hook Elementary School - December 14, 2012: Suspect entered the school and shot and killed 26 people (20 students and six adults) before taking his own life. 2 others were injured but survived during the attack.
- Aurora, Colorado - July 20, 2012: Suspect entered a movie theater and began shooting. 12 people were killed and 70 wounded before suspect was apprehended.
- Columbine High School - April 20, 1999: 2 students killed 12 classmates and a teacher before both committed suicide. 24 additional victims were wounded.
- Fort Hood, Texas - November 5, 2009: Suspect killed 13 people, injured 42 others before being apprehended.
- Virginia Tech - April 16, 2007: Suspect killed 33 people and injured 17 before committing suicide.

Case Example

Active Shooter Preparedness

More Notable Incidents

- Santa Barbara, CA - 5/23/2014: 6 dead, 13 wounded
- Franklin H.S., PA - 4/9/2014: 21 wounded (stabbed)
- Accent Signage, MN - 9/27/2012: 5 dead, 3 wounded
- Sikh Temple, WI - 8/5/2012: 6 dead, 4 wounded
- Safeway Parking Lot, AZ - 1/8/2011: 6 dead, 13 wounded
- Emcore, NM - 7/12/2010: 2 dead, 4 wounded
- Pentagon - 11/10/2009: 2 wounded, gunman killed by Pentagon Police
- Si Port, CA - 11/14/2008: 3 dead
- Naval Business Center, PA - 2/13/2007: 3 dead, 1 wounded
- Labor Ready, AL - 2/25/2003: 4 dead, 1 wounded
- Edgewater Technology, MA - 12/26/2000: 7 dead
- Momentum Securities, GA - 7/29/1999: 9 dead, 12 wounded
- GMAC (General Motors), FL - 6/18/1990: 9 dead, 4 wounded
- CIA HQ - 1/25/1993: 2 dead, 3 wounded
- ESL, CA - 2/16/1988: 7 dead, 4 wounded

Case Example

Active Shooter Preparedness

January 15, 2014
Columbia Mall, MD
2 killed, +Shooter
5 Injured

September 16, 2013
Washington Navy Yard
12 killed, +Shooter
3 Injured

December 14, 2012
Newtown, CT
Elementary School
27 Killed, +Shooter
2 Injured

July 20, 2012
Aurora, CO
Movie Theater
12 Killed
58 Injured

January 8, 2011
Tucson, AZ
Safeway Parking Lot
6 Killed
13 Injured

November 5, 2009
Fort Hood, TX
13 Killed
Over 30 Injured

April 16, 2007
Virginia Tech
32 Killed, +Shooter
17 Injured

April 20, 1999
Columbine High School, CO
13 Killed, + 2 shooters
21 Injured

Case Example

Active Shooter Preparedness

Outcome

Decision

- Executive leadership approval of all recommendations and substantial increases security's budget to effect implementation.

Actions Taken

- Administered mandatory "run-hide-fight" awareness training to all staff.
- Expanded emergency notification capabilities (PA system, mobile and desktop alerts and "giant voice").
- Conducted an organization-wide lockdown drill to test effectiveness of training and communications improvements.
- Increased video surveillance coverage and enabled connectivity to local and state law enforcement.
- Added armed, on-site, professionally trained law enforcement personnel to the organization.

Q&A

Resources

- **Contribute your metric:** https://www.surveymonkey.com/r/metrics-survey
- **New ASIS Foundation metrics site:** https://foundation.asisonline.org/FoundationResearch/Security-Metrics/Pages/default.aspx
- ***Persuading Senior Management with Effective, Evaluated Security Metrics*:** https://foundation.asisonline.org/FoundationResearch/Research/Current-Research-Projects/Pages/Metrics-Research-.aspx (contains Security Metric Evaluation Tool)
- **Presenter:** Dick Weaver, Special Security Advisor, Johns Hopkins University Applied Physics Laboratory, Richard.Weaver@jhuapl.edu
- **Presenter:** Peter Ohlhausen, President, Ohlhausen Research, peter@ohlhausen.com