PRICE®

ICEAA 2019

Measurement in Cybersecurity

Presented by:
Arlene F. Minkiewicz

Estimate with Confidence™

Agenda

- Introduction
- Cybersecurity and Information Security
  - History
  - Definitions
- Measurement in Cybersecurity Context
  - Definitions
  - Measurement Framework
- Cybersecurity Metrics
- Next Steps and Conclusions

Introduction

- More than half of survey respondents scored a failing grade when self evaluating their efforts to measure investments and performance[1]

  > *"Since 1988's Morris Worm, which infected 10% of the estimated 60,000 computers connected to the internet, cybersecurity has grown into an industry expected to exceed $1 trillion in global spending between 2017 and 2021" [2]*

  - Cybercrime will cost the global business market an estimated average of $6 trillion annually in the same time frame.

- Industry and government is aware of the perils of ignoring cyber and information security threats, but are asking themselves
  - How much security is enough?
  - How will we know when we get there?
  - How much will it cost?
  - Where is the tipping point where expenditures exceed the value added ?

[1] 2017 State of Cybersecurity Measurement Annual Report

Cybersecurity and Information Security - History

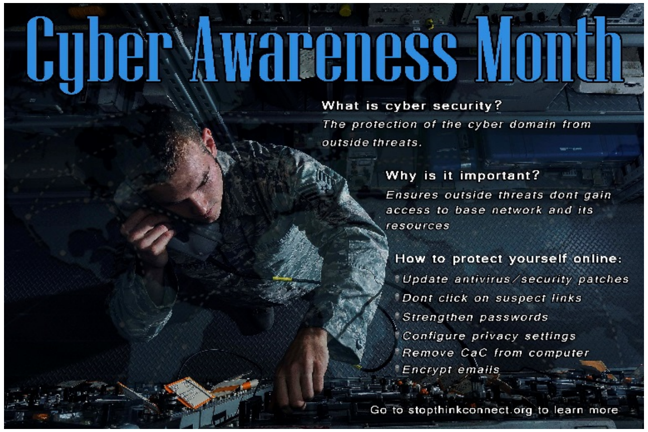
Cybersecurity and Information Security – History

- In the middle of twentieth century early model computers were rarely connected to networks.
  - Cybersecurity a non issue
  - Information security - user IDs, passwords and app access
  - Computers were a tool, not the lifeblood of the organization
- In the 80's
  - PCs flourish – require connectivity
  - Firewalls and antivirus software needed
  - IT folks question what to measure

- In the 90's
  - Virus and hacking incidents prominent in the news
  - Data and information needs protection as much as physical structures

Cybersecurity and Information Security – History (cont.)

- In the 2000's
  - 2008 – Zeus Trojan – hacking banking systems
  - 2013 – Target hacking incident
  - Since 2013 – almost four billion records lost
- Today and Beyond
  - Internet is ubiquitous
  - Cloud computing emergent
  - Internet of Things (IoT) creating smart environments
  - Information is flowing fast and furious
  - Cyber and information security are regular features in the C-level executives nightmares



Cyber Awareness Month

What is cyber security?
The protection of the cyber domain from outside threats.

Why is it important?
Ensures outside threats dont gain access to base network and its resources

How to protect yourself online:
- Update antivirus/security patches
- Dont click on suspect links
- Strengthen passwords
- Configure privacy settings
- Remove CaC from computer
- Encrypt emails

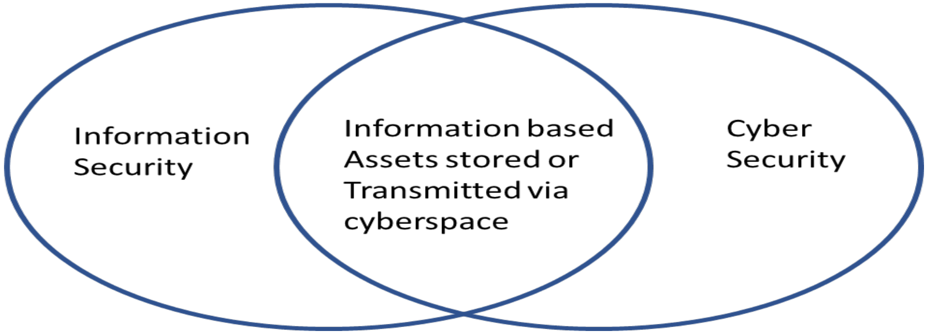
Go to stopthinkconnect.org to learn more

Cyber and Information Security - Definitions

- Cybersecurity and information security are often used interchangeably, though they have different meanings
- Information Security
  - The practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information and data can be electronic or physical. The basic focus is to ensure:
    - *Confidentiality - information not accessible, available, disclosed to unauthorized people, entities, or processes*
    - *Integrity –data remains accurate and complete*
    - *Availability – Data is accessible at the time and place where needed*
- Cybersecurity
  - The measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack Cybersecurity focuses on protecting cyberspace from any criminal action intended to compromise information or other computer assets

Overlap Between Cybersecurity and information Security

- While related, these two concepts are not the same…
- BUT there is a significant and growing overlap…
- Most cybersecurity breaches are intended to…
  - Obtain confidential information
  - Compromise the integrity of information
  - Prevent access to information
- Many metrics/measures are relevant to both



Information Security

Information based Assets stored or Transmitted via cyberspace

Cyber Security

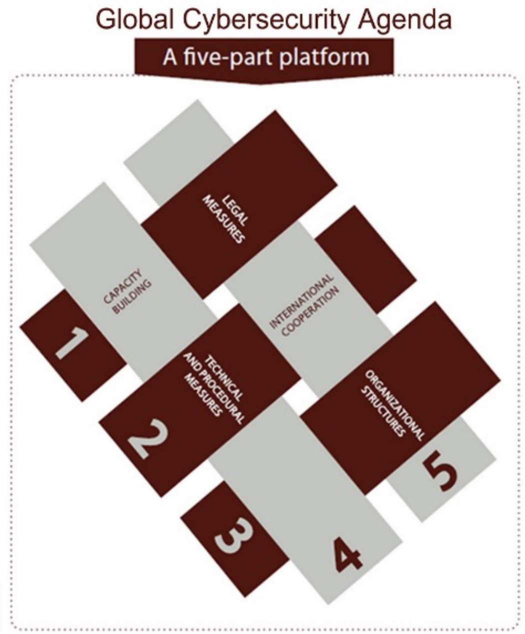
Measurements in Cyberspace

Measurement in Cyberspace

"Without sound metrics, we are in the position of a passerby who encounters a man swinging plucked chickens around his head while he stands on a street corner: asked why he is doing that he answers, 'To keep the flying elephants away', 'But there are no flying elephants' responded the befuddled observers. He crows triumphantly 'See? It works!'"

- *Cybersecurity measurements are problematic because:*
  - *The field is immature*
  - *Each organization has different needs*
  - *Metrics consumers have different needs*

Measurement in Cyberspace - Definitions


Global Cybersecurity Agenda
A five-part platform
LEGAL MEASURES
CAPACITY BUILDING
INTERNATIONAL COOPERATION
TECHNICAL AND PROCEDURAL MEASURES
ORGANIZATIONAL STRUCTURES
1
2
3
4
5

- Measurements are objective, concrete parameter values for something usually in specific units e.g.
  - Length
  - Weight
  - Area
- Metrics are more subjective and often determined in relations to several points of reference.
  - Hours per lines of code (LOC)
  - Dollars per pound
- Metametrics represent information about metrics e.g.
  - For a data set – mean, standard deviation, min, max
  - For a metric – cost to collect, believability, usefulness, actionability

Measurement in Cyberspace

For any measurement initiative, there are important things to consider:

- Metrics that answer important organizational concerns, balanced across a spectrum of objectives :
  - *Strategic*
  - *Management focused*
  - *Operationally focused*
- Information important to one or more stakeholder
- Quantifiable and actionable information
- Ease of collection
- Available, accessible and repeatable
- Meaningful and useful to the consumer

Cybersecurity Metrics

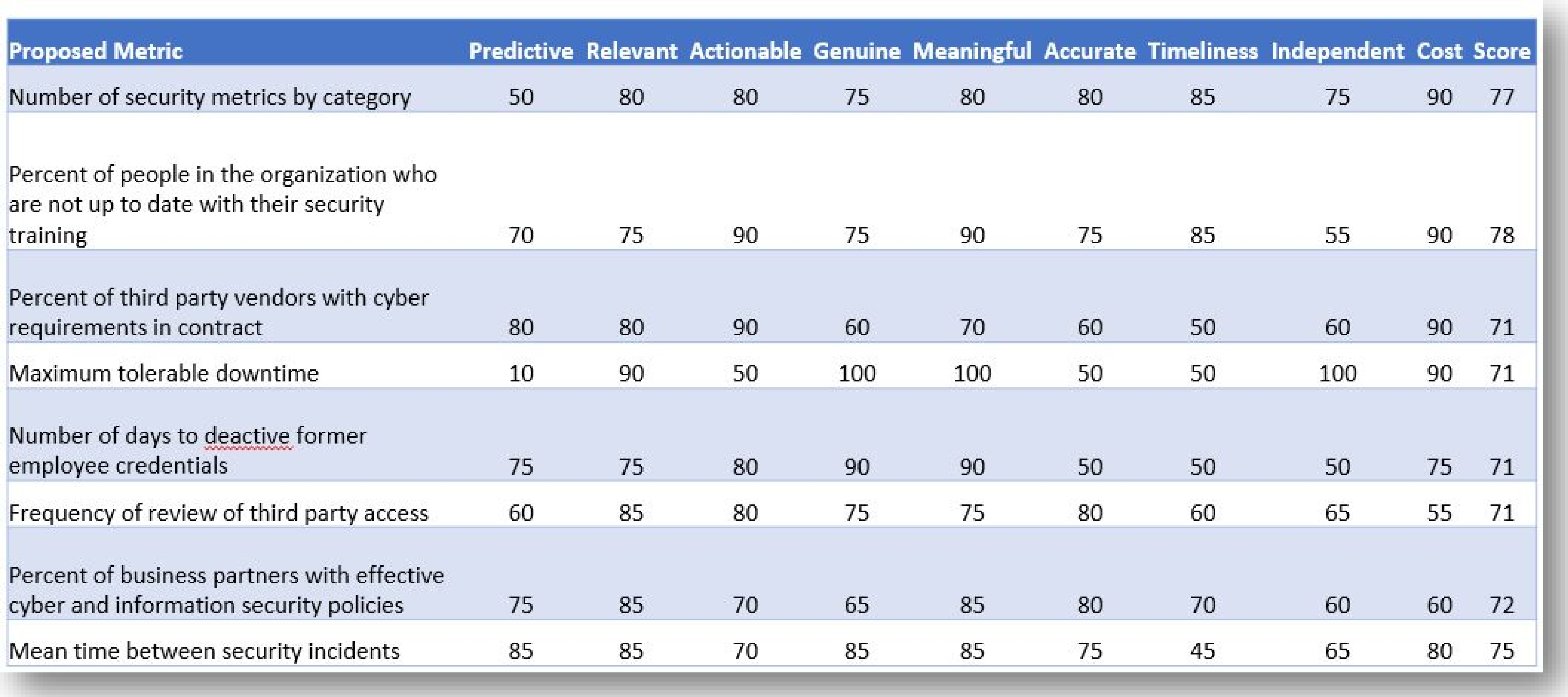
Framework for Choosing the 'Right Metrics'

- Framework proposed is titled PRAGMATIC[1]. For each proposed metric the following metametrics are examined:
  - Predictive
  - Relevant
  - Actionable
  - Genuine
  - Meaningful
  - Accurate
  - Timely
  - Independent
  - Cost Effective

- Each proposed metric is scored for each metametric and the results are averaged to determine the suitability for the organizations security needs, risk aversion, available resources, etc.

[1] Brothby W.K., Hinson GG, "*PRAGMATIC Security Metrics: Applying Metametrics to Information Security*",

Example of Ranked Metrics



Proposed Metric	Predictive	Relevant	Actionable	Genuine	Meaningful	Accurate	Timeliness	Independent	Cost	Score
Number of security metrics by category	50	80	80	75	80	80	85	75	90	77
Percent of people in the organization who are not up to date with their security training	70	75	90	75	90	75	85	55	90	78
Percent of third party vendors with cyber requirements in contract	80	80	90	60	70	60	50	60	90	71
Maximum tolerable downtime	10	90	50	100	100	50	50	100	90	71
Number of days to deactive former employee credentials	75	75	80	90	90	50	50	50	75	71
Frequency of review of third party access	60	85	80	75	75	80	60	65	55	71
Percent of business partners with effective cyber and information security policies	75	85	70	65	85	80	70	60	60	72
Mean time between security incidents	85	85	70	85	85	75	45	65	80	75

Cybersecurity Metrics

- Impossible and impractical to list all the possible cybersecurity metrics because…
  - The field is constantly evolving
  - Not all metrics are relevant to all organizations.
- The metrics that follow are not comprehensive - intended to offer breadth and depth to the possibilities
- The metrics presented are aligned with the structure of ISO/IEC Standard 27002 – "Information Technology – Code of Practice for Information Security Management"
- The metrics presented provide good coverage of the areas of concern from the NIST Special Publication 800-53 - "Security and Privacy Controls for Federal Information Systems and Organizations"

Cybersecurity Metrics

- Cybersecurity Risk Management
  - Number of known risks currently untreated or unresolved
  - Cybersecurity budget variance over time
  - Number of unpatched technical vulnerabilities
- Cybersecurity Policy
  - Percent or number of security artifacts (policies, standards, procedures, metrics, etc.)
  - Traceability of policies, control objectives, standards and procedures
  - Policy coverage of frameworks such as ISO/IEC 27002

Subcommittee on
Cybersecurity and Long-Term Policy
Objective: Assess potential cybersecurity risks and examine State vs. Federal roles in cybersecurity regulation, as well as data collection and consumer privacy.
LONG-TERM POLICY
Data accuracy & ability to audit
Adaptability
Land use and urban design
Road and infrastructure design / Security
Data reporting and management
Sustainability

Cybersecurity Metrics

- Cybersecurity Management and Governance
  - Percentage of security controls that may fail silently
  - Cybersecurity ascendency (levels between CEO and most senior cybersecurity professional)
  - Days since the last serious cybersecurity incident
  - Number of security metrics being tracked by category
  - Percentage of critical third party vendors whose contracts include cybersecurity requirements with the organization’s policies
- Information Asset Management
  - Percent or number of orphaned information assets without an owner
  - Proportion of information assets not classified
  - Unowned information asset days

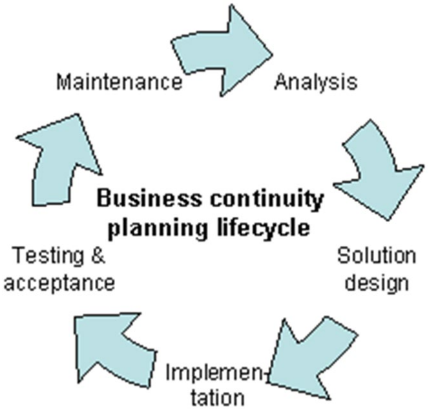
Cybersecurity Metrics

- Human Resources
  - Security awareness level
  - Rate of change in employee turnover or frequent absences
  - Percent of employees who are not up to date on security training
- Physical and Environmental Security
  - Discrepancies between physical locations and logical access locations
- Information Technology Security
  - Proportion of systems checked and fully compliant to technical standards
  - Time from change approval to change
  - Average number of changes per category received per time period
  - Rates of change of emergency change requests
  - Proportion of highly/privileged trusted users
  - Maximum tolerable down time

Cybersecurity Metrics

- Access Control
  - Rate of messages received at central access logging/alerting system
  - Days since logical access control matrices for application systems were last reviewed
  - Number of days to deactivate former employee credentials
  - Frequency of review of third party access
  - Percent of business partners with effective cybersecurity policies
- Software Security
  - Percentage of controls tested realistically
  - Software quality assurance (QA) maturity
  - Extent to which cybersecurity is incorporated into the software development process
  - Security testing coverage

Cybersecurity Metrics



- Incident Management
  - Time take to remediate security incidents
  - Mean time between security incidents
- Business Continuity
  - Coverage of business impact analysis
  - Percentage of business processes having a defined recovery time Objective (RTO) and recovery point objective (RPO)
  - Uptime
  - Disaster recovery test results
- Security Compliance and Assurance
  - Breakdown of exceptions and exemptions
  - Number and severity of findings in audit reports, reviews, assessments, etc.
  - Status of compliance with externally imposed security obligations

Conclusions and Next Steps

- Cybersecurity and information security are not easy topics to grapple with
- Landscape is rapidly changing as technology improves and bad actors get smarter
- Business leaders are constantly challenged with understanding cybersecurity and determining the best way to conquer potential evils
- Measurement and metrics need to be part of the solution. Measurement makes metrics possible and metrics make it possible to …
  - Assess the efficacy of cybersecurity initiatives in place
  - Understand the cost and value of planned cybersecurity initiatives
  - Make trade offs between an organization’s cybersecurity needs, goals, risk aversions, and resources

Conclusions and Next Steps

- First step is to understand the notion of cybersecurity and the activities, processes and practices that are important in the cybersecurity world
- This sets the stage for identify the important things to measure and assess
- Measurement enables …
  - Assessment of current state of cyber wellness in an organization
  - Assessment of future cyber investments
- Research underway to continue to study measures and metrics particularly suited to understanding and predicting costs
- Historical values for these measures and metrics will be used to develop cost estimating relationships and rules of thumbs for predictive cost analysis

Questions?

References

[1] “The 2017 State of Cybersecurity Metrics Annual Report”, Thycotic, available at https://thycotic.com/resources/cybersecurity-metrics-report-2017/, retrieved 1/15/2019

[2] “Cybersecurity Performance: 8 Indicators”, Carnegie Mellon University Software Engineering Institute – Insider Threat Blog, March 25, 2018, available at https://insights.sei.cmu.edu/insider-threat/2018/03/cybersecurity-performance-8-indicators.html, retrieved 1/21/2019