Cybersecurity Metrics

Leaders & Laggards

Leo F Howell, MBA CISSP CISA
Chief Information Security Officer
About UO

- 23K Students
- 5K Faculty & Staff
- $122M Grant $$
- AAU Member, R1
- $1B Ops Budget
- $2.2B Economic Impact
- Major Construction
  Knight Campus, Hayward...
- 2021 World Games
  (IAAF Track & Field)
Objectives

Background
Business Drivers
Metrics Framework
Useful Metrics
Implementation Ideas
BACKGROUND
Definition

• **Metrics** are tools to facilitate decision making and improve performance and accountability. Lower-level for tactical; high-level for strategic decision making; abstract and subjective

• **Measures** are quantifiable, observable, and objective data elements that support metrics

• Organizations use measures and metrics to set goals or **Benchmarks**

• **Security metrics** should be used to communicate performance, guide resource allocation, improve risk management effectiveness, and align business and security decision-making
Why do we need 'em?

“When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind...”

- Lord Kelvin
Why do we need 'em?

“When you can measure what you are speaking about, and express it in numbers, you know something about it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind...”

- Lord Kelvin

.... because, we can't MANAGE without 'em
Business Drivers for Cybersecurity Metrics

- Business decisions
- Risk management
- Business improvement
- Efficiency & Effectiveness management
Attributes of GOOD Metrics

**Measures**
- Quantitative
- Accessible
- Obtainable
- Automatable

**Metrics**
- Clear Objective
- Repeatable
- Meaningful
- Broadly accepted
- Statistically sound
Leaders & Laggards
Objective: Weight Loss

Caloric Intake
Calories Burnt
METRICS FRAMEWORK
Cybersecurity Strategic Plan

**Vision**

A knowledgeable and capable UO community working together to safeguard our digital assets and capabilities to empower excellence in research and instruction in a resilient cyber environment.

**Mission**

To empower the UO community to leverage digital assets and capabilities, and defend our cyber environment through proactive measures.
# Cybersecurity Balanced Scorecard (enterprise)

<table>
<thead>
<tr>
<th>Objective</th>
<th>Goal</th>
<th>Grade</th>
<th>Target</th>
<th>Objective</th>
<th>Goal</th>
<th>Grade</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VALUE</strong></td>
<td>B</td>
<td>C+</td>
<td>B</td>
<td><strong>COMMUNITY</strong></td>
<td>B</td>
<td>B</td>
<td>B+</td>
</tr>
<tr>
<td>Reduce Risk Impact</td>
<td>C</td>
<td>C-</td>
<td>C</td>
<td>Confidence &amp; Capability</td>
<td>C</td>
<td>B</td>
<td>B</td>
</tr>
<tr>
<td>Optimize Investment</td>
<td>B</td>
<td>B</td>
<td>B+</td>
<td>Compliance</td>
<td>B</td>
<td>B</td>
<td>B+</td>
</tr>
<tr>
<td>Enable Digital Capability</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>Access &amp; Availability</td>
<td>B</td>
<td>B</td>
<td>B+</td>
</tr>
<tr>
<td><strong>OPERATION</strong></td>
<td>A</td>
<td>B</td>
<td>A</td>
<td><strong>PROGRESS</strong></td>
<td>D</td>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>Operate within Risk Appetite</td>
<td>C</td>
<td>C</td>
<td>B</td>
<td>Cybersec Function Dev</td>
<td>D</td>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>Cybersecurity Governance</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>NCFW Compliance</td>
<td>D-</td>
<td>D-</td>
<td>D</td>
</tr>
<tr>
<td>Guided D.I.Y. Security</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>Cybersec Team Dev</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Built-in Security &amp; Resilience</td>
<td>A</td>
<td>C</td>
<td>A</td>
<td>Community Capability</td>
<td>D</td>
<td>D</td>
<td>B</td>
</tr>
</tbody>
</table>
Metrics must support all decision levels!

Cybersecurity Metrics Framework

- **Strategic**
  - Risk & Value

- **Functional**
  - Community
  - Operations

- **Operational**
  - Confidence
  - Compliance
  - Access
  - Resilience
  - Security

Measures (automated collection)

110111001001010101000111011100111001111100110000101
USEFUL METRICS

Value, Community, Operations, Progress
Value Decision Metrics
Value: Reduce Risk & Maximize Access

Leader: Incident Prevention Score (IPS)

- Data Attack Surface Area. How many high-risk records are online? Goal: LOW
- Availability Score. What is the average availability of critical services? Goal: HIGH
- STORR. What is the strategic-to-operational resource ratio? Goal: HIGH
- Investment Burn Rate. How quickly are cybersecurity-dollars operationalized? Goal: HIGH
- Technology Shelve-Time. What is the time-to-implement after you bought it? Goal: LOW

Laggard: Incident Response Score (IRS)

- Incident Thwart Rate. What % of incidents are thwarted by implemented controls? Goal: HIGH
- ROSA. What is the Return-on-Security-Asset? Goal: HIGH
- Scope of Incident. What is the average scope of assets impacted? LOW
Value: Maximize Investment

Leader: Cost of Prevention

- **Patch Cost.** What is the average cost-to-patch application systems? Goal: **LOW**
- **Vulnerability Mitigation Cost.** What is the average cost-to-mitigate vulnerabilities? Goal: **LOW**
- **Insurance Coverage Ratio.** What is the current-to-desired coverage ratio? Goal: **HIGH**

Laggard: Cost of Response

- **Direct Incident Cost.** What is the direct cost of incidents – fees, forensics, legal, crisis management, notification cost, credit monitoring, lawsuits? Goal: **LOW**
- **Reputational Hit.** What is the level of loss in confidence by stakeholders? Goal: **LOW**
Community Decision Metrics
Community: User Susceptibility

Leader: Awareness Training

- **Training Coverage.** What % of users are being trained? Goal: **HIGH**
- **Phish Awareness.** What % of phish are user-identified? Goal: **HIGH**
- **Heroes & Heroines.** What % of users forward messages to the Phish Tank? Goal: **HIGH**

Laggard: User Susceptibility Score

- **Phish Clicks++.** What % of users have “clicky” fingers++? Goal: **LOW**
- **Phished.** What % of users are phished? Goal: **LOW**
- **Password Strength.** What percent of users create strong passwords? Goal: **HIGH**
- **Policy Violators.** What % of users violate policies? Goal: **LOW**
Community: Configuration Management Maturity

Leader: Security Training

- **Security Knowledge.** How knowledgeable is IT in implementing security controls? Goal: **HIGH**
- **Baseline Adoption.** What is the level of adoption of defined baseline? Goal: **HIGH**
- **Self-Identified Vulnerability.** What % of vulnerabilities are fixed in development? Goal: **HIGH**

Laggard: Control Effectiveness

- **Misconfigurations.** What is the rate of misconfigurations? Goal: **LOW**
- **Baseline Deviation.** What is the level of non-compliance with standards? Goal: **LOW**
Community: Endpoint Protection

Leader: Configuration Management System (CMS)

• **Patch Updates.** How long does it take for high-risk endpoints to be patched? Goal: **LOW**
• **Unmanaged Devices.** What % of connected devices are unmanaged? Goal: **LOW**
• **Antimalware.** What % of users are using approved antimalware service? Goal: **HIGH**
• **Disk Encryption.** What % of high-risk endpoint devices have encrypted disks? Goal: **HIGH**
• **System Backup.** What % of high-risk endpoint systems are backed up? Goal: **HIGH**

Laggard: Control Scope

• **Malware Infection.** What % of endpoints are infected by malware? Goal: **LOW**
• **Outdated Software.** What % of software are missing high-risk updates? Goal: **LOW**
• **Vulnerability Mitigation.** How long does it take to address vulnerabilities? Goal: **LOW**
• **Data Loss Instances.** What % of endpoint incidents involve data loss? Goal: **LOW**
Community: User Access

Leader: User Access Control

- **2FA**. What % of users are using 2FA for accessing systems? Goal: **HIGH**
- **Termination Latency**. What is the average time to terminate access? Goal: **LOW**

Laggard: Compromised Account

- **VIP Compromise**. What % of VIP accounts are compromised? Goal: **LOW**
- **Privilege User Compromise**. What % of privilege users are compromised? Goal: **LOW**
- **Non-Privilege Users Compromise**. What % of normal users are compromised? Goal: **LOW**
Community: Formal Compliance

**Leader: Policy**

- **User Feedback.** What is the average user feedback score on policy, standards, and guidelines provided? Goal: *HIGH*
- **Policy Knowledge.** What % of users are policy-aware? Goal: *HIGH*
- **High-Risk Policy Exception.** What % of policy exception requests are high-risk? Goal: *LOW*

**Laggard: Compliance**

- **Policy Violations.** What % of users violate established policies? Goal: *LOW*
- **Level of Compliance.** What is the level of compliance with laws and regulations? Goal: *HIGH*
Operational Decision Metrics
Operational: Vulnerably Management

Leader: Patch Management

- **Patch Coverage.** What % of systems are under patch management? Goal: HIGH
- **Patch Latency.** How fast are patches applied after vendor-release? Goal: LOW
- **Vulnerability Scan Coverage.** What % of systems are scanned? Goal: HIGH
- **MTTMV.** What is the *mean-time-to-mitigate-vulnerabilities* after discovery? Goal: LOW
- **Pre-Go-Live Security Tests.** What % of systems are security-tested pre-go-live? Goal: HIGH

Laggard: Vulnerabilities Present

- **Critical.** What % of system has critical (CVSS9.0 - 10.0)? Goal: LOW
- **High.** What % of systems has high (CVSS7.0 - 8.9)? Goal: LOW
- **Medium.** What % of systems has medium (CVSS4.0 - 6.9)? Goal: LOW
- **Low.** What % of systems has low (CVSS 0.1 -3.9)? Goal: LOW
Operational: Change Management

**Leader: Change Success Ratio**

- **Rogue Changes.** What % of changes are *rogue changes*? Goal: LOW
- **Emergency Changes.** What % of changes are emergencies? Goal: LOW
- **Critical & Complex Changes.** What % changes are C&C? Goal: LOW
- **Normal Changes.** What % of changes are normal? Goal: HIGH
- **Security-Approved Changes.** What % of changes are approved by Security? Goal: HIGH

**Laggard: Change Failure Ratio**

- **Security Diminishing Changes.** What % of changes result in new vulnerabilities or security exceptions? Goal: LOW
- **Data Corruption.** What % changes result in data corruption? Goal: LOW
- **Security Incident via Change.** What % of changes lead to security incidents? Goal: LOW
Operational: Incident Management

Leader: IR Planning

- **IR-Awareness.** How capable are key players in their roles in an incident? Goal: **HIGH**
- **IR Drill Score.** What is the overall readiness or *drill score* of the IR-team? Goal: **HIGH**
- **Attack Surface Area.** How large is the *attack surface area* (# online apps, % of high-risk apps, online database sizes, etc.)? Goal: **LOW**

Laggard: Incident Response

- **Incident Indirect Cost.** What is the indirect cost of the incident (e.g., FTE-hours, opportunities foregone, ...)? Goal: **LOW**
- **MTTD.** What is the *mean-time-to-detect* incidents? Goal: **LOW**
- **MTBI.** What is the *mean-time-between-incidents*? Goal: **Low**
- **MTTR.** What is the *mean-time-to-recover* from incidents? Goal: **LOW**
PROGRESS
Decision Metrics
Advancement: Growth Metrics

Value
- Reduce Risk & Maximize Access
  - Prevention Score
  - Availability Score
  - Response Score

Maximize Investment
- Cost of Prevention
- Cost of Response

Operations
- Vulnerability Mgmt.
  - Patch & Config. Mgmt.
  - Vulnerabilities
- Change Mgmt.
  - Change Success Ratio
  - Change Failure Ratio
- Incident Mgmt.
  - IR Planning
  - Incident Response

Community
- User Susceptibility
  - Awareness Training
  - Susceptibility Score
- Configuration Management
  - Security Training
  - Control Effectiveness
- Endpoint Protection
  - CMS
  - Control Scope
- User Access
  - User Access Control
  - Compromised Accounts
- Formal Compliance
  - Policy
  - Compliance
<table>
<thead>
<tr>
<th>Objective</th>
<th>Goal</th>
<th>Grade</th>
<th>Target</th>
<th>Objective</th>
<th>Goal</th>
<th>Grade</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VALUE</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>COMMUNITY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prevention Score (Le)</td>
<td>B</td>
<td>C+</td>
<td>B</td>
<td>User Awareness Training (Le)</td>
<td>B</td>
<td>B</td>
<td>B+</td>
</tr>
<tr>
<td>Response Score (Le)</td>
<td></td>
<td></td>
<td></td>
<td>Susceptibility Score (La)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of Prevention (La)</td>
<td></td>
<td></td>
<td></td>
<td>Security Training (Le)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of Response (La)</td>
<td></td>
<td></td>
<td></td>
<td>Control Effectiveness (La)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>OPERATION</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>PROGRESS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patch &amp; Config. Management (Le)</td>
<td>A</td>
<td>B</td>
<td>A</td>
<td>User Access Control (Le)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability Management (La)</td>
<td></td>
<td></td>
<td></td>
<td>Compromised Accounts (La)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Success Ratio (Le)</td>
<td></td>
<td></td>
<td></td>
<td>Policy (Le)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Failure Ratio (La)</td>
<td></td>
<td></td>
<td></td>
<td>Compliance (La)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response Planning (Le)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response (La)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IMPLEMENTATION PROCESS
Impactful Metrics are Complex
Collaborative, Repetitive, Long-Term Process

Governance → Simple Set → Unit Enterprise

Refine → Unit Enterprise → Complex Set

Year 1, Year 2, ..., Year N
Key Takeaways

- Why Metrics? Can't Manage without 'em
- Compelling Business Drivers
- We need both Leaders & Laggards
- The Balanced Score Card provides a great framework
- Many years to develop an effective metrics program!!

Want to get involved?
lfhowell@uoregon.edu
Thanks!

Cybersecurity Metrics
Leaders & Laggards

Leo F Howell, MBA CISSP CISA
CISO, University of Oregon

Want to get involved?
lfhowell@uoregon.edu
References

✓ CYBER SECURITY METRICS AND MEASURES: Paul E. Black, Karen Scarfone and Murugiah Souppaya, National Institute of Standards and Technology, Gaithersburg, Maryland.  


✓ The CIS Security Metrics 2010: The Center for Internet Security  