Making Leaders Successful Every Day
Information Security Metrics – Present Information that Matters to the Business

Ed Ferrara, Principal Research Analyst

July 12, 2011
The CISO leads an organization that is critical to the business – Use business driven security metrics to prove it.
Agenda

Traditional Thinking, Traditional Metrics

Think Like a CEO and CFO - Communicate Leadership and Value

Reporting is Difficult

Effective Metrics

Seven Key Metrics – Secure Business Alignment

Forrester Recommends…
Risk Management Dashboard – Traditional Security Metrics

- CISOs often focus on operational metrics when reporting to senior leadership:
  - Percentage of users who undergo background checks each year
  - The number of virus infections addressed during the year
  - Etc.

Source: Eastman Kodak Company's Global IT Security Risk Dashboard
Reporting Can be Difficult and Time Consuming
Traditional Thinking, Traditional Metrics

Think like the CEO and CFO – Communicate Leadership and Value

Effective Metrics

Seven Key Metrics – Secure Business Alignment

Forrest Recommends…
CISO Leadership

“You Get What You Measure”

- **CISOs have much broader responsibilities than just operational security issues:**
  - Economic, Legal, Regulatory
  - Human Resources, Compliance
  - Traditional IT information security concerns

- **CISOs need information for better decision-making.**
  - Security metrics need to support decision-making and should drive broad based risk management strategies…”

- **CISOs need information to demonstrate the value they and their programs provide.**
  - Security metrics need to demonstrate business alignment, and support for the strategic and tactical goals of the business.
Agenda

Traditional Thinking, Traditional Metrics

Think like the CEO and CFO - Communicate Leadership and Value

Effective Metrics

Seven Key Metrics – Secure Business Alignment

Forrester Recommends…
Effective Reporting Has Impact.
Effective Metrics

- **Consistently measured** — Provide benchmarks and opportunities for continuous improvement.
- **Cheap to gather** — If metrics are expensive to gather, they will not be gathered.
- **Uses numbers** — Uses numbers that show relationships.
- **Show Trends** — Use numbers to show trends.
- **Relevant to decision-makers** — Are these the numbers the CEO and CFO care about? Why?
- **Presented graphically** — A picture is worth a thousand words.

Agenda

Traditional Thinking, Traditional Metrics

Think like the CEO and CFO - Communicate Leadership and Value

Effective Metrics

**Seven Key Metrics – Secure Business Alignment**

Forrester Recommends…
Seven example metrics: to secure* business alignment

1. **Strategic Alignment**
   - Demonstrate strategic alignment. Take ownership of the governance, risk and compliance management process.

2. **Functional Alignment**
   - Define problem you are solving
   - Decide what tool you are going to use.
   - Convince stakeholders of the need or opportunity.

3. **Efficiency and Effectiveness**
   - Develop metrics that show how you can do more with less.
   - Automation is critical here.

4. **Quality and Service levels**
   - Business operations should be measured for quality.
   - Information security is not exempt.
   - Implement a six-sigma or similar program.

5. **Process Measurement**
   - Security is the business of People, Process and Technology.
   - Understand the vulnerabilities presented by core business processes.

6. **Innovation**
   - Report on the implementation of new technology leading to improved security and efficiency.

7. **Compliance**
   - The number of laws and regulations organizations must comply with are growing.
   - Report on your compliance activities.

* Pun Intended.

Dashboard Reporting

- Pictures don’t always tell 1000 words.
- However, for busy executives the ability to see things in color and to show comparisons is important for impact.
- Make sure you can back up the pictures with real data.

Agenda

Traditional Thinking, Traditional Metrics

Think like the CEO and CFO - Communicate Leadership and Value

Effective Metrics

Seven Key Metrics – Secure Business Alignment

Forrester Recommends…
In the near term for 2011 & 2012, Security & Risk Professionals need to:

**Step 1: Identify your organization’s priorities.**
- Conduct a four- to six-week metrics strategy assessment.
- Interview the key business leaders in your organization. Find out what business metrics they care about.
- Pick five to seven key metrics from the categories outlined in this presentation and work from there. Less than five is too few. More than seven will dilute the impact.
- Use the criteria outlined in this presentation and make sure they align with the goals of the organization.

**Step 2: Move up the maturity ladder.**
- Prepare a continuous improvement plan that creates alignment between information security and the business over an 18- to 24-month period.

**Step 3: Report monthly or quarterly to the executive or risk committee.**
- Report each metric: strategic, operational, etc.
- Show the key trends of each metric and its performance against objectives.

**Step 4: Demonstrate business leadership as well as security leadership.**
- Meet regularly with executive and/or risk committee members outside of formal executive or risk committee meetings.
- Use the same seven key metrics in these conversations as well.
- Don’t be afraid to change or tweak metrics that outlive their ability to demonstrate business and security value.
Thank you

Ed Ferrara
+1.617.613.8836 (o)
eferrara@esferrara.com
www.forrester.com
CORE INSIGHT Enterprise
Security Testing & Measurement Solution
Core Security Technologies enables organizations to get ahead of threats with testing and measurement solutions that continuously identify and prove real-world exposure to their most critical assets.

- **Leading provider of commercial security testing software**
  - Established: 1996 / First commercial product: 2001
  - 1,000+ CORE IMPACT Pro customers (penetration testing software)
  - Segment leadership recognized by analysts, press awards, test labs

- **Diverse, experienced organization**
  - ~200 employees (Boston, Buenos Aires, India)
  - Experienced management -- backgrounds include Sophos, CA, Symantec, Seagate, IBM, World Bank
  - Key advisors include CISOs of Cisco and ADP + cyber security advisor to 2 U.S. presidents
  - Active Customer Advisory Board and Core Customer Community group

- **Groundbreaking research & product development**
  - Leading-edge consulting services brings field experience
  - CoreLabs vulnerability research team
  - High-profile research community involvement
  - Professional product and exploit development organization
  - 5 patents approved / 7 pending
Security test and measurement solutions that continuously identify and prove real-world exposures to your most critical assets.

**Enterprise-Class Security Testing Solution**
- Identifies proven threats to defined critical assets on a continuous basis.
- Benchmarks and measures enterprise-wide security posture, verifies actual business risks, and validates security controls.

**Automated Penetration Testing Software**
- In-depth, exploit-based testing across web apps, network systems, end users & wifi networks.
- Safely replicates all stages of an actual attack against systems and users.

**Targeted Penetration Testing Services**
- Ad-hoc or scheduled web, network and client-side assessments of your environment – leveraging CORE IMPACT Pro penetration testing software.

**Custom Consulting Services**
- Specialized penetration testing, security assessment, source code auditing, and technology testing services.
Where Core Security Fits

IT Security Management

Security Intelligence

Real-World Intelligence

Security Information and Event Management
- Alerts
- Log Mgt
- Event Correlation
- Compliance Certification

Comprehensive Security Test and Measurement
- Proactively Measure Real Security Risk
- Test Security Effectiveness
- Verify and Validate Security Controls

Governance Risk and Compliance
- User Policy Compliance
- Compliance Workflow and Reporting
- Remediation Workflow and Reporting

Security Information and Event Management:
- Alerts
- Log Mgt
- Event Correlation
- Compliance Certification

Comprehensive Security Test and Measurement:
- Proactively Measure Real Security Risk
- Test Security Effectiveness
- Verify and Validate Security Controls

Governance Risk and Compliance:
- User Policy Compliance
- Compliance Workflow and Reporting
- Remediation Workflow and Reporting
Use Cases

1. Vulnerability Validation
2. Gain Actionable Information
3. Testing Security Controls
4. Scaling Security Testing
5. Assessing Application Vulnerabilities
6. Testing End Users and Endpoints
7. Achieving Asset Visibility
What Sets Our Solutions Apart

Real-World

Proactive testing that reveals actual security exposures

Our solutions identify and prove paths of exposure to critical IT assets with techniques used by attackers—in a safe and controlled manner. No false positives.

Comprehensive

Automated assessment across ... 

- web applications
- network systems
- endpoint systems
- end users

Our solutions replicate threats that leverage weaknesses spanning different layers of IT.

Validation

Demonstrative proof of security controls efficacy

Our solutions deliver real-world metrics that confirm the effectiveness of whether controls are in-place and working properly— with no modeling or hypothesizing.
About CORE INSIGHT Enterprise

CORE INSIGHT Enterprise is a security testing and measurement solution that allows you to:

- **Automate continuous, proactive and goal-based testing of web, network and client-side security**
  - Identify real, exploitable threats to business assets with no false positives
    - Ability to throttle volume and type of tests
  - Monitor for changes in security posture over time and as new systems are added
  - Attack simulation

- **Measure precisely if your most critical assets are exposed to breaches, with prioritized testing against prioritized assets**
  - Management and regional dashboards
  - Reports that detail real-world exposures for business, IT and security
  - Determine affect of changes on infrastructure

- **Manage volumes of data from disparate security technologies to pinpoint the most critical exposures**
  - Measure effectiveness of other security investments
  - No wading through reams of data – identify critical issues quickly and efficiently
Step 1: Environment Profiling

- Tell INSIGHT about your environment topography, for instance:
  - Import info from your network asset mgt solution or network / web scanner
  - Provide a range of IPs
  - Provide a range of web application URLs
  - Provide a list of end user email addresses
Step 2: Campaign Definition

- Define the goal of the INSIGHT assessment campaign (e.g., access a specific customer database).

- Define the scope of systems to be tested (e.g., a specific subnet).
  - Define which systems are in and out of bounds for the campaign
  - Optionally, delegate campaigns to IT staff who own the systems, web app developers, etc.

- Establish the campaign schedule (e.g., once, daily, weekly, etc.).
Step 3: Attack Path Calculation

- INSIGHT profiles systems defined by the campaign and identifies potentially vulnerable systems.
- INSIGHT’s attack planning algorithm combines knowledge of system profiles with GPS-like intelligence to determine most likely path(s) to achieve the campaign goal.
- INSIGHT weights potential paths based on exploit efficacy, leveraging CORE IMPACT’s usage statistics and our unique research and field expertise.
Step 4: Attack Replication

- CORE INSIGHT’s Exploit Engine replicates an attacker’s attempts at compromising systems along the paths.
- Can target web applications, network systems, endpoint systems and end users (via phishing).
- All exploits are commercial-grade, developed in-house, and repeatedly updated, QAed and tested.
- Product receives 20-30 new exploits and other modules per month.
Step 5: Adaptive Path Adjustment

- Uses GPS-like intelligence to adjust and recalculate Attack Paths as it attempts to compromise systems, like an attacker would.

- Stays “in bounds” as defined in the campaign.

- Only tests calculated attack paths
  - Less disruptive than scanning
  - Stealthy attacker behavior

How CORE INSIGHT Enterprise Works

1. Environment Profiling
Tell INSIGHT about your environment.

2. Campaign Definition
You define critical IT assets (aka goals), scope and timing.

3. Attack Path Calculation
INSIGHT calculates likely attack paths to your defined assets.

4. Attack Replication
INSIGHT attempts to exploit vulnerabilities along the paths.

5. Adaptive Path Adjustment
INSIGHT seeks new paths as systems are compromised.
Step 6: Infrastructure Change

- Newly deployed systems that fall within the scope of a campaign (e.g., and IP range) can automatically be tested the next time a campaign is run.
  - Ensures that security tests keep up with your changing environment

How CORE INSIGHT Enterprise Works

1. Environment Profiling
   Tell INSIGHT about your environment.

2. Campaign Definition
   You define critical IT assets (aka goals), scope and timing.

3. Attack Path Calculation
   INSIGHT calculates likely attack paths to your defined assets.

4. Attack Replication
   INSIGHT attempts to exploit vulnerabilities along the paths.

5. Adaptive Path Adjustment
   INSIGHT seeks new paths as systems are compromised.

6. Infrastructure Change
   Campaigns can automatically adapt as you deploy new systems.
Step 7: Dashboard / Reporting

- Details real potential for breach of critical assets with no false positives.
- Shows where defenses stop attacks.
- Reveals exposures to attacks that combine different techniques and vectors.
- Details attack paths and penetration points for remediation planning.
CSO Dashboard + Reporting

- **Assessment and risk trends**
  - Show the progress of security testing and vulnerability remediation over time

- **Heat maps**
  - See the current security standing of operational areas throughout your IT environment
  - Filter by geographic location, business unit, system category, data category, or compliance area

- **Active campaigns**
  - Monitor test coverage and frequency
  - View the progress of active tests

- **INSIGHT updates**
  - Monitor IMPACT’s library of commercial-grade exploits and other testing modules
  - Ensure that tests address latest threats

- **Emerging Threats**
  - Test for newly discovered vulnerabilities

- **Executive and technical reports**
  - Drill-down to details for conducting further analysis and taking action
  - Focus in on specific operational areas and test campaigns
  - Access quantifiable data and contact info for asset owners and security testers

**INSIGHT presents test results in terms specific to your organization:**

- **Your systems** for financial transactions, operations controls, etc.
- **Your databases** containing customer records, financial data, patient histories, etc.
- **Your data types**, such as credit card numbers, social security numbers, etc.
Assessment and Risk Trends:
Measure security testing and vulnerability remediation over time

- Chart potential breaches (i.e., Goals achieved) and penetration points (i.e., exposures forming paths to Goals) by day, week, month, etc.

- Demonstrate progress to management and other stakeholders

- Compare Campaigns by geographic location, business unit, system category, data category, or compliance area
CORE INSIGHT Benefits

• Provides definitive answers about IT security risks
  • Measures precisely if your most critical assets are exposed to breaches

• Saves time, makes your team more efficient
  • Cuts through security data volume and identifies exposures that matter

• Determines the best use of resources
  • Extends value of current investments in people and technology

• Reduces exposures, minimizes threat surface through testing
  • Helps you answer question, “are we more secure than we were yesterday?”
Next Steps

Mike Yaffe
Senior Director, Enterprise Marketing
Office: (617) 695-1107
Mobile: (781) 864-6096
mike.yaffe@coresecurity.com

Tim Byrne
Senior Sales Engineer
Office: (617) 695-1141
Mobile: (617) 281-6898
tim.byrne@coresecurity.com