Demonstrating the Business Value of Security

By Bob Hayes
Security Executive Council Staff
Date: August 10, 2006
Securing the enterprise is a value proposition. Cost consciousness and proactive management is a fundamental expectation of shareholders. What measures and metrics best convey security's value?

Council members and staff engage in benchmarking and common practice documentation, case studies demonstrating security ROI, building a comprehensive library of security-related metrics and measures, and helping to document programs' contributions to managing risk and enhancing internal influence and corporate value.
Security Program Evolution: Core to Emerging Approach
Council Initiatives

Strategic Initiatives

- Risk Management
  - Regulation & Compliance
  - IT Security / Cyber-Crime
  - Intellectual Property
  - Product Protection / Supply Chain
  - Core Program Documentation & Risk Assessment
  - Terrorism / WMD

- Business Continuity
  - Emergency Preparedness / Incident Prevention
  - Public/Private Partnership
  - Crisis Management
  - Managing First Response & Recovery

- Leadership Management
  - Executive Development
  - Enhancing Influence
  - Meeting the Regulatory Challenge
  - Enterprise Security / Leadership Convergence
  - Strategic Planning, Program Validation and Business Alignment

- Value Equation
  - Security Practices / Benchmarking
  - Metrics That Matter and Benchmarking
  - Returning Value & Managing Cost & Benchmarking
Looking at Security Costs

- **YESTERDAY’S business view of security**
  - Security is a staff function
  - Security is a cost with no return
  - Security is fungible

- **TOMORROW’S Business view of security**
  - Security enhances profit
  - Security reduces costs in excess of its expense
  - Security is a differentiator
## Security Scorecard

<table>
<thead>
<tr>
<th>Financial Contribution (Business and Shareholder):</th>
<th>Customer Contribution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security programs increase profits, reduce costs.</td>
<td>Security programs enhance customer relations and protect the brand.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee/Operational Contribution:</th>
<th>Awareness/Growth &amp; Maturity Contribution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security programs enhance productivity and reduce attrition.</td>
<td>Security programs enhance the awareness of risks and compliance issues.</td>
</tr>
</tbody>
</table>
Characteristics

- **VARIABLE COSTS**
  - One-time events
  - Function of scale
  - Unpredictable
  - Hard to control

- **FIXED COSTS**
  - Predictable
  - Measurable
  - Identified
  - Controllable
Variable Costs Vs Fixed Costs

Fixed
Examples:
- Facilities protection
- Employee protection
- Brand protection
- Due diligence
- New employment verification
- Insurance

Variable
Examples:
- Brand exposure
- Crisis exposure
- Internal theft and fraud
- External theft and fraud
- Reconciliation expense
- Outsourcing failure
- Violence in the work place
Security’s Value?

- You can measure where/how security programs enable the business to do what would otherwise be too risky
- A risk prevented is a cost avoided. You can demonstrate how an eliminated vulnerability could enable the bad guy
- You can:
  - measure your costs against accomplishments
  - estimate the cost of a dishonest employee,
  - demonstrate customer satisfaction
  - demonstrate the impact of a security-aware employee
  - measure your costs and results against peers
  - demonstrate how security’s competencies mitigated a risk
- If they understand and support your mission and you have exceeded expectations, you have undoubtedly added value.
Measurable Indicators of Security’s Influence

- Senior management exhibits clear support for security policy.
- Security’s customer base exhibits broad knowledge of security policy and risk awareness.
- Security’s programs have a positive impact on the ethical hygiene of the organization.
- Security has sufficient resources to accomplish the mission.
Expanding Internal Influence

Corporate Security - Protecting Critical Business Assets

An Executive-Level Agenda For Tackling Today’s Top Security Threats

Corporations must protect their assets, employees and customers from an ever-evolving threat matrix. But where does one begin? How can executives make informed decisions that will benefit the entire organization while responsibly using resources to reduce risk and employ appropriate countermeasures? Read this article to learn more about how to communicate the import, impact and implementation of effective corporate security.

CSO Magazine CIO Magazine Forbes Magazine - November 2005
CSOEC Operational Metrics Benchmark Database

Note: Only the Industry category will be used in benchmarking. Other information is used to evaluate the validity of data. * Required

Name: 
* Title: 
* Email Address: 
Phone number: 
* SIC Code (Industry): 
* State/Province: 
Country: 
Annual Revenues: 
Company Name: 
Company Website: 
Are you involved in the sale of products or services to people or companies outside of your corporation? Y   N

Select a topic:
> Security Related Trends - General
> Communicating Risk Knowledge
> Audit Implications
> Background Investigations
> Due Diligence Examinations
> Business Conduct & Reputational Risk
> Criminal Incidents and Investigations
> Security Operations, Physical Security & Premises Protection
> Informational Risk Management
> Contingency Planning & Business Continuity
> Business-based Security Programs
> Confidence with the Corporate Security Functions
> Management, Professional Development & Employee Satisfaction

Submit
A Possible CSO Dashboard

- **SECURITY COST**
  Security cost per dollar of revenue is up past 2 quarters

- **INFO SECURITY**
  14% decrease Q2 vs. Q1 in devices with appropriate patches installed and current

- **BUSINESS CONDUCT**
  Year-to-date investigative results indicate 20% increase in non-compliance with business conduct policies

- **SECURITY AUDITS**
  100% of all notable security-related audit findings have been successfully resolved

- **PRE-HIRE BI's**
  99% of all new hires have completed & resolved background investigations

- **BUSINESS CONTINUITY**
  17% of critical business processes do not have up-to-date & tested response plans
Benchmarking Security Operations

Security Officers per occupied sq. ft.

Corporation Security

A

B

C

D

Employees per Security Officer

A

B

C

D

E

F

G

H

I

J

K

0

25

50

75

100

125

150

175

200

225

250

275

300

325

350

375

400

425

450

475

500
Charting A Solution

- Badge Awareness Program
- Access limitations Imposed at key entries
- Public/Private Communications
- Commence ticketing unsecured laptops
- Cable locks Installed
- Security commences seizing unsecured laptops
- Key arrests made
Critical Reminders

- The absence of security problems have huge, often, underappreciated value.
- Develop metrics that reflect enterprise savings
- Identify reducing variable costs beyond the fixed cost of the security program
About The Council:

The CSO Executive Council is a professional membership organization for leading senior security executives spanning all industries and both the public and private sectors. Our members seek repeatable innovative issue solutions and documentation of model core security programs. The Council utilizes professional staff and retained experts (former CSOs from world class companies and content experts) to develop, based on member requirements, strategic services and products for the entire membership. Unlike typical peer-to-peer organizations, the CSOEC does not depend on member volunteers; members are involved in projects only to the extent they desire to be. Our vision is to deliver solutions exceeding those of dedicated security business consultancy firms at a significantly lower cost.

Contact: Bob Hayes, Managing Director
Web: www.csoexecutivecouncil.com
Address: 492 Old Connecticut Path
P.O. Box 9208
Framingham, MA 10701
Phone: 508.988.6843