PART 2 of 2

# Insight into Security Leader Success

## *How to get the Enterprise to Understand the Value of Security*

A SEC Research Finding

SEC

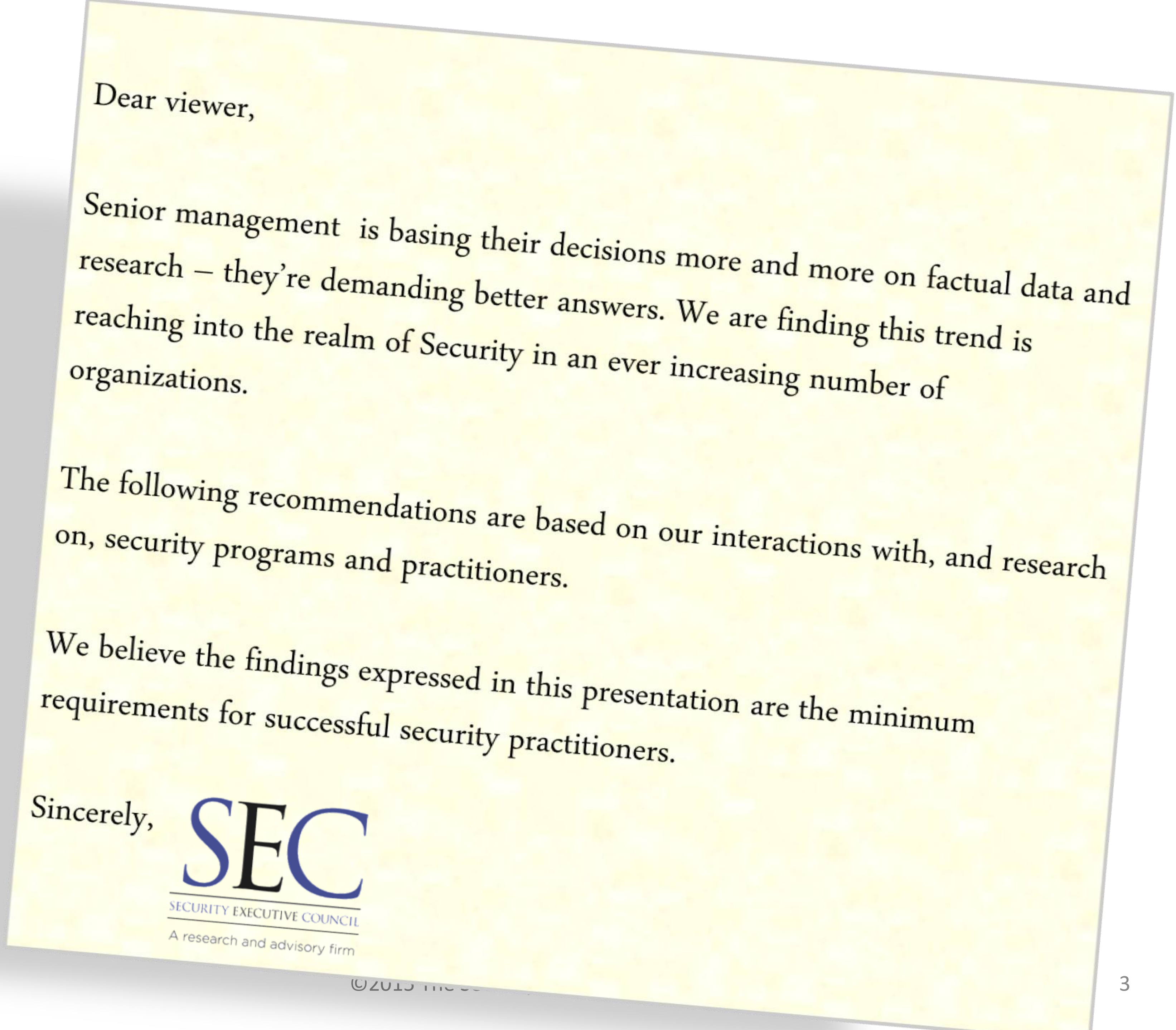
SECURITY EXECUTIVE COUNCIL

A research and advisory firm

# Intended Audience

This presentation is intended for security leaders who want to create a **business-based** security department that **provides value**, and is **valued by the enterprise**.

The following recommendations are based on 10+ years of SEC relevancy-based research.



Dear viewer,

Senior management  is basing their decisions more and more on factual data and research – they're demanding better answers. We are finding this trend is reaching into the realm of Security in an ever increasing number of organizations.

The following recommendations are based on our interactions with, and research on, security programs and practitioners.

We believe the findings expressed in this presentation are the minimum requirements for successful security practitioners.

Sincerely,

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

# Expectations Are Changing

## Old Expectations

## New Expectations

# What does it take to meet the NEW expectations?

# 6

## Communicate in Common Terms and Effectively

# Telling Security's Story

Don't rely on others understanding Security.

The following elements should be considered to help delineate Security and its role; for both yourself and your team, as well as those outside of security:

- History of the program
- Milestones
- Mission/vision statements
- Programs and services
- Timeline of program development
- Service delivery model
- Functional organization chart
- Internal SWOT analysis
- Current state of the program status heat map
- Accomplishments and results
- Internal value analysis status
- Metrics
- Strategic initiatives/strategic plan
- Measuring business value roadmap chart
- Emerging and futuristic trends that will affect the organization and security

# **ALL** staff on Security should be able to tell the story - not just the security leader.

(See I*nsight into Security Leader Success* part 1 page 7 - using Board-Level Risk terminology).

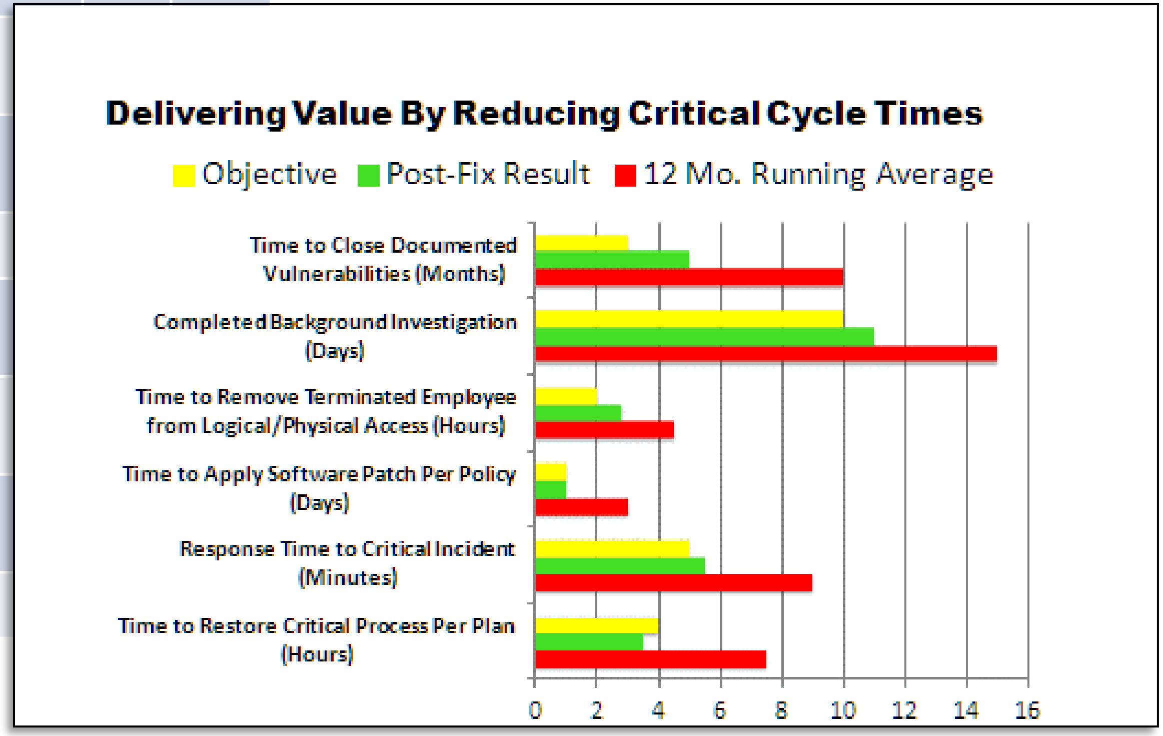
# 7

# Measuring Value and Sharing that Knowledge

# This is OK…

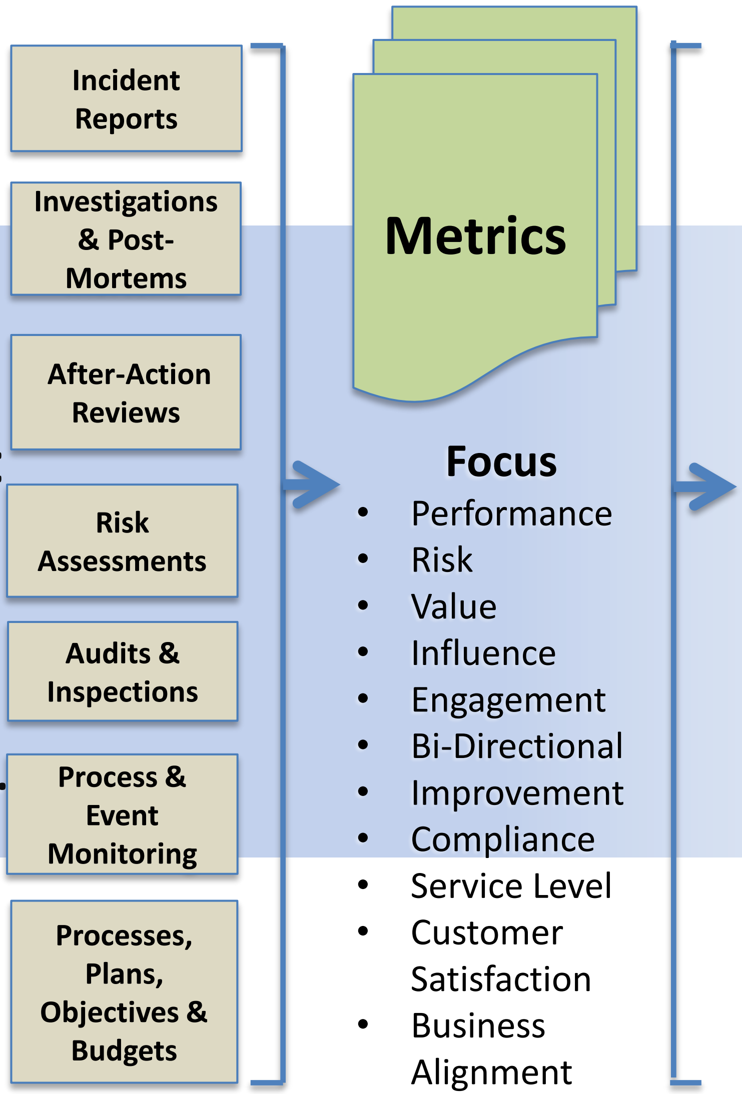
| Activity | January | February | March | April | May | June |
|---|---|---|---|---|---|---|
| Initial Background Investigations Processed | 14 | 27 | 32 | 21 | 37 | 46 |
| Periodic Reviews Processed | 3 | 3 | 13 | | | |
| Orientation & Refresher Briefings | 7 | 10 | 12 | | | |
| Security Policies Developed | 2 | | 2 | | | |
| Data Spill Mitigation/Incidents | 1 | | 1 | | | |
| Secure Area Alarm Responses | 3 | 11 | 5 | | | |
| Internal Incidents/Investigations | 5 | 3 | 2 | | | |
| Foreign Travel Briefings | 5 | | 5 | | | |

# This is Better…



Counting things shows you're active. Instead create a metric that shows performance, value, improvement, customer confidence, etc.

Find *your* meaningful value story that is relevant to *your* company and then tell people about it.



## Embedded Data & Measures

- Incident Reports
- Investigations & Post-Mortems
- After-Action Reviews
- Risk Assessments
- Audits & Inspections
- Process & Event Monitoring
- Processes, Plans, Objectives & Budgets

## Actionable Metrics

Metrics

**Focus**

- Performance
- Risk
- Value
- Influence
- Engagement
- Bi-Directional
- Improvement
- Compliance
- Service Level
- Customer Satisfaction
- Business Alignment

## Communicating The Value Story

- ***Reduced risk & loss attributable to security initiatives / reduced cost of insurance***
- ***Reduced cost of security-related processes and incidents***
- ***Reduced risk to insiders and within 3rd party relationships***
- ***Increased engagement of employees in securing corporate assets***
- ***Assurance of Security response effectiveness***
- ***Assurance of regulatory compliance***
- ***Enhanced ability to satisfy customers with improved methods of protection***
- ***Reduced risk of attack through more measurably effective protective measures***
- ***Reduced recovery time from incidents***
- ***Increased brand protection & market penetration attributable to security measures***
- ***Reduced notable audit findings attributable to security defects***

# 8

# Grasping the Total Cost of Security

# Total Cost of Security ≠ Security Budget

## Definition of total cost of security:

The cost of security, staff and services at all locations that the corporation operates on a worldwide basis. This includes all corporate and IT security elements and the related staff and services, whether proprietary or contractual, managed by the security department *or by other corporate staff groups*.

# Analyzing the Total Cost of Security Can Lead to Valuable Benefits

→ Aggregated costs can point to gaps in security risk mitigation.

→ Total security cost analysis detects duplication of effort and cost savings.

→ Enterprise perspective leads to more effective security program risk mitigation management.

→ Robust data sets offer improved benchmarking comparisons.

→ Helps differentiate between mandatory and discretionary costs.

# Important Factors to Consider:

- ✓ The issue is not “ownership of security programs.”
- ✓ The opportunity is to examine the cost of security to the entity, prioritize program costs against risk and estimated value.
- ✓ Act as an agent of influence in program improvements and costs reduction.
- ✓ Be a positive partner to other entity units to achieve greater value.
- ✓ Define and agree upon metrics measuring success.
- ✓ Benchmark within your sub-sector and outside your sector to identify opportunities and improve.

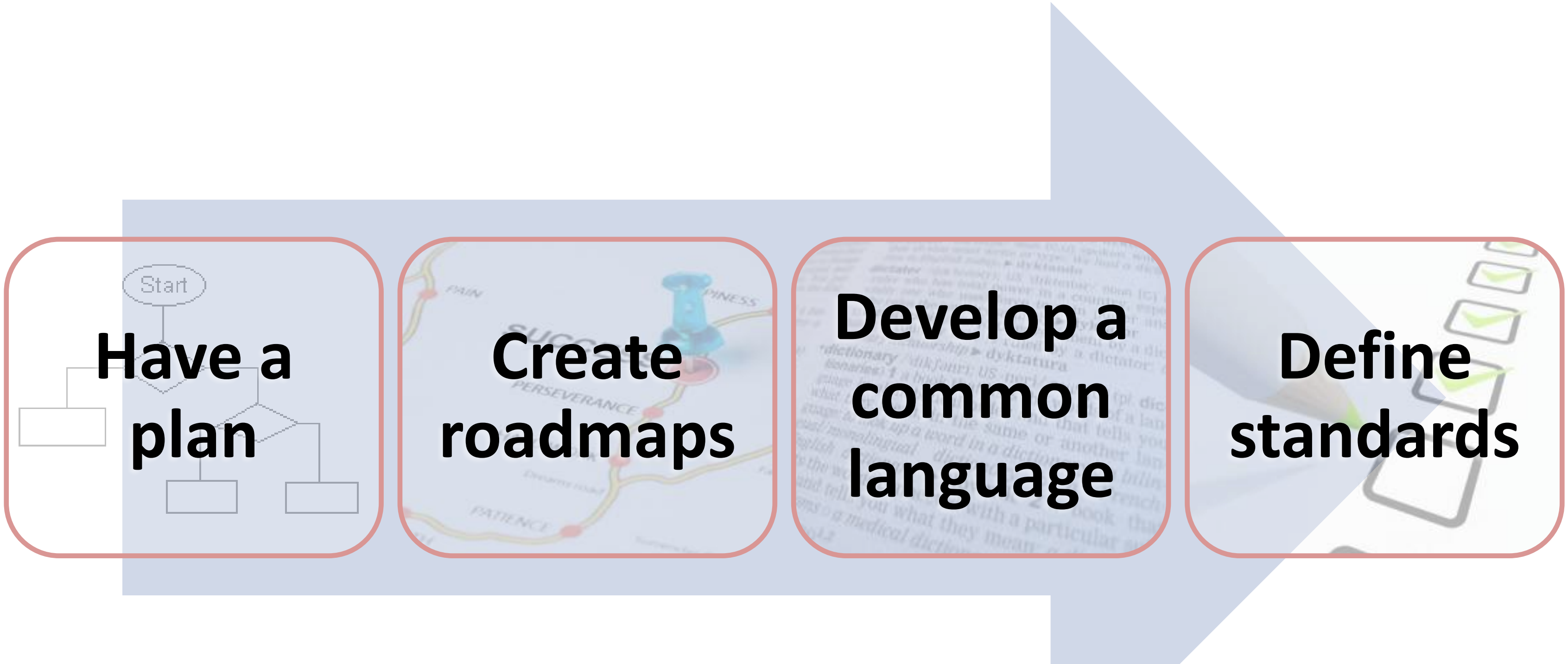
# 9

# Define and Execute a Shared Strategy

# Planning for Success

To help ensure success, a plan for developing a Security program should incorporate the following:

- Conduct enterprise/security risk assessment to define risks
- Conduct gap analysis
- Be able to articulate Security's value
- Define your desired programs and/or develop a service directory
- Decide on the service delivery model
- Establish policy or governance mechanisms
- Determine workload activity
- Develop equipment specifications
- Recalibrate with management
- Create standards for global implementation
- Develop metrics to measure activity and KPIs
- Strive for business alignment



Have a plan

Create roadmaps

Develop a common language

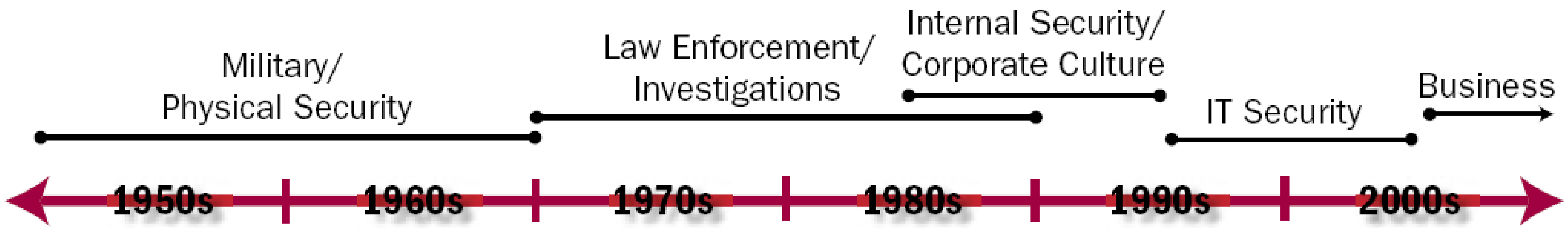
Define standards

Try whiteboard sessions to get everyone thinking and to come to a common ground. Interview internal stakeholder on what they think is important or missing. Create an elevator speech all staff can repeat.

# 10

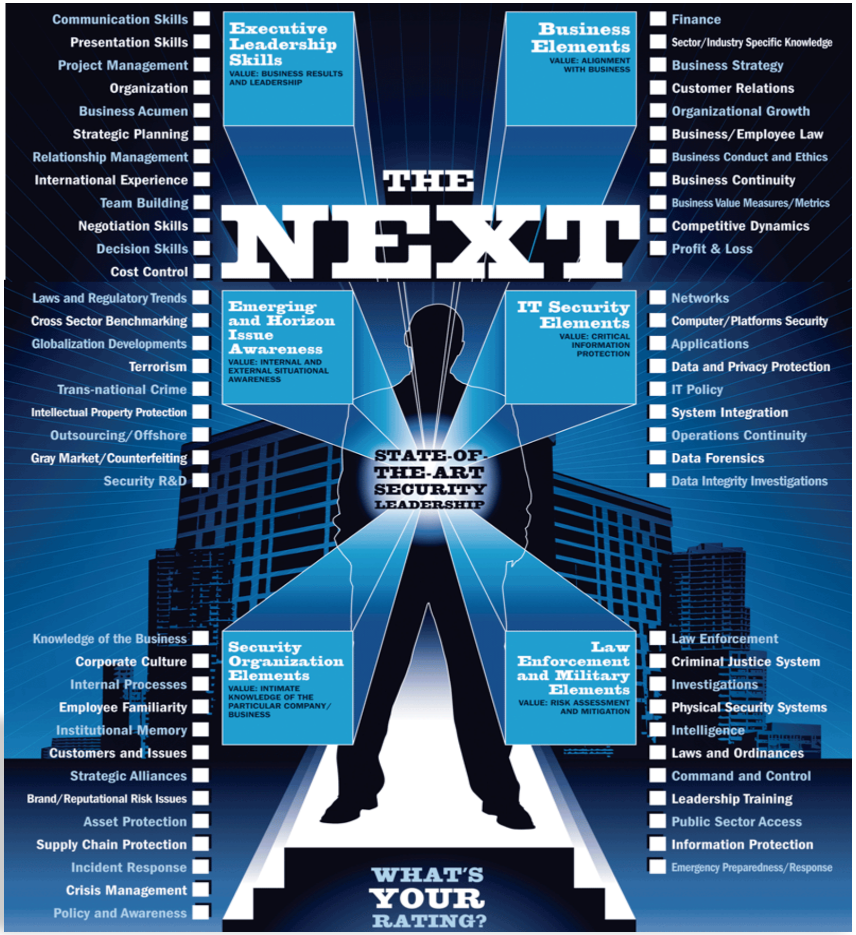
# Develop the Next Generation

# Historical Security Leader Selection: Previous Business Challenges



**Emphasis on various knowledge areas has shifted over the years: From military experience in the 1950s to today's need for a balanced skill-set.**

# Previous Generation Skill Requirements are Evolving



THE NEXT

STATE-OF-THE-ART SECURITY LEADERSHIP

**Executive Leadership Skills**
VALUE: BUSINESS RESULTS AND LEADERSHIP

- Communication Skills □
- Presentation Skills □
- Project Management □
- Organization □
- Business Acumen □
- Strategic Planning □
- Relationship Management □
- International Experience □
- Team Building □
- Negotiation Skills □
- Decision Skills □
- Cost Control □

**Business Elements**
VALUE: ALIGNMENT WITH BUSINESS

- □ Finance
- □ Sector/Industry Specific Knowledge
- □ Business Strategy
- □ Customer Relations
- □ Organizational Growth
- □ Business/Employee Law
- □ Business Conduct and Ethics
- □ Business Continuity
- □ Business Value Measures/Metrics
- □ Competitive Dynamics
- □ Profit & Loss

**Emerging and Horizon Issue Awareness**
VALUE: INTERNAL AND EXTERNAL SITUATIONAL AWARENESS

- Laws and Regulatory Trends □
- Cross Sector Benchmarking □
- Globalization Developments □
- Terrorism □
- Trans-national Crime □
- Intellectual Property Protection □
- Outsourcing/Offshore □
- Gray Market/Counterfeiting □
- Security R&D □

**IT Security Elements**
VALUE: CRITICAL INFORMATION PROTECTION

- □ Networks
- □ Computer/Platforms Security
- □ Applications
- □ Data and Privacy Protection
- □ IT Policy
- □ System Integration
- □ Operations Continuity
- □ Data Forensics
- □ Data Integrity Investigations

**Security Organization Elements**
VALUE: INTIMATE KNOWLEDGE OF THE PARTICULAR COMPANY/BUSINESS

- Knowledge of the Business □
- Corporate Culture □
- Internal Processes □
- Employee Familiarity □
- Institutional Memory □
- Customers and Issues □
- Strategic Alliances □
- Brand/Reputational Risk Issues □
- Asset Protection □
- Supply Chain Protection □
- Incident Response □
- Crisis Management □
- Policy and Awareness □

**Law Enforcement and Military Elements**
VALUE: RISK ASSESSMENT AND MITIGATION

- □ Law Enforcement
- □ Criminal Justice System
- □ Investigations
- □ Physical Security Systems
- □ Intelligence
- □ Laws and Ordinances
- □ Command and Control
- □ Leadership Training
- □ Public Sector Access
- □ Information Protection
- □ Emergency Preparedness/Response

WHAT'S YOUR RATING?

**Business/Organizational Alignment:** Budget, conduct, governance, mission, plan, strategy

**Current/Emerging/Residual/Risk & Compliance:** All-hazards and Board-level Risk  model

**IT:** Applications, architecture, data, forensics, networks, software, tools

**Leadership:** Business case communication, crisis mitigation and team building

**Performance Assurance:** People-Process-Technology, measures and metrics

**Organizational:**  Brand, culture, partner, supply chain, stakeholder  issues

# Selected* performance criteria for Next Generation Security Leaders

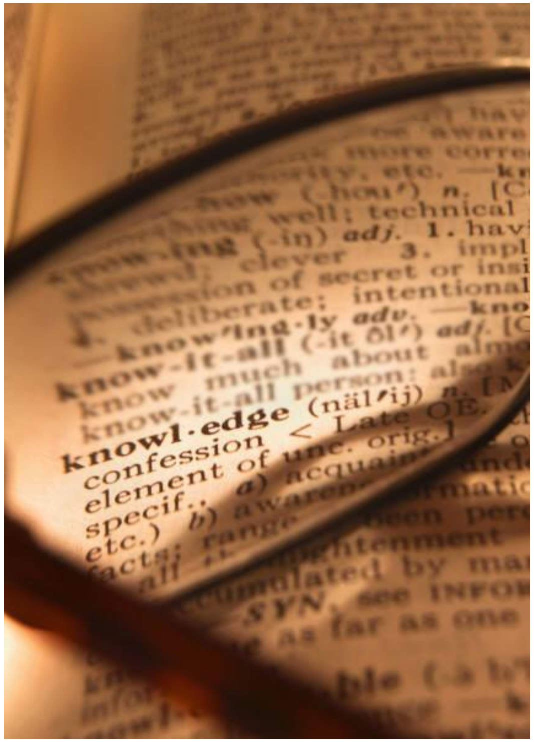
- Align Board Level Risk and business mitigation strategy
- Influence community preparedness and resilience for emerging global risks
- Manage information protection, breaches and situational intelligence
- Add business value with mission assurance and P&L performance
- Deliver performance measures and metrics
- Run security as a business
- Define and deliver operational excellence

© ACEA 2015 / Photo Gilles Martin-Raget

*This is just a subset of the performance criteria we have identified in our research. Contact the Security Executive Council for more information about our Next Generation Security Leader program.*

## This concludes part 2 of *Insight into Security Leader Success*.

This presentation (parts 1 and 2) incorporates aspects of the following SEC developed research and content from the SEC Corporate Security Knowledge Base:



Board-Level Risk Model
Enterprise/Security Risk Alignment Model
Unified Risk Oversight Model
9 Practice of the Successful Security Leader Research
OPaL+ Assessment Research
Security Measures and Metrics Program
Internal Valuation Assessment Model
Next Generation Security Leader Program
Running Security as a Business Research
Regulation and Compliance Management Database
Executive Management Communication Best Practices
SEC Technology Roadmap
And the collective knowledge of SEC staff and subject matter experts (former security executives and security industry leaders)

# We can bring our research and extensive experience to work with you on:

- Aligning security risk mitigation strategies with enterprise risks
- Assessing risks, threats and vulnerabilities
- Creating your value driven metrics program
- Developing and telling Security's story
- Becoming a part of the business-wide risk team
- Aligning organizational readiness, program maturity and leadership strategy
- Contributing to enterprise driven risk compliance
- Running a business-based Security operation
- Transforming the Security organization through powerful executive communication

Contact us. We're a security risk mitigation research and advisory firm. We're made up of former successful security executives. We enjoy exploring how to make Security a valued part of the business.

contact@secleader.com
+1 202.730.9971
https://www.securityexecutivecouncil.com

SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm