Building the High-Performance Information Security Team

Excerpt from the Full Research

To learn more about this full study or to inquire about membership, please e-mail IT.Support@executiveboard.com or call +1-866-913-8101.

Most security functions already have competency models that are often incorrect or inadequately implemented.

- The mistakes shown at right are not mutually exclusive and are often interconnected or cyclical.
- For example, executives or managers may perceive the organization's competency model as generic and choose to ignore it entirely.

COMPETENCY MODELS ARE OFTEN MISUSED OR ABUSED

Common Mistakes in Information Security's Use of Competency Models

	What It Means	Result
 **Using a Statistically Unverified or Generic Model**	Using a generic competency model that is not empirically based and that focuses on a common set of competencies that only seem right	■ Managers focus on improving performance for the wrong competencies. ■ Functional performance stagnates.
 **Paying Lip Service**	Using organizational competency model only required by HR, and otherwise continued reliance on credentials—such as education and certifications—to hire and promote staff	■ Managers make poor hiring and promotion decisions. ■ Qualified job candidates are overlooked and high-quality talent leaves the organization.
 **Striving for Breadth Instead of Depth**	Using an organizational competency model in its entirety without identifying specific competencies to focus on that are most important for security staff	■ Staff are overwhelmed at the number of competencies they are expected to demonstrate and fail to excel at any. ■ Managers are unsure where to focus training and coaching investments.

Source: CEB analysis.

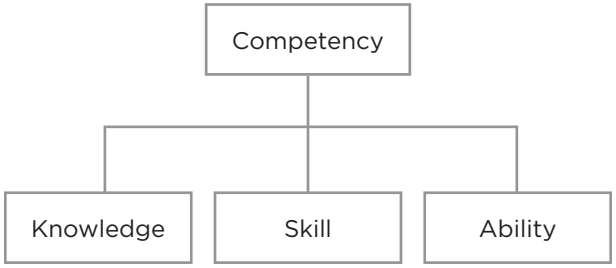
Competencies are a mix of skills, knowledge, and abilities required to deliver a desired objective.

- A finite number of competencies can usually be identified and applied across multiple functions or job families.
- Competencies are usually directly linked to business objectives and strategies—and therefore consider future job requirements either directly or indirectly.

CREATING A COMMON UNDERSTANDING OF COMPETENCIES

Defining Competency

Schematic



Measured via Behaviors: Observable or reportable indicators of a given competency, usually assessed through specific behaviors

Competency Framework for Information Security Staff

Based on CEB IT Competency Framework

1. Analytic Ability
2. Business Results Orientation
3. Decision Making
4. Influence
5. Organizational Awareness
6. Prioritization
7. Communication
8. Creativity
9. Process Orientation
10. Learning Agility
11. Relationship Management
12. Teamwork

Working Definitions

Competency: A set of knowledge, skills, and abilities required to deliver a desired objective

Knowledge: An individual's familiarity with information, facts, or descriptions acquired through experience or education

Skill: An individual's proficiency at performing a learned activity

Ability: An individual's innate proficiency at and potential to perform a specific behavior at a higher proficiency

Source: CEB analysis.

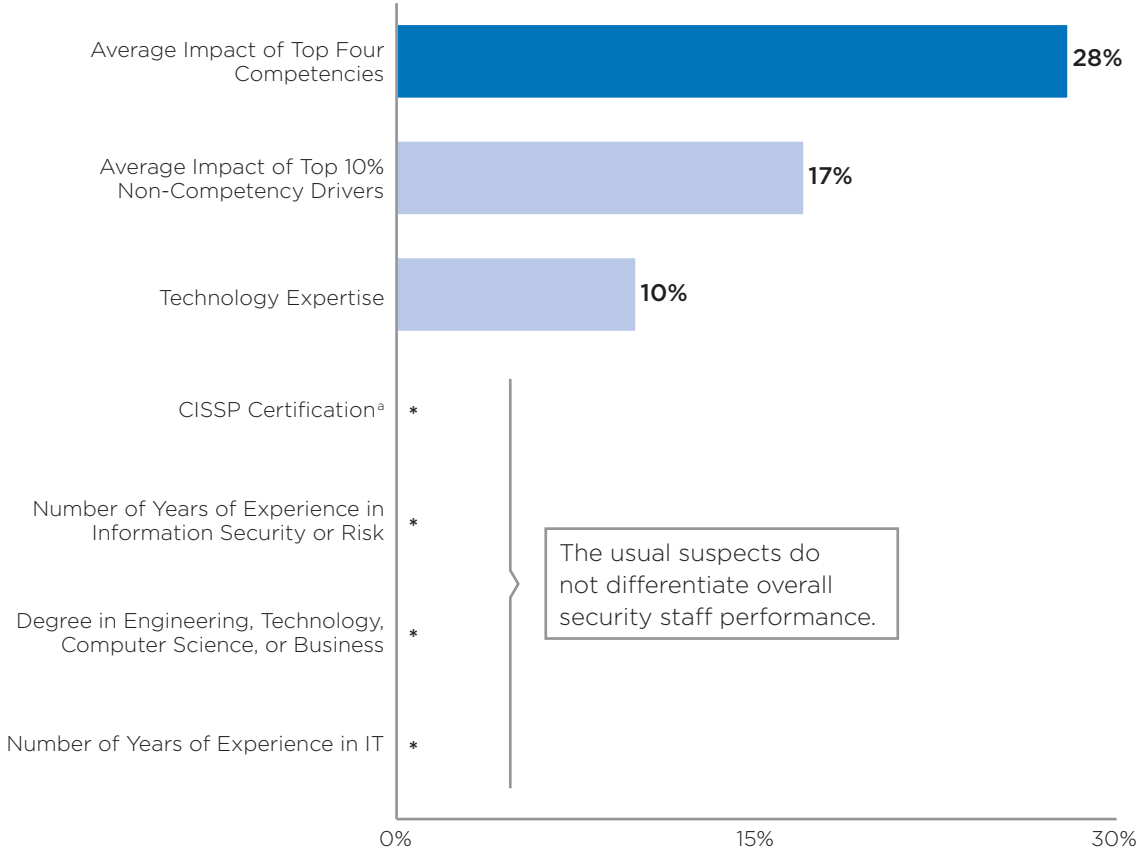
Four key competencies are the most powerful predictors of security staff performance—far more predictive than demographic attributes.

- CISOs unnecessarily narrow their talent pools by ruling out staff with demographic characteristics—such as years of experience, educational background, or professional certifications.
- Our research for heads of HR and Recruiting shows that assessing potential candidates based on the competencies most relevant to their work has a 26% impact on new-hire quality.

FOCUS ON THE COMPETENCIES THAT DRIVE SECURITY STAFF PERFORMANCE

Competencies Drive Staff Performance

Maximum Impact



* Driver is not a statistically significant performance differentiator.

n = 267 information security staff.

Source: CEB 2014 Information Security Talent Survey.

[a] CISSP certification does have a moderate impact on staff performance for certain security activities: risk assessment (8% maximum impact) and security architecture and design (9% maximum impact).

CISOs must focus talent management efforts on the four competencies that define high performance in security staff.

- All 12 competencies are important for security staff to have, but the top four have a disproportionately greater impact on security staff performance.

UNDERSTANDING THE COMPETENCIES THAT DEFINE HIGH PERFORMANCE IN SECURITY

Information Security Staff Competencies

Competency	Definitions
Business Results Orientation	Seeks to understand the business needs and deliver prompt, efficient, quality service to the business
Decision Making	Considers the relative costs and benefits of potential actions to choose the most appropriate one
Influence	Applies different strategies to convince others to change their opinions or plans
Organizational Awareness	Understands the organization's mission, values, operations, and goals
Prioritization	Self-directs activities and works through goal setting, time management, and planning
Communication	Conveys complex and technical issues to diverse audiences
Creativity	Uncovers and implements innovative solutions to address inefficiencies in security processes
Process Orientation	Uses practices, processes, procedures, and systems to manage work and to simplify and use resources efficiently
Learning Agility	Rapidly acquires new knowledge and learns new skills
Relationship Management	Creates relationships with new acquaintances quickly and confidently
Teamwork	Promotes and facilitates coordination and cooperation among peers
Analytic Ability	Effectively uses science, statistics, and computer technology to solve problems

n = 267 information security staff.
Source: CEB 2014 Information Security Talent Survey.

KEY SECURITY STAFF COMPETENCIES MATTER ACROSS THE BOARD

Competency–Activity Alignment Matrix

Maximum Impact on Staff Performance

A. Performance Differentiators: These competencies drive performance across a variety of security activities.

B. Table Stakes: Although these don't explain variations in staff performance, most security staff display a high proficiency in them.

C. Functional Expertise: Functional areas of expertise drive staff performance, but with relatively modest impact.

	Competencies and Functional Areas of Expertise	Prevalence of Proficiency	Business Interfacing	Risk Assessment	Risk Policies and Awareness	Security Architecture and Design	Security Operations	Running the Function
A	1. Business Results Orientation		36%	27%	36%			23%
A	2. Decision Making		23%		26%	18%	24%	26%
A	3. Influence		36%	29%	21%		21%	33%
A	4. Organizational Awareness		40%	20%	35%			32%
	5. Prioritization			22%	25%			
	6. Communication							23%
	7. Creativity			16%				
	8. Process Orientation							
	9. Learning Agility							
	10. Relationship Management							
	11. Teamwork							
	12. Analytic Ability							
B	a. Risk Management			19%	24%			19%
B	b. Technology Expertise					18%		
	c. Policy and Control Knowledge			16%				
C	d. Advanced Threat Monitoring and Detection			12%				
C	e. Regulatory Knowledge							
C	f. Vendor Management							
C	g. Response Management							

n = 267 information security staff.

Source: CEB 2014 Information Security Talent Survey.

Note: Blank fields in the matrix indicate that the driver is not a statistically significant performance differentiator.

Learn More

CEB identifies the best business solutions to challenging functional and IT management problems facing senior IT executives. Our solutions are vendor independent, peer informed, and immediately actionable, helping our members elevate corporate performance by becoming not just better IT managers but better business leaders.

To learn more about membership, please contact:


IT.Support@executiveboard.com


www.cebglobal.com/IT


+1-866-913-8101

CEB
WHAT THE BEST COMPANIES DO