The Balancing Act: Managing Expectations Across the Enterprise

ISE® Southeast Signature Luncheon | March 4, 2015
The Balancing Act - Managing Expectations

The Business
- Expects full protection and security of enterprise while keeping its headcount static
- Perception disconnect between delivery and reality

The InfoSec Organization
- Agile and high-performing
- Jugglers and multi-taskers
- Carries the heavy burden of defending their organizations against unrelenting cyber threats
InfoSec’s Increasing Set of Responsibilities

“To what extent is your firm’s IT security group responsible for the following activities?”

- Security is fully responsible
- Security is mostly responsible
- Security is about half responsible
- Security is slightly responsible
- Security is not at all responsible
- Don’t know

<table>
<thead>
<tr>
<th>Activity</th>
<th>Security is fully responsible</th>
<th>Security is mostly responsible</th>
<th>Security is about half responsible</th>
<th>Security is slightly responsible</th>
<th>Security is not at all responsible</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat and vulnerability management</td>
<td>42%</td>
<td>29%</td>
<td>18%</td>
<td>7%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Endpoint security and network security</td>
<td>42%</td>
<td>27%</td>
<td>18%</td>
<td>8%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Data security</td>
<td>35%</td>
<td>31%</td>
<td>23%</td>
<td>8%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Identity and access management</td>
<td>32%</td>
<td>30%</td>
<td>22%</td>
<td>11%</td>
<td>2%</td>
<td></td>
</tr>
<tr>
<td>Application security</td>
<td>26%</td>
<td>26%</td>
<td>25%</td>
<td>18%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Policy and risk management</td>
<td>25%</td>
<td>31%</td>
<td>26%</td>
<td>13%</td>
<td>1%</td>
<td></td>
</tr>
<tr>
<td>Privacy and regulations</td>
<td>19%</td>
<td>27%</td>
<td>28%</td>
<td>17%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>Third-party security</td>
<td>18%</td>
<td>26%</td>
<td>26%</td>
<td>16%</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>Business continuity/disaster recovery</td>
<td>17%</td>
<td>25%</td>
<td>24%</td>
<td>22%</td>
<td>11%</td>
<td>1%</td>
</tr>
<tr>
<td>Physical security</td>
<td>14%</td>
<td>17%</td>
<td>22%</td>
<td>24%</td>
<td>21%</td>
<td>2%</td>
</tr>
<tr>
<td>Fraud management</td>
<td>11%</td>
<td>17%</td>
<td>25%</td>
<td>23%</td>
<td>14%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Strings Attached: Power and Influence Comes at Price

How CISOs are viewed by Executives:

<table>
<thead>
<tr>
<th>%</th>
<th>Viewpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>54%</td>
<td>CISOs should not be responsible for cybersecurity purchasing decisions</td>
</tr>
<tr>
<td>46%</td>
<td>CISOs should be responsible and accountable for all information security strategies and cyber security technology purchasing decisions.</td>
</tr>
<tr>
<td>44%</td>
<td>CISOs should be accountable for any organizational data breaches.</td>
</tr>
<tr>
<td>31%</td>
<td>CISOs are being hired to address critical gaps in organizations’ information security capabilities.</td>
</tr>
</tbody>
</table>
In spite of the growing set of responsibilities, CISOs struggle to gain support from their C-suite peers, the board HR, etc...

Are you getting the resources you need? How does this affect your ability to fulfill your mission and achieve your strategic goals?
Security Has Become a Team Sport

- An effective information security program can only be achieved when a holistic approach is adopted.
- You need numerous security leaders that specialize and share knowledge to prevent gaps.
- Your leadership team needs to be both technical and business savvy.
- Employees — not technologies — are the ones responsible for security strategy design, implementation, and behavioral change.
- 51% of organizations said it’s a challenge or major challenge to hire security staff with the right skills* - Forrester 2013
The Cost of Not Having a CISO/Leadership Team

- The 2013 Cost of Data Breach Study, issued by the Ponemon Institute, found that companies that had suffered a data breach with a CISO in place experienced reduced costs to the tune of $8 per record. That number was notably higher in the U.S., where organizations without a CISO suffered losses of $23 more per record stolen.

- Security leadership reduces risk/vulnerabilities: leadership serves as a subtle, internal driver for employees and management to consider information security in their big-picture business decisions and in individual, day-to-day actions.

- Effective security leadership means that a data breach is more likely to be discovered, analyzed and responded to more quickly, limiting or often preventing serious monetary damage to a company.
Malicious threats continue to evolve targeting high profile organizations, and without a visible CISO that is accountable for security, you are at a much higher risk for an attack.

According to USA Today, Sony, JP MorganChase, Target, Heartland and TJX did not have a CISOs when breached, emphasizing the importance finding the right candidate quickly and having CISOs overall.

Sony & Sands Casino – the examples are endless. Nation states are looking for areas of opportunity and not having visible security leadership in place opens up that opportunity.

In additional to security strategy and operations, CISOs are also able to be an advocate for security initiatives with the board of directors and HR.
The Challenge: Finding Qualified Leaders

Information security jobs are expected to grow by 53% by 2018

Average annual salary of cyber security worker is $116K

25% of all organizations have a problematic shortage of information security skills

Among the most sought-after professionals in the tech sector with demand for workers in cyber security field outpacing the other IT jobs by a wide margin

Demand for cyber security profs has grown more than 3.5x faster than the demand for other IT jobs over the past 5 years and more than 12x faster than the demand for all other non-IT jobs. Current staffing shortages are estimated between 20,000 and 40,000 and are expected to continue for years.

Bureau of Labor Statistics
Semper Secure Survey
Network World 2014
CIO Magazine 2014
Burning Glass International
Why is recruiting security talent so difficult?

What skills, qualities, attributes are you looking for in your security leadership team?
Salaries Do Not Address Demand & Range of Skills

- In spite of growing demand and range of skill needed, salary needs are not being addressed.

- Complexity drives compensation. There is a trend toward high salaries for security professionals than IT professionals

- HR is NOT recognizing the effect of demand on compensation and as result it is causing you to lose qualified candidates
### Respondent’s perception of security salaries:

<table>
<thead>
<tr>
<th>%</th>
<th>Viewpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>39%</td>
<td>Security professionals report higher salaries for security than IT in their companies</td>
</tr>
<tr>
<td>35-40%</td>
<td>Report having unfulfilled senior security leadership positions for 12-18 months or longer</td>
</tr>
<tr>
<td>50%</td>
<td>Blame their inability to pay competitive salaries as a significant reason that they have unfilled security positions</td>
</tr>
<tr>
<td>50%</td>
<td>Believe the security salaries for their organization are at least 5% lower than salaries for similar positions at competitor companies and within the industry</td>
</tr>
</tbody>
</table>

T.E.N. & IDC Survey, ongoing
Information Security Salary Breakdown

Source: InfoSec Institute
Does Your Company Possess the Right Attributes?

Today’s Cyber Pros Want Employers to Demonstrate Integrity and Leadership

What Are the Most Important Attributes of an Ideal Security Employer?

- Excellence of coworkers: 23%
- Excellence of leadership: 30%
- Expansive cyber security career opportunities: 30%
- Relatively High Compensation Scale: 33%
- Known for addressing leading challenges in cyber...: 33%
- Reputation as a leader in cyber security: 34%
- Reputation for integrity; a code of honor: 44%

Your Opinion

**DISCUSSION**

The cost of hiring: is it worth it?
The Inability to Acquire Security Talent

- No one can do it alone
- Positions are too baffling for many internal talent sourcing departments
- Lack of connections and fatigue rolodexes lead to lost time and poor hiring results
- Too much involved or too complex to be done internally
- Too critical to be trusted to just IT staffing job shops

*Specialized expertise and deep knowledge of the InfoSec Industry and characteristics of core leadership positions is vital*
Are You Aligned with HR?

- **What is your ability to acquire security talent?**
  - Leveraging internal HR – can they assess the skills and abilities?
  - It is a small world but are they an insider?
  - Does your HR/Talent/Recruiting department have the right vendor relationships?

- **Understand your ability to scale your security needs**
  - Why are you looking for security talent?
  - A wrong hire can do more damage than having an open request
  - Aligning with the business
Common Ways that HR Often Falls Short...

Talent acquisition/recruiters are not well trained to understand...

- Necessary security certifications
- Complex layers of security operations and teams
- How to identify candidates that possess understanding of the needed skill sets
- Differing skill sets for various functions in different industries (ie: energy vs financial services vs entertainment/media)
- Where the largest pools of talent are residing

No sense of urgency...

- Does not understands the value of security roles
- Does not understand talent demand to work quickly and attract the right candidates before they are off the market
Case Study

**REAL WORLD EXAMPLE**

What does it look like when the hiring team misses the mark?
"I use to work in the D.C. area and was constantly having my staff and candidates stolen by [the Department of Homeland Security] as well as others in the area that have been very strongly recruiting," he says. "Since moving back to Chicago, I expected to be rid of that challenge. Unfortunately, recently I learned that that one of my better analysts submitted his resignation because he was moving to D.C. to work for DHS."

Arian McMillan, CISO, City of Chicago

ISMG 2014
Initiating Change: Aligning Security with HR

Be Proactive

- Your needs are not top of mind for HR – you must drive change
- It starts with a meeting
- Determine in advance your clear goals and outcomes
  - Regular training for recruiters?
  - Address salary models?

REMEMBER: This is a strategic endeavor. Do not blame HR; focus on collaboration.
You Have their Attention – Sell it!

Who will lead the charge?
- Are you, the CISO, going to work with HR to transform hiring practices? Will you delegate? Who will follow up?
- Recruiters need training to better vet candidates. Who will train them?
  - *Internal security staff? Outside experts like ISE Industry Experts?*

Who will cover the cost?
- Are you allocating enough funds for hiring?
- Who will cover the cost of training?
- Do recruiters need certifications? Who will pay?

Recognize when you need third-party assistance.
Top TEN Reasons for Hiring a Retained Search Company

1. The number one reason: Salary.
2. Your company needs a dedicated partner to fill the position within 30-60 days.
3. You are looking for a specific talent/skill set, or need the "proven" abilities of a market leader.
4. Your company wants an impartial 3rd party to conduct and screen candidates.
5. Confidentiality!
6. Your company would like to benchmark between your internal talent pool and outside candidates.
7. Your company needs a professional who will understand your culture and other environmental nuances that may affect the candidate on the search.
8. Your company needs an outside 3rd party to contact, persuade and convince an executive to leave his/her exiting position.
9. Your company wants more than just a superficial search.
10. Your company wants to make sure that the potential candidate will know that the position is critical to the success of your company and that they are looking for "the best of the best."
An executive search and talent management firm dedicated exclusively to Information Security Executives®

- Retained Search: CISO, CSO, and Core InfoSec Leadership Team Search
- Specializing in security leadership positions in Information Security, IT Risk Management, GRC and Privacy
- Trusted partner that will identify, evaluate, recruit and present top-level candidates to meet our clients’ diverse recruitment and talent management needs

A division of T.E.N., the leading national technology and security executive networking organization that facilitates peer-to-peer relationships between top executives, industry visionaries and solutions providers

- Flagship Program Series: ISE® Executive Forum and Awards

100% Woman Owned Business
Marci McCarthy, CEO and President, T.E.N.

- An award winning technology and information security executive networking and relationship-marketing firm.
- Founder of the ISE® Programs, the premier recognition and networking program for security professionals in the U.S. and Canada
- 2012 recipient of a 4th Congressional District of Georgia citation for fostering greater visibility and professionalism for the IT security industry

Darnell Frymire, President, ISE® Talent, A T.E.N. Company

- Fifteen years of experience in leading and building a leading IT Staffing Company through rapid growth to acquisition
- Understands company cultures and consistently has a track record for matching the right talent
- Respected Leader in the community – TechBridge, TAG, WIT, American Red Cross, WBENC
We have the deep industry knowledge, recruiting expertise and personal connections
• We know who – *is up to the challenge*
• We know what – *skills are required for success*
• We know where – *to find strong candidates*
• We know why – *someone is an excellent fit*
• We know how – *to reach them*

*We focus on high-quality leadership talent – and deliver!*
Your Opinion

**DISCUSSION**

What other reasons do you struggle to gain support and resources? Could it be how you are perceived by your organization?

Do you need a trusted advisor to improve your rapport with peers and the board?
## Where is the Trust?

<table>
<thead>
<tr>
<th>%</th>
<th>Viewpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>28%</td>
<td>Say a decision by their CISO hurt their business’ bottom line</td>
</tr>
<tr>
<td>61%</td>
<td>Do not believe their CISO would be successful in a leadership role outside of Information Security</td>
</tr>
<tr>
<td>73%</td>
<td>Believe their CISO does not contribute greatly to improving day-to-day security</td>
</tr>
<tr>
<td>68%</td>
<td>Believe CISOs do not possess a broad awareness of organization objectives and business needs outside of information security</td>
</tr>
</tbody>
</table>

ThreatTrack Survey, July 2014
ISE® Vantage – Your Business and Career Partner

- **Our ISE® Industry Experts**
  - Highly credentialed IT business veterans – more than 150 years experience combined
  - Possess specialized education and real-world leadership experience in security, technology and risk management

- **ISE® On-Call Services with our ISE® Industry Experts**
  - Board Preparation & Communications
  - B2B Development
  - Leadership Consulting & Executive Coaching
  - Specialty Speaking Engagements
  - Advisory Services

*Imagine being totally prepared for whatever comes your way*
ISE® Industry Experts

Larry Brock
Retired Chief Information Security Officer
DuPont
ISE® Luminary Leadership Award Winner 2009

Rich Jackson
Retired Senior Advisor to the CIO for Cyber Security
Chevron Corporation
ISE® Luminary Leadership Award Winner 2011

Ken Tyminski
Retired Vice President and CISO
Prudential Insurance Company
Biography

Anne Kuhns
Retired Vice-President of Information Security
The Walt Disney Company
ISE® Luminary Leadership Award Winner 2012

Craig Shumard
Principal
Shumard Associates
ISE® Luminary Leadership Award Winner 2010

Kimberly Van Nostern
Retired Chief Security Officer
Allstate Insurance Company
ISE® Midwest Executive Award Winner 2005
ISE® Midwest People's Choice Award Winner 2005
You Are the New ISE®: A Transformative Leader

- Learn to articulate the cost of not having a leadership team to those involved in the hiring process.
- Be proactive: Put your needs on HR’s radar.
- Remember: This is a strategic endeavor. Approach HR with collaborative intent, not blame.
- Develop a collaborative strategy but understand their limitation. Bring in an expert third-party with deep knowledge when needed.
- Communication and perception are key: Rely on a trusted advisor to prepare for board engagements; forge new business relationships to bring value; bring in third party experts for additional support.
T.E.N. and IDC are conducting a survey to identify and compare salary structures and expectations within the information security career field. We would like to invite you to share your personal knowledge and experience. Responses will be analyzed to develop a report and your feedback ensures you are one of the first to receive the report at no cost. By completing the questionnaire, you will also be entered to win a $100 gift card!

All personal information collected will only be used for raffle purposes and distributing reports once they are produced.
ISE® Talent is an executive search and talent management firm dedicated exclusively to Information Security Executives. A 100% woman-owned business, ISE® Talent is a division of T.E.N., the leading national technology and security executive networking firm that facilitates peer-to-peer relationships between top executives, industry visionaries and solution providers.

www.isetalent.com

Marci McCarthy
CEO and President
T.E.N
Direct: 404-920-8582 x101 | Cell: 404.273.3045
mmccarthy@ten-inc.com

Darnell Frymire
President
ISE® Talent, a T.E.N. Company
Direct: 770-331-1805
dfrymire@isetalent.com