The Life and Times of Cybersecurity Professionals

Jon Oltsik
Senior Principal Analyst
Enterprise Strategy Group
@joltsik

Candy Alexander, CISSP CISM
International Board Director
ISSA International
@NH_Candy
Project Overview

- **Second annual project and report**
- **343 completed online surveys** with information security and IT professionals from ISSA member list (and beyond)
- Small/small midmarket (less than 500 employees), large midmarket (500 to 999 employees) and enterprise organizations (1,000 or more employees) in North America, Europe, Central/South America, Africa and Asia
  - 33% small/small midmarket, 8% large midmarket, 59% enterprise
  - 85% North America, 15% other
- **Multiple industry verticals including** information technology, financial, government and business services
Cybersecurity Challenges

29% The cybersecurity staff is understaffed for the size of my organization

28% My organization depends upon too many manual and/or informal processes for cybersecurity

24% Business managers don’t understand and/or support an appropriate level of cybersecurity
# The Cybersecurity Skills Shortage

## 70% of organizations have been impacted by the cybersecurity skills shortage

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing workload on existing staff</td>
<td>63%</td>
</tr>
<tr>
<td>My organization has had to hire and train junior employees rather than hire people with the appropriate level of cybersecurity skills needed</td>
<td>41%</td>
</tr>
<tr>
<td>Cybersecurity staff time is spent disproportionately on high-priority issues and incident response with limited time of planning, training or strategy</td>
<td>41%</td>
</tr>
<tr>
<td>Cybersecurity staff has limited time to work with business units to align cybersecurity with business processes</td>
<td>39%</td>
</tr>
</tbody>
</table>
In your opinion, how vulnerable are most organizations (other than your own) to a significant cyber-attack or data breach (i.e., one that disrupts business processes or leads to theft of sensitive data)?

- 45% Somewhat vulnerable
- 46% Extremely vulnerable
- 9% Not very vulnerable
- Not at all vulnerable
- Don’t know/no opinion
Cybersecurity Professionals’ Opinions

96% AGREE
Cybersecurity professionals must keep up with their skills or the organizations they work for are at a significant disadvantage against today’s cyber-adversaries.

61% AGREE
Security certifications are far more useful for getting a job than they are for doing a job.

59% AGREE
To my knowledge, there are no standards for or agreement on cybersecurity job titles and responsibilities in the industry.
In your opinion, does your current employer provide the cybersecurity team with the right level of training in order for them to keep up with business and IT risk? (Percent of respondents, N=343)

- No, my organization should provide significantly more training so the cybersecurity team can keep up with business and IT risk, 27%
- No, my organization should provide a bit more training so the cybersecurity team can keep up with business and IT risk, 35%
- Yes, 38%
Job Satisfaction

Which of the following are the biggest factors determining job satisfaction for you?

- **42%** Competitive or industry leading financial compensation
- **38%** Organization provides support and financial incentives enabling cybersecurity staff to advance their careers
- **37%** Business management’s commitment to strong cybersecurity
- **34%** The ability to work with a highly-skilled and talented cybersecurity staff
- **30%** Organization provides opportunities for career advancements and promotions
As a former IT professional, which of the following were most helpful when you moved on to a career as a cybersecurity professional?

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking and/or other infrastructure knowledge and skills</td>
<td>57%</td>
</tr>
<tr>
<td>IT operations knowledge and skills</td>
<td>52%</td>
</tr>
<tr>
<td>Gaining experience with different types of technologies and/or applications</td>
<td>51%</td>
</tr>
<tr>
<td>Collaboration between IT and business units on IT initiatives</td>
<td>31%</td>
</tr>
</tbody>
</table>
Which of the following would be the most helpful in getting to the next level career-wise? (Percent of respondents, N=231)

- A mentor or a career coach to help me define a uniquely personal path, 20%
- A standardized career map with progressive training, education, certifications outlined according to job titles or responsibilities, 16%
- Combination of the above, 42%
- Technical training curriculum map, 3%
- Other, 3%
- None of the above, 8%
- Don’t know, 8%
- None of the above, 8%
KSAs

76%
Attending specific cybersecurity training courses

71%
Participating in professional organizations and events
## Certification Value

### Certifications achieved

<table>
<thead>
<tr>
<th>Certification</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEH</td>
<td>9%</td>
<td>12%</td>
</tr>
<tr>
<td>CISA</td>
<td>16%</td>
<td>16%</td>
</tr>
<tr>
<td>CISM</td>
<td>17%</td>
<td>18%</td>
</tr>
<tr>
<td>Comp TIA Security+</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>CISSP</td>
<td>17%</td>
<td>17%</td>
</tr>
</tbody>
</table>

### Certifications important in getting job

<table>
<thead>
<tr>
<th>Certification</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEH</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>CISA</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>CISM</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>Comp TIA Security+</td>
<td>8%</td>
<td>8%</td>
</tr>
<tr>
<td>CISSP</td>
<td>8%</td>
<td>48%</td>
</tr>
</tbody>
</table>

Skills Shortages and Opportunities

<table>
<thead>
<tr>
<th>Skill</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security analysis and investigations</td>
<td>31%</td>
</tr>
<tr>
<td>Application security</td>
<td>31%</td>
</tr>
<tr>
<td>Cloud computing security</td>
<td>29%</td>
</tr>
</tbody>
</table>
Future Actions

43% Add cybersecurity goals as metrics to IT and business managers

41% Document and formalize all cybersecurity processes

36% Make organizational changes so that the cybersecurity and IT departments have the right tools and compensation

35% Provide more cybersecurity training to infosec and IT teams
THANK YOU!

Jon Oltsik
Senior Principal Analyst
Enterprise Strategy Group
@joltsik
jon.oltsik@esg-global.com

Candy Alexander, CISSP CISM
International Board Director
ISSA International
@NH_Candy