ESG Brief

Cybersecurity Skills Shortage: A State of Emergency

Date: February 2016  Author: Jon Oltsik, Principal Analyst, Doug Cahill, Senior Analyst, and Bill Lundell, Director of Research

Abstract: ESG has been researching, writing about, and addressing the cybersecurity skills shortage for a number of years. Unfortunately, this situation continues to deteriorate. In a disquieting development, nearly half of organizations now claim to have a problematic shortage of cybersecurity skills. Additionally, a vast majority of organizations acknowledge that it is difficult to recruit and hire cybersecurity talent. ESG believes that this trend represents a national security risk demanding a comprehensive strategy from national governments.

Overview

ESG recently completed its annual IT spending intentions survey of 633 senior IT and cybersecurity professionals at midmarket (i.e., 100 to 999 employees) and enterprise (i.e., 1,000 or more employees) organizations across North America, Western Europe, and Asia Pacific.¹ As part of this research, ESG asks survey respondents where their organizations have a problematic shortage of specific IT skillsets. For the past four years, information security/cybersecurity topped the list of skills shortages and in 2015, 28% of organizations claimed to have a problematic shortage of cybersecurity skills.

While ESG expected the cybersecurity skills shortage to continue, Figure 1 reveals this year’s results to be especially distressing—46% of organizations now claim that they have a problematic shortage of cybersecurity skills, which is up significantly from last year when just more than one-quarter (28%) of respondents categorized their lack of cybersecurity skills as problematic. This is an especially alarming upsurge given more modest annual increases in the past (i.e., 23% in 2013, 25% in 2014, and 28% in 2015).

The cybersecurity skills shortage manifested itself in the form of an opportunity as well. Specifically, when these senior IT and cybersecurity professionals were asked to identify the areas in which skills development would be the most beneficial to their employees’ career paths, and ultimately to the organization as a whole, 44% pointed to cybersecurity (see Figure 2). To put this into perspective, this is nearly double the number of respondents who said big data analytics, which has been among the most talked and written about subjects in IT over the last several years.

¹ Source: ESG Research Report, 2016 IT Spending Intentions Survey, to be published.
FIGURE 1. Areas of IT Skills Shortage

![Graph showing the areas of IT skills shortage. The bar chart indicates the following percentages for each area: Cybersecurity 46%, Mobile application development 37%, Business intelligence/data analytics 36%, Social media/marketing technologies 34%, Enterprise mobility management 31%, Server virtualization/private cloud infrastructure 31%, Compliance management, monitoring and reporting 30%, Social enterprise/collaboration technologies 30%, IT architecture/planning 30%, Application development 28%, Data protection 27%, Database administration 25%, Help desk/service desk 24%, Storage administration 24%, Server administration 22%, Network administration 22%, We do not have any IT skills shortages 12%, Other 1%, Don’t know 2%. Source: Enterprise Strategy Group, 2016.]

FIGURE 2. Where IT Managers See Career Growth Potential

![Pie chart showing the areas where IT managers see career growth potential. The chart indicates the following percentages for each area: Cybersecurity (i.e., information security) 44%, Big data analytics 26%, Infrastructure management 17%, Application development and deployment 12%. Source: Enterprise Strategy Group, 2016.]

In which of the following areas do you believe your IT organization currently has a problematic shortage of existing skills? (Percent of respondents, N=627, multiple responses accepted)

- Cybersecurity: 46%
- Mobile application development: 37%
- Business intelligence/data analytics: 36%
- Social media/marketing technologies: 34%
- Enterprise mobility management: 31%
- Server virtualization/private cloud infrastructure: 31%
- Compliance management, monitoring and reporting: 30%
- Social enterprise/collaboration technologies: 30%
- IT architecture/planning: 30%
- Application development: 28%
- Data protection: 27%
- Database administration: 25%
- Help desk/service desk: 24%
- Storage administration: 24%
- Server administration: 22%
- Network administration: 22%
- We do not have any IT skills shortages: 12%
- Other: 1%
- Don’t know: 2%


In which of the following functional areas do you believe skills development would be most beneficial to your employees (i.e., IT staff) in terms of their career path and benefit to your organization? (Percent of respondents, N=627)

- Cybersecurity (i.e., information security): 44%
- Big data analytics: 26%
- Infrastructure management: 17%
- Application development and deployment: 12%

Cybersecurity Skills Trends

Nearly half of all organizations surveyed claim to have a problematic shortage of cybersecurity skills, but are these skills in any particular area? To some extent. As the ESG data illustrates, one-third of organizations say that their biggest cybersecurity skills need is for cloud security specialists (see Figure 3). This shouldn’t be particularly surprising since many organizations are aggressively moving workloads to cloud-based environments and thus need to find employees who know how to protect and monitor this activity. Beyond cloud however, ESG is troubled by many of the other needs such as network security specialists, security analysts, and data security specialists. These are standard cybersecurity skills by any measure, so this data indicates that many organizations remain understaffed and under-skilled in core cybersecurity domains.

FIGURE 3. Cybersecurity Areas with Biggest Skills Deficiency

<table>
<thead>
<tr>
<th>Area</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud security specialists</td>
<td>33%</td>
</tr>
<tr>
<td>Network security specialists</td>
<td>28%</td>
</tr>
<tr>
<td>Security analytics</td>
<td>27%</td>
</tr>
<tr>
<td>Data security specialists</td>
<td>26%</td>
</tr>
<tr>
<td>Security engineering</td>
<td>23%</td>
</tr>
<tr>
<td>Security operations</td>
<td>20%</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>15%</td>
</tr>
<tr>
<td>Application security specialists</td>
<td>14%</td>
</tr>
<tr>
<td>Endpoint security specialists</td>
<td>14%</td>
</tr>
<tr>
<td>We don’t have any cybersecurity skills deficiencies</td>
<td>9%</td>
</tr>
</tbody>
</table>


ESG (and others) have been calling attention to the cybersecurity skills shortage for a number of years, but the data presented in this brief indicates that the situation continues to degrade. This point is further evidenced by the fact that 87% of survey respondents claim that it is very difficult, difficult, or somewhat difficult to recruit and hire cybersecurity professionals (see Figure 4). This is consistent with anecdotal stories in which CISOs claim that open requisitions go unfilled for months at a time while cybersecurity staff complains of being constantly overwhelmed by the amount of work at hand, as well as ahead.

How can CISOs stand out from the crowd and attract cybersecurity talent? Competitive salaries are table stakes when it comes to being competitive in recruiting (see Figure 5). Beyond money, however, ESG data indicates that cybersecurity professionals are attracted to opportunities for personal growth such as the ability to work with leading security technologies and processes, side benefits related to training and skills development, and the ability to work in an organization and/or industry targeted by cyber-threats. Clearly, cybersecurity professionals want opportunities that challenge them, educate them, and support them.
FIGURE 4. Difficulty in Recruiting and Hiring Cybersecurity Professionals

In your opinion, how difficult is it for your organization to recruit and hire cybersecurity professionals? (Percent of respondents, N=299)

- Very easy, 3%
- Easy, 10%
- Somewhat difficult, 44%
- Difficult, 29%
- Very difficult, 13%

Source: Enterprise Strategy Group, 2016

FIGURE 5. Factors Most Important to Potential New Cybersecurity Hires

When your organization does recruit and hire cybersecurity professionals, which of the following factors do you believe are most attractive to potential candidates? (Percent of respondents, N=299, five responses accepted)

- Competitive salary: 52%
- The ability for new employees to work with leading cybersecurity technologies and processes: 40%
- Side benefits related to training and skills development: 35%
- Cyber threats associated with your organization or industry: 29%
- The ability for new employees to work with seasoned cybersecurity professionals working at your organization: 27%
- The cybersecurity reputation of your organization: 26%
- The ability for new employees to participate in cybersecurity events: 24%
- The reputation of your CISO and/or other cybersecurity management: 23%

Source: Enterprise Strategy Group, 2016
Driven by continuing cybersecurity skills shortages, many organizations have no choice but to turn to managed and professional services organizations to supplement internal staff. As Figure 6 demonstrates, more than one-third (35%) of organizations engage these firms in preparation for regulatory compliance audits, while 30% leverage these services to help with strategic cybersecurity planning and/or cybersecurity insurance underwriting, the latter of which is a relatively new services need. Additionally, 23% of organizations will outsource some cybersecurity tasks to an MSSP. Given the pervasive cybersecurity skills shortage, this percentage will most likely grow in the future.

**FIGURE 6. Areas Organizations Will Engage a Third-party Services Firm for 2016 Cybersecurity Initiatives and Projects**

In which of the following areas do you believe your organization will likely engage a third-party services firm for consultation on 2016 cybersecurity initiatives and projects?

(Percent of respondents, N=299, multiple responses accepted)

- We will engage a third party to help us prepare for an audit of our compliance with industry regulations, specifically the cybersecurity requirements: 35%
- We will engage a third party to help us with strategic cybersecurity planning with respect to internal policies and procedures: 30%
- We will engage a third party to help us prepare for a cybersecurity assessment as part of the underwriting process for a cybersecurity insurance policy: 30%
- We will engage a third party to help us assess the large number of vendors who offer security solutions: 23%
- We will outsource some of our security management functions to a managed security services provider (MSSP): 23%
- We will not engage a third-party services firm for consultation on 2016 cybersecurity initiatives: 20%

*Source: Enterprise Strategy Group, 2016*

**The Bigger Truth**

ESG has been one of several organizations tracking the cybersecurity skills shortage and sounding the alarm for many years. While a few tactical programs have attempted to address this shortfall, ESG views them as lip service rather than a real solution. Alarmingly, the situation appears to be getting much worse—so much so that ESG now believes that the growing cybersecurity skills shortage represents a national security risk. Simply stated, demand for trained and experienced cybersecurity professionals far exceeds supply. Lacking a comprehensive cybersecurity education and training strategy, large organizations will continue to battle highly sophisticated and well-organized cyber-advocates with their own skeleton crew.