

April 2014

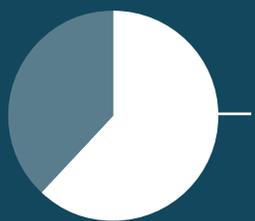
# The Growing Cybersecurity Skills Crisis

Addressing the conflict  
of too many threats,  
too few skilled professionals

Information and technology are delivering increasingly strategic benefits to enterprises today. At the same time, today's cyber environment has become exponentially more dangerous. In the past few years, the numbers of threats, risk scenarios and vulnerabilities have grown at an alarming rate. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Governments and public-sector enterprises are engaging in cyberdefense, as well as, increasingly, offense and attack. If the world continues on this path, it is safe to say that the future expertise and responsibilities associated with cybersecurity will be essential to organizational survival and profitability.

## Increased Cyber Threats

A report by Symantec notes that the total number of breaches in 2013 was 62 percent greater than in 2012, with eight of the breaches exposing more than 10 million identities each.<sup>i</sup> Organizations also face an increase in advanced persistent threats (APTs), which infiltrate a system by stealth, can take months or years to detect and are aimed squarely at commercial gain—typically the theft of credit card information, customer data or proprietary intellectual property. ISACA's research shows that one in five enterprises surveyed in 2013 has experienced an advanced persistent threat, and 66 percent feel it is likely they will be the target of an APT attack.<sup>ii</sup>



**62%**  
more than  
**HALF**  
not increasing  
security training

Despite this increase in cyberattacks, many organizations do not appear to be aggressively increasing the number or skills of their cybersecurity staff. ISACA's 2014 APT Survey found that more than half of the organizations polled (62 percent) are not increasing security training in 2014.

**“It is often not until [businesses] have been hit that they realize there is an issue and a need to be proactive and to put resources into this area.”**

Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, FACS CP, director of information security and IT assurance, BRM Holdich

## “Both classic security skills and advanced skill areas like malware, big data analytics or executive management of security programs are hard to find or very expensive.”

Eddie Schwartz, CISA, CISM, CISSP, PMP, MCSE, vice president of global cybersecurity and consulting solutions at Verizon Enterprise Solutions and chair of ISACA's Cybersecurity Task Force

### Help Wanted: Cybersecurity Professionals

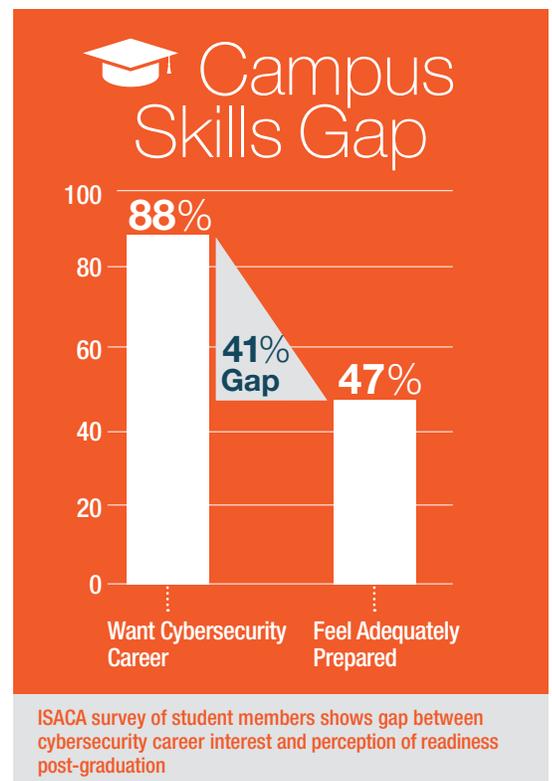
Yet even the enterprises that recognize they need to add cybersecurity professionals to their staff face a daunting challenge—there are more job openings than there are qualified professionals. A study by Cisco estimates that close to 1 million positions for security professionals currently remain unfilled.<sup>iii</sup>

There are several reasons for this shortage. One is that it is not a trivial task to master the knowledge required to become truly effective at threat detection and mitigation. Countering a sophisticated attack by a well-resourced adversary requires much more than a set of baseline security practices. It demands specialist security skills, intelligence-led risk assessments, street-smart education of staff and state-of-the-art forensic analysis skills. Ideal candidates are well-rounded and have a solid foundation in networking, operating systems, web technologies, incident response, and an understanding of the threat landscape and risk management.

### The View From On Campus

Another contributor to the cybersecurity skills shortage is that post-secondary educational institutions are not producing a sufficient quantity of new graduates with the skills to satisfy government and enterprise needs. A number of vendors, government and nonprofit institutions are partnering with universities to provide educational resources on this subject. ISACA, for example, already provides professors with the Model Curriculum for Information Security Management, and is planning to make available cybersecurity case studies, teaching notes and a student book later in 2014. However, this academic/corporate collaboration has not spread across the globe, and the number of cybersecurity-trained graduates emerging from universities in a typical year falls far short of the massive number of new hires and experts needed today.

ISACA recently polled 171 of its student members at academic institutions around the world on the subject of cybersecurity. Fully 88 percent of respondents plan to work in a field or job that requires some level of cybersecurity knowledge. Yet only 47 percent feel they will have adequate cybersecurity knowledge to do the type of job they are seeking when they graduate. Interestingly, only 23 percent said their university does not offer courses in cybersecurity, so concerns about inadequate knowledge cannot be attributed solely to course availability.



### Technology Skills Are Not Enough

Advanced threat vectors and emerging technologies require that cybersecurity professionals be skilled in technology. But that is not enough. Cybersecurity as a discipline includes the social environment of people, enterprises and related processes. In addition to other types of risk, social risk primarily arises from people and their behavior, human factors in IT use, and the emergence of change within the overall system.

To raise awareness of threats within an organization and drive behavior changes, cybersecurity professionals should also be skilled at speaking the language of business, understanding their employer's business strategy and organizational structure, and communicating effectively with employees at all levels in the organization, from the mailroom to the boardroom.

In the event of an incident, these skills are even more important, as the organization's specialist team of IT and cybersecurity professionals, generally referred to as a CSIRT (computer security incident response team), must have the skills to effectively navigate managing a major incident, conducting a forensic analysis, investigating the likely business impact and preparing a post-mortem report for senior management and often board members.

**“Cybersecurity candidates must understand the business they are trying to protect and provide good customer service. If you don’t do those two things, the rest won’t matter.”**

Darren Van Booven, CISSP, CISM, CISA, CPA, chief information security officer, U.S. House of Representatives

## The Need for a Holistic Approach

Cybersecurity is a fast-changing and complex field whose professionals will benefit from access to a foundational body of knowledge, education, and thought leadership from chief information security officers (CISOs) and other security experts working in the industry. As the tip of the spear for cyberattacks, professionals must grapple with several challenges in trying to remain knowledgeable about their work:

- The launch of ISACA’s Cybersecurity Nexus signifies the unique availability of a single, international source of cybersecurity tools and services – professionals no longer have to seek out different organizations for globally recognized and respected certification, networking, knowledge offerings, professional membership, and training and education.
- There is a major need among cybersecurity professionals for opportunities to come together to address complex cybersecurity problems and evolve solutions.
- Cybersecurity mastery is a journey, not a single moment in time. Whether a recent university graduate or a practitioner with several decades of experience, these professionals need information and access to peers and mentors that will evolve as their career evolves.

The growing cybersecurity skills crisis will not disappear in the near future. However, with many companies, schools, government institutions and professional associations raising awareness about the issues and collaborating to identify solutions, strides are being made to broaden the global talent pool of cyber defenders and make progress in the ongoing battle against cyberattacks.

**“If a cybersecurity program is not holistic (for example, it deals only with technology and does not address elements like organization, culture or the human factor), one should not be too optimistic about the effectiveness of the program.”**

Christos Dimitriadis, Ph.D., CISA, CISM, CRISC, head of information security for INTRALOT Group



ISACA defines cybersecurity as the actions related to protecting information assets by addressing threats to information processed, stored and transported by information systems that are internetworked.

## About Cybersecurity Nexus

ISACA’s new Cybersecurity Nexus (CSX) was created to help fill the growing cybersecurity skills gap. According to ISACA’s 2014 APT Study, one in five businesses have experienced an advanced persistent threat (APT) attack, yet 62 percent have not increased security training in 2014. Research by Cisco estimates that close to 1 million positions for security professionals remain unfilled, a finding backed by an ESG report showing that 83 percent of enterprises feel they lack the right skills and IT resources to protect their enterprise.<sup>iv</sup> ISACA’s CSX program offers guidance, career development, education and community for cybersecurity professionals at every stage of their careers. This program is designed not only to meet the needs of the approximately 20 percent of ISACA’s 115,000 constituents who already identify themselves as security professionals, but also to meet the critical mandate that professionals in all disciplines have at least basic knowledge of cybersecurity.

For more information and to view CSX resources, visit [www.isaca.org/cyber](http://www.isaca.org/cyber).

## About ISACA

With more than 115,000 constituents in 180 countries, ISACA® ([www.isaca.org](http://www.isaca.org)) helps business and IT leaders build trust in, and value from, information and information systems.

i. Symantec Internet Security Threat Report 2014, Volume 19  
ii. ISACA 2014 APT Report  
iii. Cisco 2014 Annual Security Report  
iv. Cybersecurity Skills Have and Have Nots, March 2014, ESG