RESEARCH REPORT EXECUTIVE SUMMARY

The State of Cyber Security Professional Careers:

An Annual Research Report (Part I)

By **Jon Oltsik,** ESG Senior Principal Analyst

September 2016

A Cooperative Research Project by ESG and ISSA

Enterprise Strategy Group

Information Systems Security Association International

Contents

Report Conclusions

Report Conclusions

When it comes to cyber security, there is no shortage of frightening data. As a small example:

In 2015, there was a total of 254 publicly disclosed data breaches exposing almost 160 million records of personally identifiable information (source: The Privacy Rights Clearinghouse). This trend continues in 2016. As of this writing, there have been 317 publicly disclosed breaches this year, exposing nearly 5 million records.

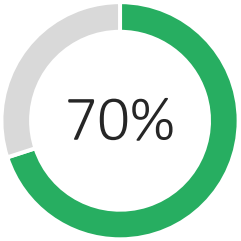
There were approximately 100,000 net new malicious IP addresses created per day in 2015, a significant increase from the 2014 average of 85,000 per day, indicating cybercriminals rely less on the same list of IPs and are expanding to new IPs to avoid detection (source: Webroot).

In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125% increase from the year before. Or put another way, a new zero-day vulnerability was found every week (on average) in 2015 (source: Symantec).

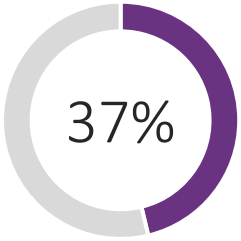
According to the 2016 Verizon Data Breach Investigations Report (DBIR), there were a total of 1,429 incidents of credential theft last year. Attackers used a combination of hacking, malware, and social engineering to steal credentials and then used those stolen credentials to advance their attacks more than three quarters (77%) of the time (Source: Verizon DBIR).

According to the McAfee labs threat report, more than 157 million attempts were made (via emails, browser searches, etc.) each day to entice users into connecting to risky URLs. Furthermore, approximately 55 million users attempted to connect to risky IP addresses, or those addresses attempted to connect to the same user networks each day (source: McAfee Labs Threat Report, 2016).

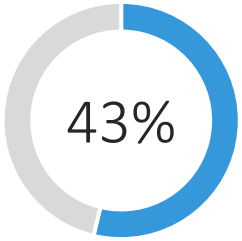
Recognizing an increase in cyber-threats, many organizations are willingly bolstering their cyber security defenses and making cyber security a top business and IT priority. According to ESG research published earlier this year: [1]



Seventy percent of organizations planned to increase their cyber security spending in 2016.



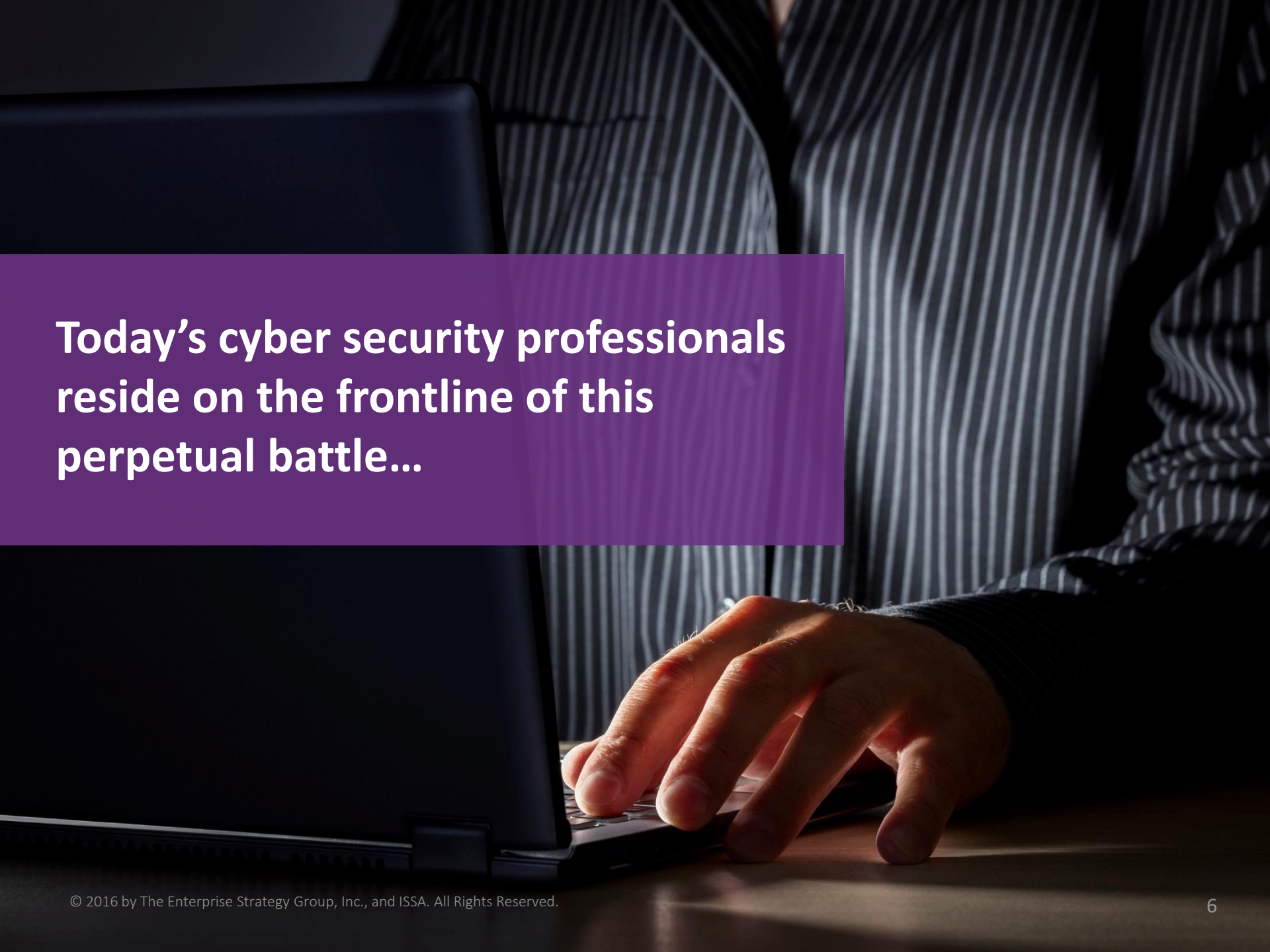
Thirty-seven percent of organizations said that cyber security initiatives are considered to be their highest IT priority for 2016, the largest percentage of all priorities listed.



Forty-three percent of IT professionals said that increasing cyber security is the *business* initiative that will drive the most IT spending at their organizations over the next 12 months.

The data presented here illustrates an escalating and dangerous game of cyber security "cat and mouse." Cyber-adversaries continue to develop creative tactics, techniques, and procedures (TTPs) for attacks. Recognizing the risk, large and small organizations are prioritizing and investing in cyber security defenses and oversight.

Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.



Today's cyber security professionals reside on the frontline of this perpetual battle, tasked with applying limited resources to outthink would be cyber-attackers and defend their organization against everything from embarrassing website defacement through unseemly ransomware extortion to devastating data breaches. Alarmingly, cyber security professionals often accept this challenge knowing they are undermanned for the fight. According to ESG research, 46% of organizations claim to have a problematic shortage of cyber security skills.

Given this daunting responsibility, it's natural to wonder just how well cyber security professionals are holding up. Are they able to coordinate on cyber security strategies and tactics with their business and IT peers? Do they have the skills necessary for their jobs as cyber-adversaries develop new exploits? Are they overwhelmed and burnt out?

To answer questions like these, the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) teamed up and initiated a primary research project in mid-2016 with the goal of capturing the voice and thoughts of cyber security professionals on the state of their profession, and gaining a perspective on situational analysis from those closest to the fight. In pursuit of this goal, ESG and ISSA surveyed 437 information security professionals (and ISSA members). Survey respondents represented organizations of all sizes and included professionals located in all parts of the world.

The cyber security professionals participating in this project were asked a series of questions on a variety of cyber security topics. This report is focused on the lifecycle of cyber security professional careers while a subsequent report (part II in the series to be published later this year) will concentrate on cyber security professionals' opinions about their organizations' cyber security practices as well as the overall state of cyber security today.

Based upon the data collected as part of this project, this report concludes:

Cyber security professionals are attracted by a moral imperative. When asked why they became cyber security professionals, 27% said it gave them the chance to use their technical skills to help protect valuable business and IT assets while 22% claim they were attracted to the morality of the profession. In the mind of many cyber security professionals, their jobs equate to a battle between right and wrong.

The majority of cyber security professionals got their start in IT. More than three-quarters (78%) of survey respondents say that their career started somewhere in IT and then evolved into cyber security. When asked to identify the most helpful skills gained as IT professionals (that can be applied to cyber security) respondents listed attributes like experience with different types of technologies, IT operations knowledge and skills, and networking (technology) knowledge and skills. While these were the top selections, responses did vary based upon experience. More senior cyber security professionals emphasized lessons learned as part of IT collaboration with the business while junior cyber security professionals highlighted technical training.

Most cyber security professionals struggle to define their career paths. Nearly two-thirds (65%) of respondents do not have a clearly defined career path or plans to take their careers to the next level. This is likely due to the diversity of cyber security focus areas, the lack of a well-defined professional career development standard and map, and the rapid changes in the cyber security field itself. Business, IT, and cyber security managers, academics, and public policy leaders should take note of today's cyber security career morass and develop and promote more formal cyber security guidelines and frameworks that can guide cyber security professionals in their career development in the future. Independent organizations such as the ISSA with its Cyber Security Career Lifecycle are taking the lead on such initiatives.

Cyber security professionals have solid ideas for skills advancement. When asked how they improve their knowledge, skills, and abilities (KSAs), cyber security professionals pointed to activities like attending specific cyber security training courses (58%), participating in professional organizations (53%), and engaging in on-the-job mentoring from more experienced cyber security professionals (37%). Responses varied by seniority with experienced cyber security managers (i.e., CISOs, VPs, Directors, etc.) leaning toward professional organizations while cyber security staff members favored on-the-job mentoring.

Cyber security certifications are a mixed bag. Over half (56%) of survey respondents had received a CISSP and felt it was a valuable certification for getting a job and gaining useful cyber security knowledge. Other than the CISSP certification however, cyber security professionals appear lukewarm on other types of industry certifications. Based upon this data, it appears that security certifications should be encouraged for specific roles and responsibilities, but downplayed as part of a cyber security professional's overall career and skills development.

Cyber security professionals are relatively satisfied with their jobs. While 41% of respondents claim to be very satisfied with their jobs, 44% are only somewhat satisfied and 15% are not very satisfied or not at all satisfied. What leads to job satisfaction? Cyber security professionals point to factors like financial compensation (32%), an organizational culture that includes cyber security (24%), business management's commitment to cyber security (23%), and the ability to work with a highly skilled and talented cyber security team (22%). CISOs should strive to make sure that their organizations offer these attributes.

Continuous cyber security training is lacking. When asked if their current employer provides the cyber security team with the right level of training to keep up with business and IT risk, more than half (56%) of survey respondents answered "no," suggesting that their organizations needed to provide more or significantly more training for the cyber security staff. This represents one of the "red flags" uncovered in this research project. Organizations that don't provide continuous training to cyber security staff will fall further behind cyber-adversaries while increasing business and IT risk. This should be an unacceptable situation for all business and technology managers.

Cyber security professionals are in extremely high demand. This is another critical data point exposed in this research project, as 46% of cyber security professionals are solicited to consider other cyber security jobs (i.e., at other organizations) at least once per week. In other words, cyber security skills are "a seller's market" where experienced professionals can easily find lucrative offers to leave one employer for another. Turnover in the cyber security ranks could represent an existential risk to organizations in lower paying industries like academia, health care, the public sector, and retail.

Many CISOs are not getting enough face time in the boardroom. While industry rhetoric claims that "cyber security is a boardroom issue," 44% of respondents believe that CISO participation with executive management is not at the right level today and should increase somewhat or significantly in the future. Alarmingly, this perspective is more common with more experienced cyber security managers (who should be working with the business) than cyber security staff members.

Internal relationships need work. While many organizations consider the relationship between cyber security, business, and IT teams to be good, it is concerning that 20% of cyber security professionals say the relationship between cyber security and IT is fair or poor, and 27% of survey respondents claim the relationship between cyber security and the business is fair or poor. The biggest cyber security/IT relationship issue selected relates to prioritizing tasks between the two groups while the biggest cyber security/business relationship challenge is aligning goals. The report data reveals that cyber security and IT teams are taking steps to improve collaboration but also uncovers that more work is necessary to bridge the gap between cyber security and business management.

CISO turnover has business and economic roots. When asked why CISOs tend to seek new jobs after a few short years, cyber security professionals responded that CISOs tend to move on when their organizations lack a serious cyber security culture (31%), when CISOs are not active participants with executives (30%), and when CISOs are offered higher compensation elsewhere (27%). To retain strong CISOs, organizations must not only provide competitive compensation but also make a serious commitment to cyber security executives and comprehensive programs.

Conclusion

On the positive side, this report reveals that cyber security professionals are relatively happy with their careers and generally agree on what makes a job satisfying or not. Unfortunately, the report also calls out a number of troubling trends including:

1. Many cyber security professionals aren't sure how to develop their career paths.
2. The majority of cyber security professionals aren't receiving the right level of skills development to address the rapidly evolving threat landscape.
3. The cyber security skills shortage has created a job market that is a disruptive force, leading to, attrition, unfilled positions, and perpetual changes in cyber security departments. Overall, these issues can add job-related stress to cybersecurity personnel while making it harder for organizations to protect critical IT assets
4. The relationships between cyber security, business, and IT teams remain a work in progress.
5. Too many organizations are still happy with "good enough" security rather than good security.

These ramifications have a profound impact on cyber security professionals and the organizations they work for.

Top Five Research Implications for Cyber Security Professionals

Top Five Research Implications for Cyber Security Professionals

Cyber security professionals can use the research presented in this report as a guideline for career planning. This is especially true for those in the early stages of a cyber security career or individuals seeking to enter the field. The data suggests that cyber security professionals should:

Invest more time in career development. The report reveals that only 35% of cyber security professionals claim that they have a well-defined career path and plan to get to the next level. This is understandable for several reasons. The cyber security field is in a state of perpetual change, so it can be hard to pinpoint where it is going and how emerging cyber security trends align with career goals. Additionally, many cyber security professionals begin their career with some type of fixed-function responsibility like firewall or email security administrator. Based upon these circumstances, many cyber security professionals maintain a short-term focus, concentrating on the tasks at hand rather than their future career path. Given the variety of cyber security career opportunities, ESG and ISSA believe that cyber security professionals should invest time in career development and planning at all stages of their career lifecycles. This is especially true for junior cyber security professionals who have the opportunity to take their careers into emerging technical areas (i.e., cloud security, IoT security, etc.) or focus on business aspects of cyber security (i.e., risk management, CISO positions, etc.). Cyber security professionals should take the time to explore career possibilities, research appealing options, and map out a career progression to achieve their goals over time.

Look to training and peers rather than security certifications to improve cyber security KSAs. The data indicates that knowledge, skills, and abilities development tends to come from on-the-job experiential training rather than security certifications. Of course, cyber security certifications may play a role for specific types of training, but experienced cyber security professionals seem to develop their skills by networking with peers, and attending training courses taught by cyber security practitioners. Cyber security professionals should join professional organizations/user groups and attend industry events in order to maximize networking opportunities that can help them bolster the skills they need on a daily basis.

Seek out mentors. Closely related to the points above, cyber security professionals should find and learn from mentors throughout their careers. The good news here is that the cyber security world is populated with experienced professionals willing to give back to their community. Seeking out mentors should be one of many "check-box" requirements in all cyber security professionals' career planning to-do list.

Develop business acumen in the early stages of a cyber security career. The research presented in this report reveals that junior cyber security professionals tend to have limited understanding of the business aspects of cyber security. This is understandable as they are probably drawn to the technical side of cyber security, but it's important to understand that business requirements will intersect with cyber security technology as their careers progress. This should be a priority for cyber security professionals with eventual CISO aspirations. To maximize their career development, ambitious cyber security professionals would also benefit by focusing their business training on the how cyber security and business subjects intersect in specific industries. Once again, finding mentors, networking with peers, and learning from experienced tacticians may be the best course of action.

Take advantage of "the seller's market" when appropriate. Recall that 41% of survey respondents say they are very satisfied at their current job, but the data also reveals that 61% of cyber security professionals have had at least one job experience working for an organization that didn't really understand cyber security. Dissatisfied cyber security professionals and those working in "dead end" jobs should realize that they have an unprecedented opportunity due to the current global cyber security skills shortage. As this report reveals, 46% of cyber security professionals are being solicited by job recruiters at least once per week. Before jumping at the next higher paying job, however, cyber security professionals should invest time in career planning as suggested and create a list of ideal conditions for employment. For example, survey respondents indicated that factors like a strong cyber security culture, business managements' commitment to cyber security, and the ability to work with a highly skilled cyber security team help make their jobs satisfying. Job-shopping cyber security professionals should look for new opportunities that include all of these attributes rather than focus on compensation alone.

Research Implications for Employers

Research Implications for Employers

Like it or not, businesses, non-profits, and government agencies are engaged in a competition to attract and retain cyber security talent. To appeal to cyber security professionals at large, these organizations should:

Recruit cyber security professionals from IT when possible, but be creative elsewhere. Eighty-percent of the cyber security professionals surveyed for this report started their careers in IT before proceeding to information security. With no end in sight for the global cyber security skill shortage, CISOs should create a structured program to recruit IT talent interested in cyber security opportunities. Based upon the report data, it may be worthwhile to target candidates who've worked with multiple technologies, those with IT operations and networking technology experience, and those with a background of collaborating with business managers on IT initiatives. Alternatively, it is worth noting that the cyber security staffing shortage may be a function of a myopic HR recruiting strategy centered on the IT resource pool alone. There may be other areas in the business, such as business analysts, with similar skill sets. CISOs should think outside the box and supplement creative recruiting efforts with the right training.

Invest more in cyber security training. Whether teaching IT professionals about cyber security or advancing the KSAs of the existing cyber security team, the ESG/ISSA research points to a profound need for continuing education and training. This is especially important since only 44% of survey respondents believe they receive the right level of cyber security training from their employer today. Investing in leading cyber security professionals will not only improve the effectiveness of the current cyber security staff, but will also help CISOs recruit cyber security professionals seeking an environment where they can develop their skills.

Provide career development advice and services. Aside from training, CISOs should adopt programs and support services to help cyber security team members develop their careers. This effort can include mentoring programs, guest speakers, and organizational participation in cyber security professional organizations. Investments in career development programs can help organizations retain employees and attract new hires seeking cyber security jobs and career guidance.

Assess whether the organization meets the criteria for cyber security job satisfaction. As the research reveals, cyber security professionals are attracted to organizations with strong cyber security cultures, business commitments to cyber security, and those that provide opportunities for skills development and career growth. Alternatively, cyber security professionals are alienated by organizations that relegate cyber security to a low priority, or those that skimp on security budgets, training, and career development. CISOs should survey the cyber security staff to see how the organization is doing in each of these areas and encourage suggestions for improvement.

Find ways to improve cyber security team relationships. As stated throughout this report, relationships between cyber security, business, and IT teams are a work in process that sometimes suffer from poor coordination around tasks, priorities, and overall objectives. CISOs must work with business and IT executives to improve these relationships from end to end. How? Some suggestions include developing cross-functional groups focused on business (rather than IT) initiatives where team members are measured on outcomes, not technical metrics. Cross-training or job rotation programs may present another opportunity to improve empathy and define collective processes and goals. Improving cyber security relationships should be a top-down objective for all organizations, with senior management leading and accountable for improvement. In this regard, CEOs should have oversight into programs and progress in this area while acting as cyber security cheerleaders across the entire organization.

As organizations make progress in the areas outlined above, they should strive to become cyber security centers of excellence by monitoring advancements and striving for continuous improvement. They should also promote their commitment to cyber security to the cyber security professional community at large. These actions can help them improve the effectiveness of their cyber security programs and make them an attractive employer for cyber security professionals at all stages of their careers.

The Information Systems Security Association (ISSA) is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk, and protecting critical information and infrastructure. ISSA members and award winners include many of the industry's notable luminaries and represents a broad range of industries - from communications, education, healthcare, manufacturing, financial and consulting to IT - as well as federal, state and local government departments and agencies. Through regional chapter meetings, conferences, networking events and content, members tap into a wealth of shared knowledge and expertise. Visit ISSA on the web at www.issa.org and follow us on Twitter at @ISSAINTL.

The Enterprise Strategy Group (ESG) is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.