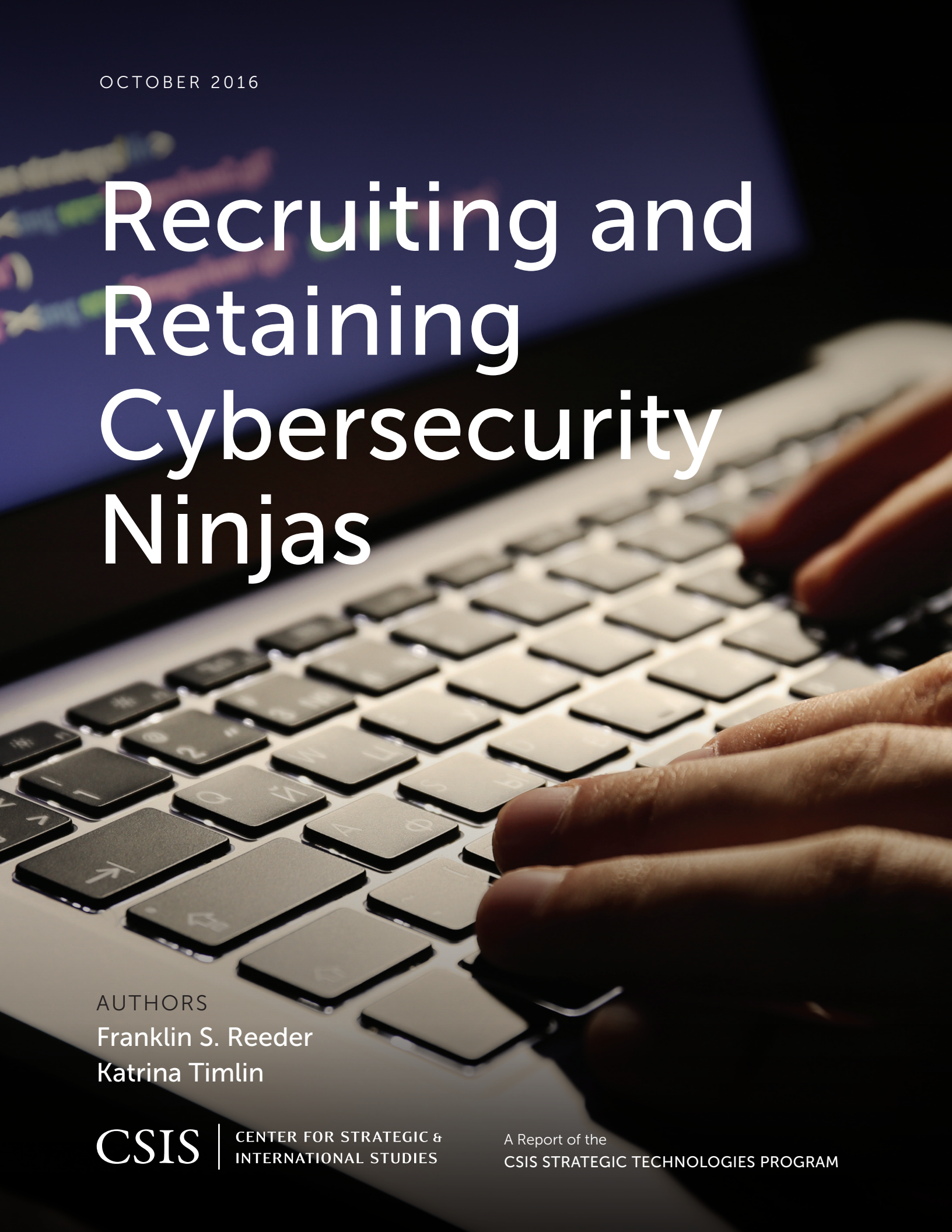
OCTOBER 2016

Recruiting and Retaining Cybersecurity Ninjas



AUTHORS

Franklin S. Reeder

Katrina Timlin

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

A Report of the

CSIS STRATEGIC TECHNOLOGIES PROGRAM

OCTOBER 2016

Recruiting and Retaining Cybersecurity Ninjas

AUTHORS
Franklin S. Reeder
Katrina Timlin

A Report of the
CSIS STRATEGIC TECHNOLOGIES PROGRAM

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

About CSIS

For over 50 years, the Center for Strategic and International Studies (CSIS) has worked to develop solutions to the world's greatest policy challenges. Today, CSIS scholars are providing strategic insights and bipartisan policy solutions to help decisionmakers chart a course toward a better world.

CSIS is a nonprofit organization headquartered in Washington, D.C. The Center's 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look into the future and anticipate change.

Founded at the height of the Cold War by David M. Abshire and Admiral Arleigh Burke, CSIS was dedicated to finding ways to sustain American prominence and prosperity as a force for good in the world. Since 1962, CSIS has become one of the world's preeminent international institutions focused on defense and security; regional stability; and transnational challenges ranging from energy and climate to global health and economic integration.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in November 2015. Former U.S. deputy secretary of defense John J. Hamre has served as the Center's president and chief executive officer since 2000.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Acknowledgments

This report is made possible by the generous support of the SANS Institute.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Contents

Recruiting and Retaining Cybersecurity Ninjas

Franklin S. Reeder and Katrina Timlin

The ability to attract and retain highly skilled cybersecurity staff is one key to a strong defense. While automation and more resilient networks can reduce risk, highly skilled personnel are the key to preventing, detecting, and recovering from cyber attacks.

This project identifies the factors that make an organization the employer of choice for what we call "cybersecurity ninjas"—cybersecurity experts whose day-to-day tasks require higher-level technical skills. Much has been written about the shortage of cybersecurity professionals,[1] but little work has been done on the factors that help high-performing cybersecurity organizations build and keep a critical mass of specialists. This is a first attempt that we expect will prompt discussion on how organizations attract and retain high-end cybersecurity talent.

Executive Summary: Our Conclusions in a Nutshell

1. The results of our survey of cybersecurity professionals show that challenging, high-impact work and continuing investment in *training* are more critical to attracting and keeping all cybersecurity professionals than competitive pay and benefits.

2. Having a flexible work schedule also ranked higher than pay. Ninjas also valued being able to advance without having to assume management responsibilities significantly more highly than non-ninjas.

3. There is evidence of what we call a "Kevin Durant Effect"[2]—highly skilled professionals want to work with others whose talent and work they respect and from (or with) whom they can continue to learn.

4. We found a relationship between certain professional certifications and those who perform ninja tasks. Ninjas hold more and different professional credentials.

---

[1] Karen Evans and Franklin Reeder, *A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters* (Washington, DC: CSIS, November 2010), https://goo.gl/LenzEe; Martin Libicki, David Senty, and Julia Pollak, *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND, 2014), http://goo.gl/NFMqkG; CSIS, *Hacking the Skill Shortage: A Study of the International Shortage in Cybersecurity Skills* (Santa Clara, CA: Intel, July 2016), https://goo.gl/rQ2rkL.

[2] A reference to professional basketball player Kevin Durant, where his move to the Golden State Warriors was prompted by his desire to join a high-performing team.

Key Factors for Retaining Cybersecurity Staff (% who rated the factor "very important")

	Ninjas	Non-ninjas
Engaging and challenging tasks	72	71
Employer pays for training to keep skills current	72	69
Flexible work schedule	67	52
Competitive pay and benefits	58	64
Promotion for technical staff does not require moving into management	46	26

Nothing above should come as a surprise to those who have examined other professions requiring high levels of technical knowledge and prowess. What it suggests, however, is that it should be possible to develop metrics for critical success factors and devise ways to measure how high-performing organizations and their appeal to cybersecurity professionals can be based on more than feel-good factors. Our objective is to help organizations compete to become a cybersecurity employer of choice.

What Talented Cybersecurity Professionals Want from Their Employers

Cybersecurity professionals, like other workers, value employers that provide good benefits, salaries, and job security, as well as workplaces where there is respect and trust between management and employees. Those practices are in fact the "top five contributors to job satisfaction for 2014" as identified by the Society of Human Resource Managers.[3]

Interviews with dozens of highly skilled cybersecurity workers, however, have shown us that, even in organizations that pay and treat their employees well, there can be a great deal of disappointment and early turnover. Some of the reasons for such dissatisfaction are obvious. No matter how good a job may be, there are many other employers willing to pay more and promise greater responsibility to highly talented cybersecurity workers—their skills are in great demand.

This is particularly true for those with scarce skills such as threat analysis, advanced forensics and intrusion analysis, secure programming, and penetration testing. In Silicon Valley, turnover of such employees has become institutionalized, with employers such as Facebook and Google admitting that they do not expect their most talented cybersecurity personnel to stay longer than three or four years.

The literature and our data suggest that there is more to this than a simple bidding war. Anecdotal evidence suggests that many employers have found ways to provide satisfying longer-term careers for some of the most talented people in our field. Among them are the

[3] Society for Human Resource Management (SHRM), *Employee Job Satisfaction and Engagement: Optimizing Organizational Culture for Success* (Alexandria, VA: SHRM, 2015), https://www.shrm.org/ResourcesAndTools/business-solutions/Documents/2015-job-satisfaction-and-engagement-report.pdf.

National Security Agency, Cisco, Citibank, two national laboratories, and several large government contractors. We expect there are many more such innovative employers out there. If their most successful practices can be identified and replicated, we could help make the careers for other cybersecurity professionals more rewarding and stable.

Methodology

We developed a questionnaire to test our *hypothesis that there are identifiable factors that help organizations become employers of choice* (Appendix A). The questionnaire was based on a literature search (summarized in Appendix B) and discussions with cybersecurity experts. We tested the questionnaire with the staff of one of the large consulting firms to ensure the survey response options captured the most important motivational factors; the responses from that test are not included in our results.

We reached out to organizations[4] that issue professional certifications in cybersecurity and asked them to review our draft questionnaire and to send it to their constituencies. That effort yielded 284 usable responses.

Testing our hypothesis that there are important differences between factors that influence ninjas from other cybersecurity professionals proved to be an interesting challenge. Since there is no test or widely accepted list of credentials that label one as a ninja, we opted to identify ninjas by what they reported they do at work. We asked respondents to report how they spent their time using a list of tasks developed by the 2012 Department of Homeland Security Advisory Council Task Force on CyberSkills.[5] Using that task list, we labeled as ninjas those who reported spending most of their time on highly technical tasks. Since the question also allowed for free-form replies, we evaluated each such reply as to whether it was a ninja task.

We also looked at the data to determine whether there was a meaningful relationship between professional certifications and being a ninja, that is, were those who reported performing ninja tasks more likely to hold certain credentials than those that did not?

We recognize that there are potential weaknesses in this approach: (1) designating individuals as ninjas is entirely based on self-reporting; and (2) there are doubtless ninjas among those who responded who spend much of their time on non-ninja tasks. We did ask respondents to identify themselves—with a guarantee of confidentiality of individual responses—so we are confident of the candor of the replies. Tables with the detailed results of the survey can be found at Appendix C.

We recognize that our approach may not yield results generalizable to the population. That said, we are confident that the responses provide meaningful insights as we are able to

[4] CompTIA (Computer Technology Industry Association), Cisco, (ISC)[2], Mile2, GIAC (Global Information Assurance Certification).
[5] Homeland Security Advisory Council Task Force on CyberSkills, *CyberSkills Task Force Report: Fall 2012* (Washington, DC: U.S. Department of Homeland Security, 2012), https://www.dhs.gov/sites/default/files/publications/HSAC%20CyberSkills%20Report%20-%20Final.pdf.

identify trends and preferences, and our results can inform further research. We welcome recommendations for improvement.

What We Learned: Principal Findings

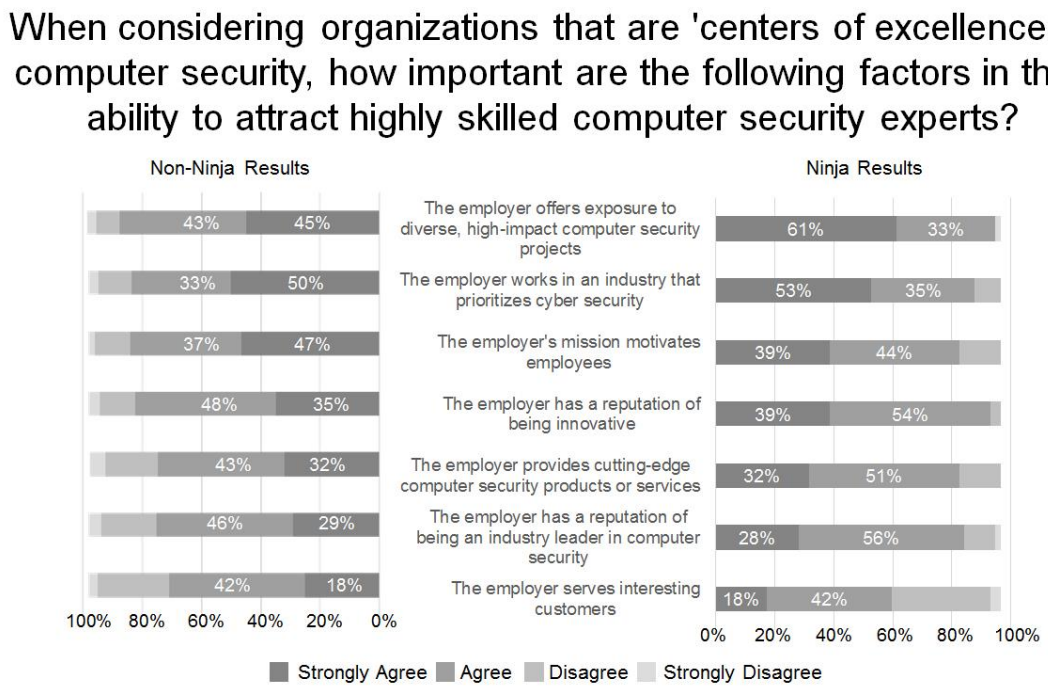
What makes organizations employers of choice? Our preliminary conclusions from the survey showed that three factors were rated as very important by more than 45 percent of respondents

- The employer works in an industry that prioritizes cybersecurity.
- The employer offers exposure to diverse, high-impact computer security projects.
- The employer's mission motivates employees.

Working on high-impact projects was rated as very important more frequently by ninjas than by non-ninjas.

Mission is an especially important motivator for cybersecurity experts in the public sector:

> *We have a critical mission; we are protecting our way of life from a cyber attack. Helping [to] keep other systems safe is important, but not as super-hero sounding.*[6]



[6] Interview with U.S. government cybersecurity adviser, March 16, 2016.

Why they stay where they are. Out of 15 reasons people gave for staying with an employer, 6 were rated as very important by more than 50 percent of respondents:

- Engaging and challenging tasks
- Employer pays for training to ensure skills stay current
- Ability to have a flexible schedule
- Competitive compensation and benefits
- Access to the resources necessary to do the job (people, funding, tools, etc.)
- Opportunities for career advancement

Engaging and challenging tasks and training were rated as very important more frequently than pay.

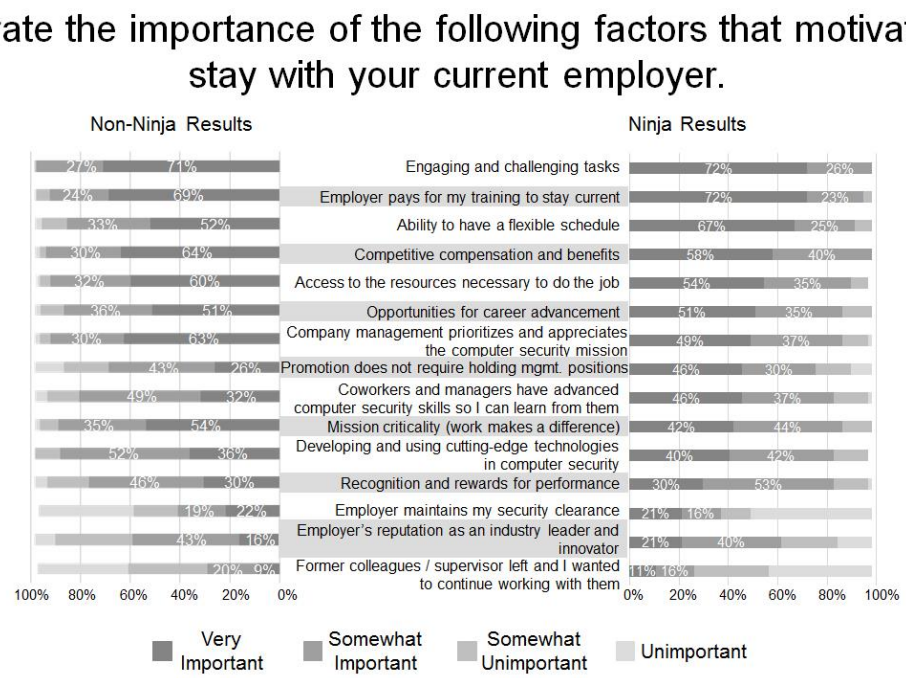
> *Cybersecurity includes so many different industries and sub-skills. Sometimes employers try to fill a specific gap and an individual is just tasked to do that. And then you don't have an opportunity to go out, do different things, and learn other parts of cyber.*[7]

> *At my level, taking into account conference fees, training seminars, and travel expenses, I'm looking at a $20,000 out-of-pocket cost per year to make sure my skills* stay current.[8]

For ninjas, more respondents rated a flexible work schedule than pay as very important.

"Promotion does not require moving into management" was rated as very important by 46 percent of ninjas but only 26 percent of non-ninjas.

[7] Interview with security engineer, June 17, 2016.
[8] Interview with security engineer, June 15, 2016.



Given the strong interest in engaging and challenging work, factors that stood out as very important by more than 50 percent of respondents were:

- Variety in tasks: not always solving the same problem
- Time to explore new technologies
- Engaging with other experts

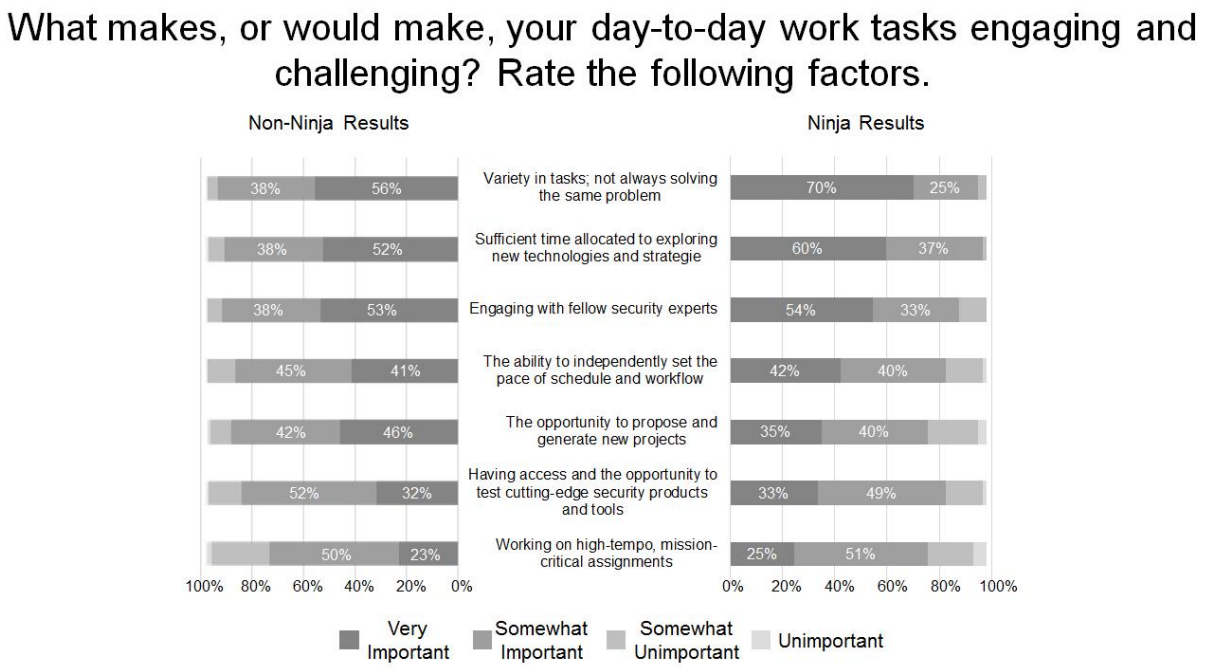
Variety in tasks and time to explore were even more important to ninjas than to non-ninjas.

> *When you're in the cybersecurity field, you want to solve problems, but not the exact same one over and over.*[9]

The ability to engage with other computer security experts was a crucial component for job satisfaction.

> *A lot of places or companies will just hire one person who they think can get all these tasks done, and that person is on an island because they have no one else to work with and no one else to learn from.*[10]

[9] Interview with computer security expert, March 21, 2016.
[10] Interview with researcher, June 15, 2016.



Why they left their previous jobs: Out of 15 reasons people gave for leaving a previous employer, 6 were rated as very important by at least 44 percent of respondents. The next highest was rated very important by only 33 percent of respondents.[11]

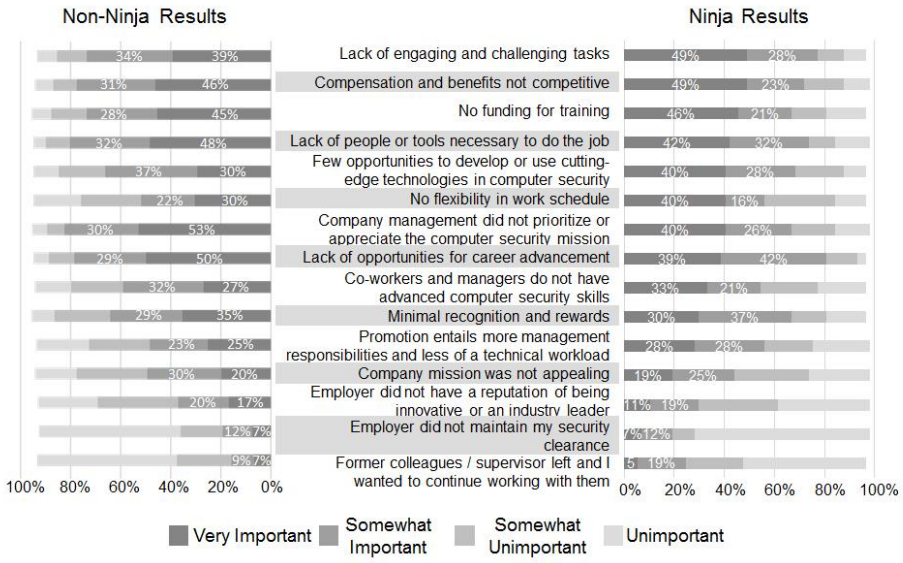
- Company management did not prioritize or appreciate the cybersecurity mission
- Lack of opportunities for career advancement
- Lack of people or tools necessary to do the job
- Compensation and benefits not competitive
- No funding for training
- Lack of engaging and challenging tasks

Responses were similar for both ninjas and non-ninjas, although lack of engaging and challenging tasks rank higher for ninjas.

> *Company management prioritizing or appreciating the computer security mission is critical, especially for penetration testers. Pen testers value leadership within their organizations having their back. Pen testing is inherently controversial, and these experts worry that some might view these activities as insubordinate and thus hurt the growth of pen testers within the company because they expose vulnerabilities and*

[11] Data for total survey respondents can be found in Appendix C.

flaws. So company management has to understand the computer security mission and facilitate the growth and reward the initiative of these employees.[12]



What credentials do ninjas hold?

As one might expect, ninjas are more likely to hold one or more professional certifications, especially the more technical ones.

Ninjas who perform highly technical tasks are far more likely to hold related professional certifications. The bolded text highlights instances where a credential was claimed by more than 20 percent of ninjas who perform that task and is substantially higher than non-ninja respondents.

[12] Interview with Ed Skoudis, founder, Counter Hack, March 21, 2016.

% of people doing these tasks with the following certifications	Pen Testing	Security Monitoring and Event Analysis	Digital Forensics	Secure Coding	Security Engineering	Non-ninjas
Ninjas who perform task daily or often	22	34	24	18	26	227*
CISSP - Certified Information Systems Security Professional	50%	32%	42%	33%	42%	59%
GCIH – GIAC Certified Incident Handler	14%	**32%**	**33%**	11%	**23%**	23%
GCIA - GIAC Certified Intrusion Analyst	9%	**26%**	**25%**	11%	**27%**	11%
GSEC - GIAC Security Essentials	**23%**	**21%**	**21%**	11%	**23%**	17%
GCFA - GIAC Certified Forensic Analyst	5%	18%	21%	0%	19%	8%
CEH - Certified Ethical Hacker	**23%**	12%	8%	17%	12%	12%
GPEN - GIAC Penetration Tester	23%	6%	0%	22%	8%	12%
GCFE - GIAC Certified Forensic Examiner	5%	15%	**21%**	6%	12%	4%
GMOB - GIAC Mobile Device Security Analyst	18%	0%	0%	17%	0%	2%

* This number includes individuals who perform ninjas tasks, but not daily or often.

Possible follow-on work

We hope that this brief survey will prompt discussion and further refinement of the factors that make an organization an employer of choice for high-end cybersecurity professionals. A good next step would be to look at those organizations with high concentrations of cyber-ninjas to identify best practices.

Wrapping it up

Earlier research has shown the importance of the human factor in determining the success or failure of an organization's cybersecurity efforts.[13] These earlier reports looked at how to create ninjas, but we realized that how you keep ninjas is just as important.

Attitudes toward work are changing—people no longer expect to spend their entire career at a single company. This is unavoidable, and creates costs for of companies not only in

[13] CSIS, *Hacking the Skill Shortage*, 4.

acquiring and training employees, but also in how well they secure their networks. The factors we have identified in this initial survey point to how companies and agencies can better manage the problem of retention.

Ultimately, cybersecurity is a national problem–no single entity can solve it on its own. But while we and other countries struggle toward building a safer cyber environment, acquiring and retaining ninjas are crucial for defense. This initial report points to how that can be done.

Appendix A. The Survey

N.B.: For questions seeking rankings or preferences (3 through 8) options were listed in random order so as not to bias responses.

Survey

The Center for Strategic and International Studies (CSIS) is conducting a research project on the computer security workforce; your response to this survey will inform our research and analysis. We estimate that the survey can be completed in 9 to 12 minutes. We ask that you complete the survey by July 1, 2016. To increase survey participation, we will use at least two reminders.

Computer Security Skills and Certifications: This section will ask about the computer security skills you employ for your job and the certifications you have earned.

1. How often do you perform the following tasks:

	NEVER	RARELY	OFTEN	DAILY
Secure coding and code review	☐	☐	☐	☐
Security engineering - building in security	☐	☐	☐	☐
Penetration testing	☐	☐	☐	☐
Incident response, hunt team activities, and reverse engineering	☐	☐	☐	☐
Strategic planning and policy development	☐	☐	☐	☐
Security engineering - operations	☐	☐	☐	☐
Security monitoring and event analysis	☐	☐	☐	☐
Computer network defense analysis and infrastructure support	☐	☐	☐	☐
Digital forensics	☐	☐	☐	☐
Threat analysis / Counter-intelligence analysis	☐	☐	☐	☐
Administrative and technical support	☐	☐	☐	☐
Risk assessment engineers	☐	☐	☐	☐
Security program management	☐	☐	☐	☐

2. What computer security certifications have you earned? List all below

Employer dynamics: This section will ask how employers recruit and maintain highly skilled computer security professionals, and what factors are motivate highly skilled computer security professionals to change employers.

3. When considering organizations that are 'centers of excellence' in computer security, how important are the following factors in their ability to attract highly-skilled computer security experts?

	STRONGLY AGREE	AGREE	DISAGREE	STRONGLY AGREE
The employer's mission motivates employees	☐	☐	☐	☐
The employer provides cutting-edge computer security products or services	☐	☐	☐	☐
The employer has a reputation of being an industry leader in computer security	☐	☐	☐	☐
The employer works in an industry that prioritizes cyber security	☐	☐	☐	☐
The employer has a reputation of being innovative	☐	☐	☐	☐
The employer offers exposure to diverse, high-impact computer security projects	☐	☐	☐	☐
The employer serves interesting customers	☐	☐	☐	☐

4. Please rate the importance of the following factors that motivate you to stay with your current employer.

	VERY IMPORTANT	SOMEWHAT IMPORTANT	SOMEWHAT UNIMPORTANT	UNIMPORTANT
Engaging and challenging tasks	☐	☐	☐	☐
Opportunities for career advancement	☐	☐	☐	☐
Developing and using cutting-edge technologies in computer security	☐	☐	☐	☐
Competitive compensation and benefits	☐	☐	☐	☐
Mission criticality (the work makes a difference)	☐	☐	☐	☐
Coworkers and managers have advanced computer security skills so I can learn from them	☐	☐	☐	☐
Recognition and rewards for performance	☐	☐	☐	☐
Employer pays for training to ensure my skills stay current	☐	☐	☐	☐
Ability to have a flexible schedule	☐	☐	☐	☐
Former colleague(s) recruited me for this position and I wanted to continue working with them	☐	☐	☐	☐
Promotion for technical professionals does not require holding management positions	☐	☐	☐	☐
Company management prioritizes and appreciates the computer security mission	☐	☐	☐	☐
Access to the resources necessary to do the job (people, funding, tools, etc.)	☐	☐	☐	☐
Employer's reputation as an industry leader and innovator	☐	☐	☐	☐
Employer maintains my security clearance	☐	☐	☐	☐

5. Given competitive compensation and benefits, opportunities for career advancement, and good management, what are additional factors that motivate you to stay with an employer? Rank the top five factors below.

- _____ Mission criticality: the work makes a difference
- _____ Employer maintains my security clearance
- _____ Access to resources necessary to excel in the job (sufficient people, funding, tools etc.)
- _____ Rewards and recognition for performance
- _____ Company management prioritizes and appreciates the computer security mission
- _____ Ability to have a flexible schedule
- _____ Coworkers and managers have advanced computer security skills so I can learn from them
- _____ Engaging and challenging tasks
- _____ Former supervisors/colleagues recruited me for this position and I wanted to continue working with them
- _____ Promotion for technical professionals does not require holding management positions
- _____ Developing and using cutting-edge technologies in computer security
- _____ Employer pays for training to ensure my skills stay current
- _____ Employer's reputation as an industry leader and innovator

6. What makes, or would make, your day-to-day work tasks engaging and challenging? Rate the following factors.

	VERY IMPORTANT	SOMEWHAT IMPORTANT	SOMEWHAT UNIMPORTANT	UNIMPORTANT
Having access and the opportunity to test cutting-edge security products and tools	☐	☐	☐	☐
Sufficient time allocated to exploring new technologies and strategies	☐	☐	☐	☐
Working on high-tempo, mission-critical assignments	☐	☐	☐	☐
Variety in tasks; not always solving the same problem	☐	☐	☐	☐
Engaging with fellow security experts	☐	☐	☐	☐
The opportunity to propose and generate new projects	☐	☐	☐	☐
The ability to independently set the pace of schedule and workflow	☐	☐	☐	☐

7. Please rate the importance of the following factors that motivated you leave your previous employer.

	VERY IMPORTANT	SOMEWHAT IMPORTANT	SOMEWHAT UNIMPORTANT	UNIMPORTANT
Minimal recognition and rewards for performance	☐	☐	☐	☐
Lack of opportunities for career advancement	☐	☐	☐	☐
No funding for training	☐	☐	☐	☐
Compensation and benefits not competitive	☐	☐	☐	☐
Lack of people or tools necessary to do the job	☐	☐	☐	☐
Employer did not have a reputation of being innovative or an industry leader	☐	☐	☐	☐
Former colleagues / supervisor left and I wanted to continue working with them	☐	☐	☐	☐
Few opportunities to develop or use cutting-edge technologies in computer security	☐	☐	☐	☐
Employer did not maintain my security clearance	☐	☐	☐	☐
No flexibility in work schedule	☐	☐	☐	☐
Lack of engaging and challenging tasks	☐	☐	☐	☐
Promotion entails more management responsibilities and less of a technical workload	☐	☐	☐	☐
Company mission was not appealing	☐	☐	☐	☐
Company management did not prioritize or appreciate the computer security mission	☐	☐	☐	☐
Coworkers and managers do not have advanced computer security skills	☐	☐	☐	☐

8. Given a lack of competitive compensation and benefits, few opportunities for career advancement, and poor management, what are additional factors that motivate you to leave an employer? Rank the top five factors below.

- _____ Few opportunities to develop or use cutting-edge technologies in computer security
- _____ Employer did not have a reputation of being innovative or an industry leader
- _____ Coworkers and managers do not have advanced computer security skills
- _____ Former colleagues / supervisor left and I wanted to continue working with them
- _____ Reputation of the company was poor
- _____ Company management did not prioritize or appreciate the computer security mission
- _____ No flexibility in work schedule
- _____ Promotion entails more management responsibilities and less of a technical workload
- _____ Employer does not maintain my security clearance
- _____ Location of employer
- _____ Minimal recognition and rewards for performance
- _____ Lack of engaging and challenging tasks
- _____ Lack of people or tools necessary to do the job
- _____ No funding for training
- _____ Company mission was not appealing

Demographic Information:

We are committed to protecting your privacy. Respondents are required to provide their name and affiliation to avoid inadvertently collecting duplicate responses. All the information you provide will be treated as confidential and will only be used by the CSIS team for research purposes. Your comments will not be identified as belonging to you, instead they will be combined with those gathered from other survey participants, anonymized, and analyzed as part of a group. We do not use any of the information you provide for direct marketing or other non-research activities.

9. Please provide the following information *This question is required*

First Name _____

Last Name _____

Title _____

Company Name _____

Appendix B. Summary of Literature Research

Articles assessed employees through a combination of performance reviews and surveys. There is some debate in the literature as to whether employees are motivated by money (Willyerd, 2014), or whether that motivation becomes irrelevant after basic needs are met (Maslow and Herzberg). Other motivating factors cited by studies include career development, empowerment, rewards, and company leadership. One study found "challenging and meaningful work" as the primary factor for employee satisfaction, which was defined as having influence over how work was done and autonomy. Other factors were opportunities to learn and grow and the sense of being part of a team (Kaye and Jordan-Evans, 2003).

Herzberg's Two-Factor Theory about employee behavior posits that satisfaction and dissatisfaction are not on a continuum but are independent factors. Why people stay at jobs is not the inverse of why they leave. Satisfaction is generally observed through "motivators": factors intrinsic to the job itself, including recognition and responsibilities. "Hygiene factors," including status, pay, and fringe benefits, do not give positive job satisfaction, but dissatisfaction results from their absence.

Implications

Our survey may well reflect trends in employee satisfaction across industries (in particular the Kay and Jordan-Evans study). We highlight how these "cybersecurity ninjas" are different in terms of motiving factors and designed the survey to identify specifics of what constitutes challenging and meaningful work in the cybersecurity field. Additionally, Herzberg's two-factor theory influenced our survey design.

Sources

Colomo-Palacios, Ricardo, et al. "The War for Talent: Identifying Competencies in IT Professionals through Semantics." *International journal of Sociotechnology and Knowledge Development* 2, no. 3 (2010): 26–36.

Hay Group. "The Hay Report: Compensation and Benefits Strategies for the Future." Philadelphia, PA: Hay Group, 1998. http://www.indiana.edu/~jobtalk/Articles/comp/hay_rprt.pdf.

Herzberg, F., B. Mausner, and B.B. Snyderman. *The Motivation to Work*. 2nd ed. New York: Wiley, 1966.

Kaye, Beverly, and Sharon Jordan-Evans. "How to Retain High-Performance Employees." In *The 2003 Annual: Volume 2, Consulting 2003*. New York: Wiley, 2003.

Lipman, Victor. "New Study Shows How High-Performing Companies Motivate Their People." *Forbes*, February 14, 2014. http://www.forbes.com/sites/victorlipman/2014/02/14/new-study-shows-how-high-performing-companies-motivate-their-people/#3c18aaf119f4.

Macky, Keith, and Peter Boxall. "The relationship between 'high-performance work practices' and employee attitudes: An investigation of additive and interaction effects." *International Journal of Human Resource Management* 18, no. 4 (2007): 537–67.

Maslow, A.H. "A theory of human motivation." *Psychological Review* 50 no. 4 (1943): 370–96.

Newton, Paula. "What Do High Performance Employees Value?" IntelligentHQ.com, March 17, 2015. http://www.intelligenthq.com/resources/what-do-high-performance-employees-value/.

Pollitt, David. "Leadership succession planning 'affects commercial success.'" *Human Resource Management International Digest* 13, no. 1 (2005): 36–38.

Ramsay, Harvie, Dora Scholarios, and Bill Harley. "Employees and High-Performance Work Systems: Testing inside the Black Box." *British Journal of Industrial Relations* 38, issue 4 (2000): 501–31.

Rynes, Sara L., Barry Gerhart, and Kathleen A. Minette. "The Importance of Pay in Employee Motivation: Discrepancies between What People Say and What They Do." *Human Resource Management* 43, issue 4 (2004): 381–94.

Stahl, Günter, et al. "Six principles of effective global talent management." *Sloan Management Review* 53, no. 2 (2012): 25–42.

Van De Voorde , Karina, and Susanne Beijer. "The role of employee HR attributions in the relationship between high-performance work systems and employee outcomes." *Human Resource Management Journal* 25, issue 1 (2015): 62–78.

Willyerd, Karie. "What High Performers Want at Work," *Harvard Business Review*, November 18, 2014. https://hbr.org/2014/11/what-high-performers-want-at-work.

Chart 1. When considering organizations that are "centers of excellence" in computer security, how important are the following factors in their ability to attract highly skilled computer security experts?

	Strongly Agree			Agree			Disagree			Strongly Disagree		
	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total
The employer offers exposure to diverse, high-impact computer security projects	61%	45%	49%	33%	43%	42%	0%	8%	6%	2%	3%	3%
The employer works in an industry that prioritizes cyber security	53%	50%	52%	35%	33%	35%	9%	11%	11%	0%	4%	3%
The employer has a reputation of being innovative	39%	35%	36%	54%	48%	50%	4%	12%	10%	0%	4%	3%
The employer's mission motivates employees	39%	47%	46%	44%	37%	40%	14%	12%	13%	0%	2%	2%
The employer provides cutting-edge computer security products or services	32%	32%	33%	51%	43%	45%	14%	18%	17%	0%	5%	4%
The employer has a reputation of being an industry leader in computer security	28%	29%	29%	56%	46%	49%	11%	19%	17%	2%	4%	4%
The employer serves interesting customers	18%	25%	24%	42%	46%	46%	33%	24%	27%	4%	3%	3%

Chart 2. Please rate the importance of the following factors that motivate you to stay with your current employer.

	Very Important			Somewhat Important			Somewhat Unimportant			Unimportant		
	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total
Engaging and challenging tasks	72%	71%	72%	26%	27%	27%	0%	1%	1%	0%	0%	0%
Employer pays for training to ensure my skills stay current	72%	69%	70%	23%	24%	24%	4%	5%	5%	0%	1%	1%
Ability to have a flexible schedule	67%	52%	56%	25%	33%	32%	7%	10%	10%	0%	3%	2%
Competitive compensation and benefits	58%	64%	64%	40%	30%	33%	0%	3%	2%	0%	2%	1%
Access to the resources necessary to do the job (people, funding, tools, etc.)	54%	60%	60%	35%	32%	34%	7%	4%	5%	0%	1%	1%
Opportunities for career advancement	51%	51%	52%	35%	36%	36%	12%	9%	10%	0%	2%	2%
Company management prioritizes and appreciates the computer security mission	49%	63%	61%	37%	30%	31%	11%	4%	6%	2%	2%	2%
Promotion for technical professionals does not require holding management positions	46%	26%	30%	30%	43%	41%	14%	18%	18%	9%	12%	11%
Coworkers and managers have advanced computer security skills so I can learn from them	46%	32%	35%	37%	49%	47%	14%	13%	13%	2%	5%	4%
Mission criticality (the work makes a difference)	42%	54%	52%	44%	35%	38%	12%	7%	9%	0%	2%	1%
Developing and using cutting-edge technologies in computer security	40%	36%	38%	42%	52%	51%	14%	10%	11%	0%	0%	0%
Recognition and rewards for performance	30%	30%	31%	53%	46%	48%	14%	17%	16%	2%	5%	5%
Employer maintains my security clearance	21%	22%	22%	16%	19%	19%	12%	18%	17%	49%	38%	42%
Employer's reputation as an industry leader and innovator	21%	16%	18%	40%	43%	43%	23%	31%	30%	14%	8%	10%
Former colleague(s) recruited me for this position and I wanted to continue working with them	11%	9%	9%	16%	20%	20%	30%	32%	32%	42%	37%	39%

Chart 3. What makes, or would make, your day-to-day work tasks engaging and challenging? Rate the following factors.

	Very Important			Somewhat Important			Somewhat Unimportant			Unimportant		
	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total
Variety in tasks; not always solving the same problem	70%	56%	60%	25%	38%	36%	4%	4%	4%	0%	0%	0%
Sufficient time allocated to exploring new technologies and strategies	60%	52%	55%	37%	38%	39%	2%	6%	5%	0%	1%	1%
Engaging with fellow security experts	54%	53%	55%	33%	38%	38%	11%	6%	7%	0%	0%	0%
The ability to independently set the pace of schedule and workflow	42%	41%	42%	40%	45%	45%	14%	11%	12%	2%	0%	1%
The opportunity to propose and generate new projects	35%	46%	45%	40%	42%	43%	19%	8%	10%	4%	1%	2%
Having access and the opportunity to test cutting-edge security products and tools	33%	32%	33%	49%	52%	53%	14%	13%	13%	2%	1%	1%
Working on high-tempo, mission-critical assignments	25%	23%	24%	51%	50%	51%	18%	22%	22%	5%	2%	3%

Chart 4. Please rate the importance of the following factors that motivate you to leave your former employer.

	Very Important			Somewhat Important			Somewhat Unimportant			Unimportant		
	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total	Ninjas	Non-Ninjas	Total
Lack of engaging and challenging tasks	49%	39%	44%	28%	34%	35%	11%	12%	12%	9%	8%	9%
Compensation and benefits not competitive	49%	46%	49%	23%	31%	33%	16%	9%	11%	11%	7%	9%
No funding for training	46%	45%	47%	21%	28%	28%	14%	14%	15%	16%	8%	10%
Lack of people or tools necessary to do the job	42%	48%	49%	32%	32%	33%	11%	10%	10%	14%	5%	7%
Few opportunities to develop or use cutting-edge technologies in computer security	40%	30%	33%	28%	37%	37%	19%	19%	20%	9%	10%	10%
No flexibility in work schedule	40%	30%	34%	16%	22%	21%	28%	24%	26%	12%	19%	19%
Company management did not prioritize or appreciate the computer security mission	40%	53%	53%	26%	30%	30%	18%	7%	10%	14%	6%	8%
Lack of opportunities for career advancement	39%	50%	50%	42%	29%	33%	12%	10%	11%	4%	6%	6%
Co-workers and managers do not have advanced computer security skills	33%	27%	30%	21%	32%	32%	23%	21%	22%	19%	15%	16%
Minimal recognition and rewards for performance	30%	35%	36%	37%	29%	32%	14%	22%	21%	16%	9%	11%
Promotion entails more management responsibilities and less of a technical workload	28%	25%	27%	28%	23%	26%	19%	24%	25%	23%	21%	23%
Company mission was not appealing	19%	20%	21%	25%	30%	30%	30%	28%	30%	25%	17%	19%
Employer did not have a reputation of being innovative or an industry leader	11%	17%	16%	19%	20%	21%	32%	32%	34%	37%	24%	28%
Employer did not maintain my security clearance	7%	7%	8%	12%	12%	13%	9%	17%	16%	70%	56%	63%
Former colleagues / supervisor left and I wanted to continue working with them	5%	7%	7%	19%	9%	12%	23%	22%	23%	49%	56%	58%

Chart 5. Certifications by task

	CISSP	CEH	GPEN	GCIH	Security+	GMOB	GSEC	GCIA	GCFA	CISM
Pen Testing	13%	9%	9%	6%	6%	4%	4%	2%	2%	3%
Security Monitoring and Event Analysis	60%	14%	12%	34%	17%	1%	20%	18%	11%	10%
Digital Forensics	18%	5%	0%	7%	3%	0%	3%	5%	9%	1%
Secure Coding	24%	3%	6%	6%	6%	9%	3%	3%	0%	0%
Security Engineering	16%	4%	4%	8%	5%	1%	5%	4%	3%	3%
Total Ninjas	13%	4%	4%	8%	4%	2%	6%	7%	1%	1%
Total Non-Ninjas	18%	4%	4%	7%	5%	1%	5%	3%	3%	3%

About the Authors

Franklin S. Reeder, a former official with the Office of Management and Budget, is cofounder and director of the Center for Internet Security and the National Board of Information Security Examiners. He served on the CSIS Commission on Cybersecurity and, with Karen Evans, coauthored the Commission's white paper on the cybersecurity workforce, *A Human Capital Crisis in Cybersecurity* (CSIS, November 2010).

Katrina Timlin is an associate fellow in the Strategic Technologies Program at the Center for Strategic and International Studies (CSIS). At CSIS, she focuses on cybersecurity, technology, and innovation. Previously, she was a senior analyst at Avascent, where she researched cybersecurity and technology in government-driven markets. Other professional experiences include the Department of State, Department of Commerce, and the Executive Office of the President. Ms. Timlin holds an M.A. in international affairs with a concentration in strategic studies from the Johns Hopkins School of Advanced International Studies (SAIS) and a B.A. in international affairs from the George Washington University.

COVER PHOTO AFRICA STUDIO/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.**csis**.org