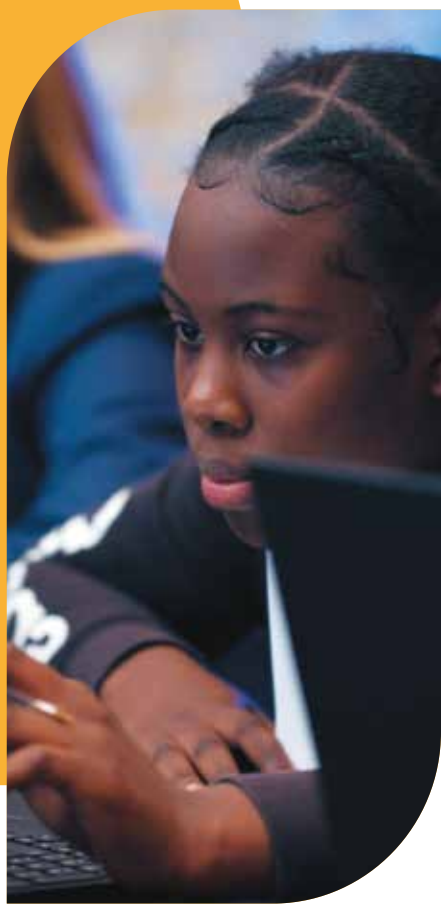
What Works in Finding Elite Cybersecurity Talent:

Promising Practices for Chief Information Officers

A Report of the CIO Institute

CIO INSTITUTE

CIO.org



Authors: Franklin Reeder, Alan Paller

ISBN 978-0-578-83950-9 US$25.00 52500>
9 780578 839509

Contents

Introduction

Finding and keeping elite cybersecurity professionals who have the deep technical expertise to protect their enterprises from new and increasing levels of ransomware and espionage threats continue to be among the most pressing challenges facing CIOs.[1,2] These cybersecurity experts are the rare professionals with the skills to:

(i) reduce attacker dwell time[3] to avoid damage
(ii) perform world-class security assessments
(iii) engineer defensible security even in the cloud
(iv) conduct advanced forensics under pressure during attacks
(v) identify and correct flaws in software-enhanced products and enterprise applications
(vi) engineer cyber hygiene automation that ensures systems and applications remain at a high level of readiness.

These same elite professionals are needed in power plants, banks, telecoms, healthcare organizations, and government agencies – federal, state, and local. In the age of ransomware , these experts are needed in any Internet-connected enterprise where organizational continuity matters.

The extremely high demand for elite cybersecurity professionals, and the challenge higher education institutions face in educating sufficient numbers of them, is a well documented problem.[4-7] This report shares lessons learned by enterprises that have implemented three promising approaches to building sustainable pipelines to provide this elite talent:

(1) Identify existing employees with high aptitude for elite performance, including non-IT employees, and develop them into productive cybersecurity professionals
(2) Recruit from colleges that are graduating cyber talent with strong hands-on cyber skills
(3) Build the pipeline of the future in their regions through local talent discovery and partnerships with colleges

Promising Approach 1:
Identify elite cyber aptitude among non-IT employees and develop their talent

Finding elite cybersecurity professionals in the open marketplace has been a fool's quest for a long time. As far back as 2012, the Washington Post reported: "Along the Baltimore-Washington Parkway, the concentration of government agencies and contractors brimming with computer geeks rivals any cyber defense area on the planet. And in this age of growing cyber threats, those firms are engaged in a cyber-hiring competition so fierce that one expert called it 'fratricide on the parkway.'" The article quotes a cybersecurity hiring manager: "We are all hiring away from each other. I'm doing it myself. They're all going to the highest bidder."[8] In other words, no matter how much you are willing to pay, someone will probably pay more.

CIOs are increasingly seeking alternative sources, and hidden talent within their own organizations appears to be a promising source of cyber talent and aptitude. As early as 2012, Goldman Sachs and Citibank CISOs were exchanging information on how they were able to recruit and train their best threat monitoring personnel by drawing on existing employees in other parts of their banks. What was unclear at that early stage was how the banks could best identify the most promising candidates among their employees and how they could develop that talent. In the intervening years they and others discovered three promising approaches to help make internal cyber talent identification and development feasible:

(i) **The 1% to 3% Discovery.** The first discovery was that the Goldman Sachs/Citi experience was not a fluke. In any population of educated people there appears to be a small subset that has the brain wiring to excel in solving challenging cybersecurity problems. The largest data sets come from the United Kingdom. In Her Majesty's Government (HMG) Cyber Discovery Programme, 200,000 students are participating in an ongoing talent discovery round. Those who excelled were allowed to progressively increase their hands-on mastery of the foundational topics in cybersecurity, and the best were engaged in high-intensity competitions and cyber camps. Out of the initial 200,000, approximately 6,000 showed elite talent and 900 showed what the U.K. named "super elite" skills. Those numbers translate to a range of .5% to 3% elite talent in a large population of people. Similarly, in HMG Cyber Retraining Academy, discussed below, 23,000 students applied; 600 were deemed to be "qualified" candidates for advanced training – or 2.6%.

If we use 1% as the expected yield of a search for talent, an enterprise with 20,000 employees could anticipate that some 200 current employees could be candidates to develop into ultra-high-performing cybersecurity practitioners, and hundreds more will become quite effective parctitioners in cybersecurity and other computer-related roles. Some may already work in cybersecurity, some in IT, and others in other departments. Many may not be interested in moving into cybersecurity, so the 200 number is an over-estimate of how many new elite cybersecurity practitioners could be found and developed. However, elite talent has an amplifying effect on cybersecurity teams, so even 40-50 such people could make an important difference in the effectiveness of the cybersecurity posture of a large organization. The data imply that it is reasonable to expect that in an enterprise of even a few hundred employees, one might expect to find a handful of individuals who have the potential to become elite performers. But the question remained: How do we find them?

(ii) **Reliable Testing for Cyber Aptitude.** The second discovery was a means of identifying people with innate talent. Cyber aptitude tests have progressed to the point that they can now identify aptitude even in people who are not tech hobbyists. Most early so-called cyber aptitude tests asked technical questions that measured familiarity with computers and programming and security. Those tests found people who had learned technology on their own, but they missed people who could learn technology but had not yet had the opportunity or shown a desire to do so. The new type of aptitude assessments identify hidden talent by measuring core traits such as critical thinking, information parsing, problem solving, logic extrapolation, and more. Essentially they find people with a "knack for cyber." The first public evidence of the success of such testing was discovered by HMG Cyber Retraining Academy in the United Kingdom. The Academy took 55 people (of 600 who were deemed qualified) who had never worked in IT or cyber, including a journalist, bartender, professional gamer, psychiatrist, and two police officers. What set those 55 apart from a thousand others who applied was that they excelled on a cyber aptitude test. Of the 55 people, 51 successfully

passed multiple advanced cybersecurity courses, earned respected technical cybersecurity certifications, and are now working in cybersecurity.[9] "The idea behind the academy," explains Program Director Stephen Jones, "is to show organizations that they don't have to wait years for new candidates; there is talent outside of [current cybersecurity professionals.] We need to change our view of who can be a good cybersecurity professional. The overall problem isn't training the people, it's finding the right people to train." The UK's success prompted the U.S. Office of Management and Budget to administer the same cyber aptitude test to 1,500 federal employees not working in IT in order to isolate successful candidates. In all, 30 people who took the test (2%) were subsequently retrained successfully for jobs in cyber. In order to broaden diversity in the field, another important goal, other academies have since used the cyber aptitude test to identify more than 400 veterans, women, and minorities as potential cyber elite performers. Almost all of them subsequently completed Cyber Immersion Academies and transitioned to cybersecurity jobs within six months of graduation.[10] Today, the largest U.S. military and law enforcement organizations use a version of that same cyber aptitude test to select which new hires to train for cyber jobs.

(iii) **Bridge Courses for Cyber Foundations.** Early on, most non-technical people who excelled on the cyber aptitude tests ran into a wall when trying to master hands-on technical cybersecurity skills. That wall is the lack of foundational understanding of the information technology on which cybersecurity proficiency is built, including computer architecture, networking in depth, operating system structure and administration (Windows and Linux) and programming (Python), as well as how the most common exploits work. Failing to start with fundamentals would be like trying to train high level medical specialists without first teaching them gross anatomy. The UK's Cyber Retraining Academy – which was able to convert 51 of 55 non-technical candidates into professionals who are now fully employed on important cyber projects – addressed this issue by starting its training with a bridge course. The course provided the candidates the opportunity to gain hands-on mastery of the foundations of cybersecurity. After the U.S. Cyber Reskilling Academy offered a similar online course to its candidates ("Foundations of Computers, Technology and Cybersecurity"), Academy graduates were nearly unanimous in reporting that the bridge course was essential to their being able to complete challenging immersion training in advanced cybersecurity skills. The U.S. Air Force's bridge course covering these same foundations reduced failure rates among airmen and women in more advanced cybersecurity training.

The bottom line is that people with substantial cyber aptitude may already be working in your organization. A cyber aptitude test can find them and a bridge course can get them ready to pursue advanced skills in cybersecurity.

Promising Approach 2:

Recruit from colleges that are producing highly skilled cybersecurity practitioners for the National Security Agency, other intelligence agencies, and critical infrastructure employers

Technical cybersecurity is a contact sport. There are tough, skilled teams on the other end of most intrusions. Skills matter because the better attackers build attack tools that evade nearly all installed security software.

For this discussion, we define technical cybersecurity as any of these nine Red Zone jobs identified and validated by the U.S. Homeland Security Advisory Council's Task Force on CyberSkills:[4]

- Incident responder
- System and network penetration tester
- Application penetration tester
- Security monitoring and event analysis
- Threat analyst / Counter-intelligence analyst
- Advanced forensics analysts for law enforcement
- Secure coders and code reviewers
- Security engineers - operations
- Security engineers / architects for building security into new systems and applications

All of these jobs are being transformed and expanded as more organizations move their computing to the cloud.

Technical cybersecurity also encompasses the role of offensive cyber operations in military and intelligence agencies, roles that were not included in the Department of Homeland Security CyberSkills Task Force mandate. Intelligence agencies have spent more than a decade raising the bar at colleges to create a pipeline of elite talent for their workforce by asking colleges to teach courses that ensure students develop hands-on skills in key areas like reverse engineering and network traffic analysis, and by then publicly recognizing the colleges that succeeded. The top talent in this emerging pipeline is quickly reserved by the intelligence agencies through internships. However, several of the undergraduate programs that produce technical talent for intelligence agencies are now growing sufficiently to produce a larger pool of graduates with elite skills who can raise the technical levels of cybersecurity teams for employers across the country.

The National Security Agency (NSA) has spent decades cultivating universities and community colleges across the country capable of educating students in cybersecurity programs tailored to its needs. By 2020, the NSA had recognized 312 colleges as Centers of Academic Excellence (CAEs). Of those, the NSA had recognized 21 schools as Centers of Academic Excellence in Cyber Operations (CAE/CO). Those schools had to provide evidence that their graduates mastered a much more rigorous program that includes elements such as network protocol analysis, programming, and reverse engineering, each with proof of hands-on mastery. The CAE/CO programs that are approved at the bachelors' degree level are included in Table 1 on the next page.

The sixteen regionally accredited undergraduate schools listed in Table 1 below (known as "The 2020 Sweet Sixteen") are leading the development of this important new pipeline of graduates with hands-on elite cyber skills. Some of the programs are designated as NSA Centers of Academic Excellence (CAE) in Cyber Operations; others provide advanced cyber skills development for the country's intelligence and law enforcement agencies.

The rigor of the CAE/CO requirements is central to effective cyber defense in any organization where ransomware is a threat. This is because organizations can reduce attacker dwell time only if they have employees with a high level of hands-on mastery of those skills. In the age of ransomware, no security metric is more important than dwell time.[11] Network traffic analysis, reverse engineering, and scripting, all required in the CAE/CO program, are core competencies of people who can reduce dwell time.

Colleges in the Centers of Academic Excellence program present their CAE designation as if it applies to their entire college rather than to the specific program that meets the standards required by the NSA program. As a result, employers interviewing graduates from those schools mistakenly assume that a computer science or cybersecurity degree from that school signifies the graduate has the skills that the CAE program is designed to build. Many do not have those skills because they do not take the hard courses specified in the schools' CAE applications. To be confident they are hiring people who have mastered the hands-on skills promised by colleges with the CAE/CO designation, enterprises have top technical people ask the candidates to explain the vector used in a recent attack and to solve two or three problems in reverse engineering. When those questions are answered successfully, they give the candidates additional problems in network traffic protocol analysis and a programming problem in Python. A shortcut is to look for validation of those key skills through the relevant professional cybersecurity certifications that validate those skills: GCIH (Hacker Exploits and Incident Response), GREM (Reverse Engineering), GCIA (Network Protocol Intrusion Analysis), and GPYC (Python Coding for Cybersecurity).

TABLE 1 - The 2020 Sweet Sixteen	
Cedarville University†	**B.S. in Computer Science with a Specialization in Cyber Operations**
Dakota State University†	**B.S. in Cyber Operations**
Northeastern University†	**B.S. in Computer Science, Concentration in Cyber Operations** **B.S. in Cyber Security, Concentration in Cyber Operations**
Old Dominion University†	**B.S. in Interdisciplinary Studies, Cyber Operations Major**
SANS Technology Institute‡	**B.S. in Applied Cyber Security**
Texas A&M University†	**B.S. in Computer Science, Minor in Cybersecurity** **B.S. in Computer Engineering, Minor in Cybersecurity**
Towson University†	**B.S. in Computer Science with a Track in Computer Security**
U.S. Air Force Academy†	**B.S. in Cyber Science**
U.S. Military Academy△	**B.S. in Cyber Science**
U.S. Naval Academy△	**B.S. in Cyber Operations**
University of Arizona†	**B.S. in Cyber Operations**
University of Maryland Baltimore County‡	**B.S. Computer Science – Cybersecurity Track**
University of Nebraska Omaha†	**B.S. in Cybersecurity, Special Track in Cyber Operations**
University of New Haven†	**B.S. in Computer Science, Cyber Operations** **B.S. in Cybersecurity and Networks, Cyber Operations**
University of Texas at El Paso†	**B.S. in Computer Science Cybersecurity Track**
University of Texas at San Antonio†	**B.S. in Computer Science, Cyber Operations Track**

† NSA CAE/Cyber Operations schools offering BS degrees.
‡ Professional cybersecurity continuing education providers for U.S. intelligence agencies as well as high tech immersion BS degrees for all students.
△ Military BS degrees with strong cybersecurity elements creating technical cyber leaders.

Promising Approach 3:
Participate in building a reliable pipeline of future talent in your region through local talent discovery and scholarship programs

The first two approaches listed above offer an immediate boost for current cyber talent searches, but both have long-term capacity limitations. As more employers discover the colleges producing qualified graduates, those graduates will become harder to recruit at reasonable salaries. To solve the workforce problem over the longer term, CIOs are working with their community outreach programs to invest in pipelines of future talent – particularly talent from their own cities and states where they can expect to have an advantage in recruiting and later reataining the top talent.

Their first and most critical step is to identify the people who are likely to excel in technical roles in cybersecurity and encourage them to explore further education in cybersecurity. As noted earlier, finding the right people to train is a prerequisite for developing elite cybersecurity practitioners. A surprisingly effective and increasingly popular talent discovery program is the National Cyber Scholarship Foundation's CyberStart America, which is being promoted by governors[12], high school counselors and teachers. The program identifies high school students who are tenacious and curious, and who have great problem-solving skills and relish taking on difficult challenges. Under the program, during November through February of each year all high school students in the United States are eligible to try their hand at a simulation – in essence a game – to solve a set of realistic cybersecurity challenges. An important attribute of the game is that it includes a Novice feature so that students who may not have had previous technical or cyber experience, can learn the basics and test whether they have the aptitude and will to go on. Students who solve a few challenges often get hooked and want to keep going, solving more and learning more. Those who reach a level that shows promise in the discovery round are invited to a challenge round where they compete for recognition and $2 million in college scholarships sponsored by the National Cyber Scholarship Foundation[13]. High school students who excel in competitions like picoCTF [https://picoctf.org/about] and members of teams that excel in CyberPatriot [https://www.uscyberpatriot.org/] also qualify for the scholarship challenge round.

CyberStart America, which began as a program to bolster recruiting of young women into the cybersecurity field, is now open to boys as well as girls. While it was a girls-only program, hundreds of teachers and students wrote notes to their governors describing why the program was so valuable. Here's an example.

> "The final weekend of the CyberStart America challenge was the beginning of our school vacation week. Three of the four girls spent most of Saturday and Sunday in my classroom with me! There aren't too many things that would get high school students to sacrifice two days of vacation to work on education! I was very proud and pleased by their work ethic and by the amount that they learned."
>
> – Will Wright, teacher,
> Mount Mansfield High School, Vermont[14]

Most high school students who try CyberStart America have never seen the technologies they encounter in the challenges. That doesn't stop interested and motivated students from learning Python programming, Linux command line, cryptography, forensics, and website security skills as they progress from level to level. The result is that the game motivates these students to want to pursue more education in computer science and cybersecurity.

"I cannot express enough gratitude for bringing this program to my state of Wyoming. I teach at the alternative school for our district and before I recruited girls to be a part of this wonderful program, I struggled to get girls to realize they could be computer scientists. I had girls actually saying they were too stupid to do this until I said, 'Just try it.' Some of my girls found out they were good at puzzles, some found out they liked programming. In all, I now have girls who are asking our counselor about computer science degrees at our local community college. My girls are now talking to others about how to do these assignments. They are becoming leaders all because of a short experience. Please continue this program. My girls want another shot at first place!"

– Sharon Seaton, teacher,
Black Butte High School, Wyoming[14]

By sending their employees to local high schools to encourage students to give CyberStart America a try, CIOs are making a huge difference in bolstering the growth of the local pipeline of the next generation oftalent. The employees making these presentations use the poster, available free through CyberStart America, that highlights cybersecurity jobs as "the coolest jobs in technology," then recount their own stories about how rewarding working in computer technology and cybersecurity can be. Participating employers also make videos of their younger cybersecurity employees answering questions about what the work is like and how they came to work in cybersecurity. These videos are posted at the Cyber Careers section of www.cyberstartamerica.org to help students learn that careers in cybersecurity are multifaceted and fascinating and can involve a lot of human interaction.

The second step in building a reliable pipeline of elite cyber talent is to give the students who excel in CyberStart America a good reason to pursue further study in the field and come back to work for the organization doing the outreach. Companies do that by underwriting additional National Cyber Scholarships earmarked for students in their city or state or even for the children

of their own employees, as is the practice of employers underwriting National Merit Scholarships. The recognition associated with winning these scholarships can change young people's lives and encourage them to explore and pursue a career in the cybersecurity field.

> "I won the CyberStart scholarship my junior year of high school, went on to learn more about cybersecurity myself, and got more people in my school involved. Senior year I was the first cybersecurity officer for my school's computer science club. I'm now a freshman in college at Texas A&M, and am learning networking from a Cybersecurity Club officer with the intent to carry on his mentorship to future students. Everything I've mentioned above was sparked by CyberStart. It introduced me to cybersecurity and showed me how fun and engaging it can be, which inspired me to learn more. Before CyberStart, I had no idea what kind of work I wanted to do once I complete my degree. It's really not an exaggeration for me to say that CyberStart changed my life."
>
> – Maya Arfat, Texas A&M University

So what are CIOs doing now?

There are a number of steps CIOs are taking to address the cybersecurity skills gap. Some directly affect their organizations; others have broader community-wide impact. Some require major organizational commitments; others only small investments.

- Mining their existing staff, in both technical and non-technical rples, for elite cybersecurity aptitude by administering cybersecurity aptitude tests, enrolling those who show high potential in bridge courses, and then rigorously training them in advanced cybersecurity skills.
- Recruiting from the Sweet Sixteen collegiate programs, though with the caveat of carefully screening them.
- Encouraging colleges and universities, including community colleges, in their communities to emulate the rigorous curricula of elite NSA CAE/CO programs.
- Encouraging high performers on their teams to teach at nearby colleges and universities. All of our analyses show that the most effective teachers are those who are currently active in the field so they improve the local pipeline. The teachers also earn the secondary benefit of having a first look at promising prospective employees.
- Setting up internship and/or apprenticeship programs in collaboration with local postsecondary schools. A critical success factor for cybersecurity programs is hands-on experience.
- Having their staff get to know the counselors and cyber teachers in local schools; volunteer for career nights and publicize opportunities like CyberStart America.
- Contribute to scholarship programs for Cyber Scholars at the National Cyber Scholarship Foundation in order to provide added incentives and resources for talented students to pursue careers in cybersecurity.

References

1. Heltzel P. The 11 Biggist Issues IT Faces Today. CIO Magaxzine. 2/15/19. https://www.cio.com/article/3245772/the-12-biggest-issues-it-faces-today.html

2. Heltzel P. Top 9 Challenges IT Leaders Will Face in 2020. CIO Magazine. 1/6/2020 https://www.cio.com/article/3509974/top-9-challenges-it-leaders-will-face-in-2020.html.

3. Dwell time is the length of time a cyber attacker has free reign in an environment from the time they get in until they are detected and eradicated. Source: https://www.optiv.com/cybersecurity-dictionary/dwell-time.

4. U.S. Department of Homeland Security Advisory Council on CyberSkills. CyberSkills Task Force Report. September 2012. https://www.dhs.gov/publication/homeland-security-advisory-council-cyberskills-task-force-report.

5. Reeder F, Evans K. A Human Capital Crisis in Cybersecurity. Center for Strategic and International Studies. 11/15/2010. https://www.csis.org/analysis/human-capital-crisis-cybersecurity.

6. Reeder FS, Timlin K. Recruiting and Retaining Cyber Ninjas. Center for Strategic and International Studies. October, 2016. https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas.

7. Crumpler W, Lewis JA. The Cybersecurity Workforce Gap. Center for Strategic and International Studies. January 2019. https://www.csis.org/analysis/cybersecurity-workforce-gap.

8. Nakashima E. Federal agencies, private firms fiercely compete in hiring cyber experts. Washington Post. 11/13/2012. https://www.washingtonpost.com/world/national-security/federal-agencies-private-firms-fiercely-compete-in-hiring-cyber-experts/2012/11/12/a1fb1806-2504-11e2-ba29-238a6ac36a08_story.html.

9. Dallaway E. All You Need to Know about the Cyber Retraining Academy. Info-Security Magazine. March 17, 2017. https://www.infosecurity-magazine.com/news-features/all-you-need-cyber-retraining/.

10. Hensch M. Inside the Federal Reskilling Academy. GovLoop Magazine, June 21, 2019. https://www.govloop.com/inside-the-federal-cyber-reskilling-academy/.

11. Villadiego R. Attacker Dwell Time: Ransomware's Most Important Metric. Dark Reading. September 30, 2020. https://www.threatshub.org/blog/attacker-dwell-time-ransomwares-most-important-metric/.

12. Governor Abbott Announces Partnership With CyberStart America To Promote Cybersecurity Career Track For Texas High School Students. Nov. 5, 2020. https://gov.texas.gov/news/post/governor-abbott-announces-partnership-with-cyberstart-america-to-promote-cybersecurity-career-track-for-texas-high-school-students.

13. National Cyber Scholarship Foundation. https://www.nationalcyberscholarship.org/.

14. Girls Go CyberStart teacher feedback. During 2017-18, 2018-19 and 2019-20, a pilot version of CyberStart America targeted young women.

Appendix 1:

Red Zone (Critical) Cybersecurity Jobs defined by the United States Department of Homeland Security Task Force on CyberSkills.[4]

Job	Critical Tasks	Consequences of Failure to Perform
Incident responder in- depth	Implement proactive measures to contain the incident, including isolation, characterization, reverse engineering, assessment of capability and activity of malicious software that has been found on agency systems, identification of intruder local changes/suspect interactions, triggering of targets to evoke malicious behaviors, and development and deployment of eradication tools. Only 2%–10% of all malicious software needs to be put through this deep analysis; the remainder will be cleaned with anti-virus tools using current and updated signatures. However, the 2%–10% constitute the most dangerous payloads.	Malicious software will be able to spread through agency systems by burrowing deep and maintaining control as well as by leaving back doors for unauthorized access at will. An unacceptable duration of attacker free time will result in freedom of movement and action. Lack of understanding of attackers and their tools (advanced malware) will undercut the defensive efforts of incident responders and threat analysts. Attackers can reuse tactics and tools to re-attack or maintain their control over systems for long periods, taking and changing data at will. Anomalous and malicious behavior by insiders will go undetected.
System and network penetration tester	Follow a systematic process to assess the ability of systems and networks to withstand sophisticated adversaries who have knowledge of the architecture and systems that are deployed. This is not social engineering or running a vulnerability testing tool or a packaged exploit tool, but rather sophisticated technical testing of the configuration and pathways and interactions between systems that mimics the techniques employed by advanced adversaries.	System configuration and composition weaknesses may be exploited by advanced adversaries and insiders to exfiltrate data and take over command-and-control of internal systems and processes. Failure to have extensive programs in this area also eliminates the valuable role such programs play in skill development. Knowing how to penetrate an architecture enables better security monitoring, event analysis, security engineering, and security architecture.
Application penetration tester	Test applications before they are deployed and when they are modified. Identify the avenues that are most riddled with flaws and holes and that give malicious actors access to the most important content or systems. This is not only a tool-deployment task; it also requires deep understanding of the application being tested.	Applications will be deployed, particularly on the web, that can be exploited and made to infect visitors' computers, deeply embarrassing the agency, or that can be used as access pathways for data exfiltration. Failure to have extensive programs in this area also eliminates the valuable role such programs play in skill development. Knowing how to find and exploit an application vulnerability allows for better code reviews, forensics analysis, threat analysis, and incident response.
Security monitoring and event analysis	Identify indicators that show an incident has occurred and initiate a swift response, differentiating between those incidents that represent impotent attack vectors and those that need to be analyzed in-depth by the incident responders. Many other tasks are performed by the security monitoring and event analysis staff, but the ones described here are the critical tasks for which skills are in very short supply.	Failure to identify new attacks that mimic old, impotent attack vectors provides savvy intruders with an easy vector to bypass defenses.
Threat analyst/ Counter-intelligence analyst	Deploy deep and current knowledge of the attack surface, its most vulnerable and high-value targets, and how its technical vulnerabilities may be exploited; maintain up-to-the-minute situational awareness on what malicious actors are using and targeting; and develop techniques and program custom tools to detect local changes, identify suspect interactions, and watch for and respond to what the malicious actors are doing. More advanced teams also are able to understand the attackers' motivation, language, organization, and social behaviors, as well as group the threat actors logically to create effective "cyber" profiles of groups, actors, and campaigns, thereby helping organizations become more proactive in their security posture and defense.	Malicious software installed by targeted attacks and other vectors will be able to evade defenses without being spotted—leading to long-term infection, freedom of action (including the exfiltration of sensitive information), and undermining of the defender's ability to act. Well-embedded adversaries can actually resist defender efforts, as those adversaries are privy to instructions and can work to stay a step ahead of observed defender actions. Further, not understanding the current threat landscape and exactly how the attacks work in technical detail will lead to insufficient defenses against those vectors and will unnecessarily raise costs.

Job	Critical Tasks	Consequences of Failure to Perform
Advanced forensics analysts for law enforcement	In investigating crimes or potential crimes, the advanced forensics analyst must perform many of the tasks of the incident responder in-depth, with special emphasis on reverse engineering but with the added requirement of establishing evidence that will stand up in court. Responsibilities include determining programs that have been executed, finding the files that have been changed by an intruder on disk and in memory, using time stamps to develop authoritative timelines of actions taken by the intruder, finding evidence of deleted files, and identifying key information in browser histories, account usage, and USB usage. The central goal is to find unknown malware hidden in systems, also known as the persistent presence.	Too few forensics analysts have the deep technical skills to go beyond the most basic capabilities of common commercial forensics tools. The FBI reports that nearly every case now involves computers; lack of deep forensics skills can render law enforcement agents impotent. The Department of Homeland Security (DHS), in partnership with law enforcement, can add value to industry by providing tools and expertise, thereby reducing industry costs during incident response and investigation.
Secure coders and code reviewers	Write code free of known coding flaws and weak design approaches, and check software to find flaws and fix them. The most proficient secure coders/code reviewers are those with the cognitive capacity to discover security vulnerabilities in programs while under time, quality, or cost pressures (i.e., the real world).	Intruders and malware exploit flaws to modify, add, or delete code on websites that infect visitors' computers, deeply embarrassing the agency; or to leverage their modifications as access pathways for data exfiltration.
Security engineers-operations	Implement and configure host and network firewalls, logging, and IPS/IDS at the highest appropriate level of security, and implement automated monitoring of configuration, patching, AV status, administrative rights, application white listing, and other security measures in order to provide system and network administrators a daily routine of actions to maintain the highest possible level of security and ensure that those actions are being performed.	The most common forms of targeted intrusions easily penetrate the defenses. Cybersecurity engineers are the main defense in power companies and other critical infrastructure enterprises. Without a team of cybersecurity engineers that can match the capabilities in industry, DHS will have trouble partnering with industry in critical infrastructure.
Security engineers/ architects for building security into new systems and applications	Maintain up-to-the-minute currency on attack techniques being used by adversaries against any of the components being engineered into new or updated systems. Avoid myths about design controls that are considered to be effective but in fact are not. Use knowledge about current attacks to identify flaws and weaknesses in the composition and design of networks, remote access schemes, and systems and applications. Specify solutions and verify the solutions that have been implemented. Rapidly adjust designs based on new threat and attack information.	When security is not baked into systems at the outset, it is very hard to glue it on later.

About the Authors

Franklin Reeder

Frank Reeder served two stints at the U.S. Office of Management and Budget totaling more than 20 years where he was chief of Information Policy (the first "federal CIO"), Deputy Associate Director for Veterans Affairs and Personnel, and Assistant Director for General Management. He subsequently served as Director of the Office of Administration of the Executive Office of the President under President Bill Clinton. Frank helped conceive and build several programs recognizing singular contributions to technology in Government, including the Federal 100 Awards.

Frank represented the Administration in negotiating and securing enactment of the Computer Privacy Act and the Computer Security Act of 1987 and wrote the guidelines on implementing the Privacy Act. He also chaired the Public Management Committee of the OECD. After retiring from government service, Frank co-founded and became the chairman of the Center for Internet Security, a not-for-profit established "to help organizations around the world effectively manage the organizational risks related to information security," and chaired the Information Security and Privacy Advisory Board of the National Institute of Standards and Technology, a federal advisory committee. Earlier in his career he was deputy director of House Information Systems, the technology support organization of the U.S. House of Representatives.

Alan Paller

Alan Paller founded STI, a regionally accredited college and graduate school, and SANS, a global provider of cybersecurity training whose 185,000 alumni are technical cybersecurity professionals protecting 17,000 government agencies, non-profit organizations, and business enterprises. Alan created the CyberStart America program with 26 state governors, which enabled tens of thousands of young women and men to discover their talent and ability to excel in cybersecurity. CyberStart inspired students to pursue a cyber career, while also allowing them to compete for $2 million in college scholarships to help them attain their potential and ultimately start a career in cybersecurity. Alan oversees a global program celebrating people responsible for remarkable improvements in cybersecurity and chairs the annual RSA keynote, "The Five Most Dangerous New Attack Vectors." He has testified multiple times before the US Senate and House and was an initial member of President Clinton's National Infrastructure Assurance Council and winner of the 2005 Azimuth Award, a lifetime achievement award recognizing outstanding service of a single, non-government person responsible for improving federal information technology. In 2010, the Washington Post named him one of seven people "worth knowing in cybersecurity." Alan co-chaired the DHS Task Force on Cyber Skills and headed the FCC Task Force on Best Practices in Cybersecurity. Earlier in his career Alan helped build one of the first large public software companies.

ISBN 978-0-578-83950-9 US$25.00 52500
9 780578 839509

CIO INSTITUTE

CIO.org