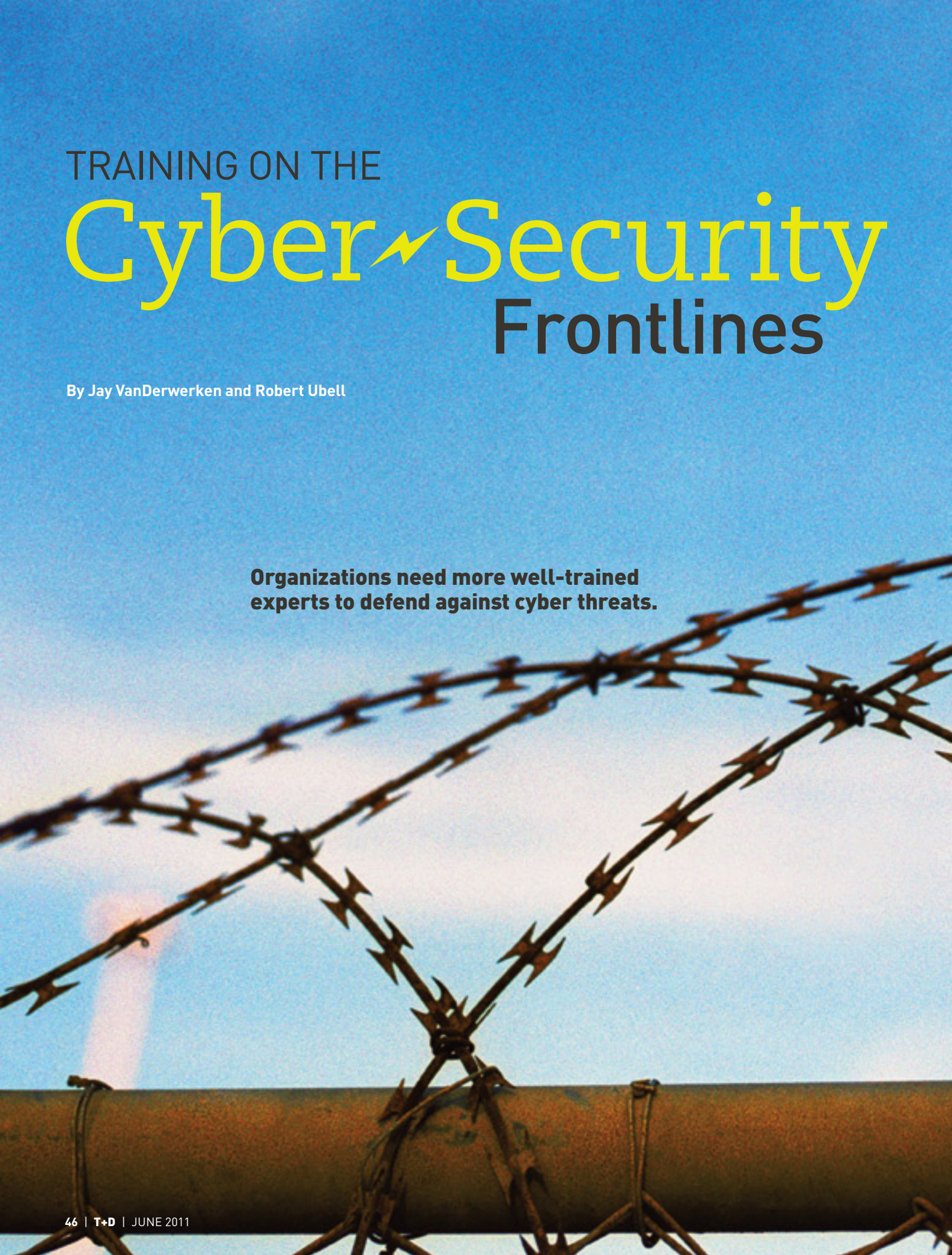
TRAINING ON THE Cyber Security Frontlines

By Jay VanDerwerken and Robert Ubell

Organizations need more well-trained experts to defend against cyber threats.



Cyber security continues to be on the top of the agenda for CEOs and high-ranking government officials because they know that online security can no longer be partially addressed or uncomfortably ignored. However, according to a Booz Allen Hamilton survey, the nation's cyber defense is seriously challenged by shortages of highly skilled cyber-security experts.

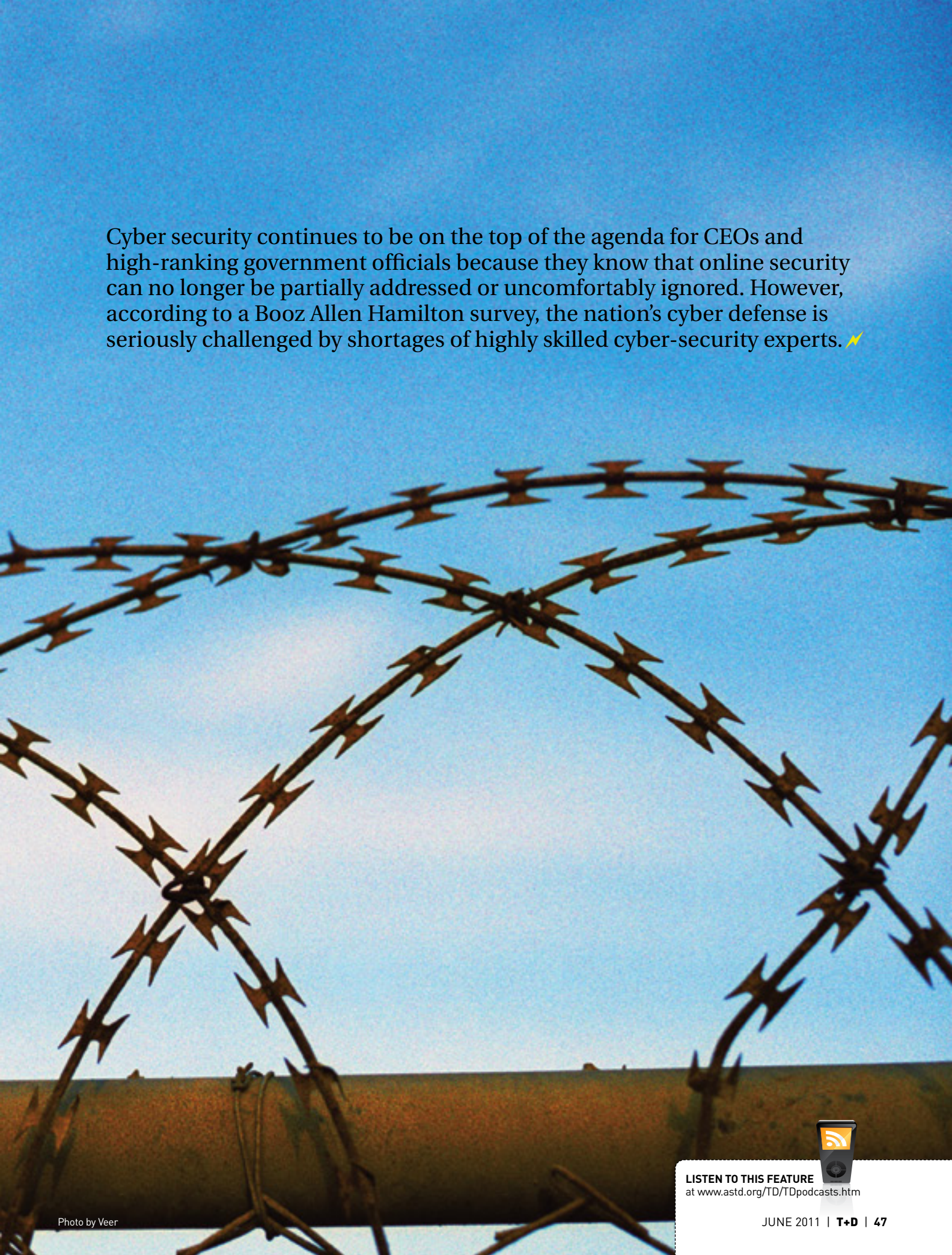


Photo by Veer

LISTEN TO THIS FEATURE
at www.astd.org/TD/TDpodcasts.htm

The report notes that 40 percent of chief information officers, chief information security officers, and IT managers are unsatisfied with the quality of cyber-security job applicants, and according to SANS Institute Research Director Alan Paller, more than 30,000 specialists are needed today. However, he claims that "only about 1,000 to 2,000 have the necessary skills" to combat the numerous real-life scenarios happening in today's organizations.

A network administrator at a Fortune 100 company is tasked by her superior to order a specific router required for a time- and budget-sensitive systems upgrade. She searches the Internet for the most cost-effective solution and finds it at a fraction of its list price on several sites, guaranteeing delivery and warrantees for the life of the product.

She places her order, and the box arrives, with name, serial number, and installation directions intact. The upgrade could not have gone more smoothly. But unbeknownst to her and others responsible for the network's integrity, she has just installed an innocent-looking piece of hardware, embedded with stealth malware that will provide access to a rogue invader to virtually any file or electronic communication on her company's network.

Totally unaware, she purchased it from an illegal, but legitimate-looking website, from a company that manufactures and sells equipment illegally, branded under well-known industry names. If she had called the real company's customer service, she might have discovered her mistake.

Difficult and expensive talent search

While cyber security is emerging as a high-demand career, the problem, SAIC's Vice President for Cyber Programs Robert Giesler discovered, is that finding qualified people today is difficult and expensive. "U.S. graduation rates for four-year degrees are declining, and of those graduating, many are not in a science, math, or engineering program. Of those in technical programs, only a third qualify for top-secret clearance; which makes for a small pool of applicants for the federal market," Giesler laments. SAIC's need for cyber personnel is aimed at providing cyber-security specialists under contract to the federal government and, increasingly, to the industry.

The U.S. military also is running into the same problem, prompting Giesler to propose that SAIC make a strategic decision to educate from within, rather than struggle to fill the company's cyber-security slots with experts from outside the firm. Mounting an internal campaign to raise the technical level of highly motivated employees, SAIC partnered with NYU-Polytechnic Institute to send more than 600 staff through the school's prestigious online cyber-security master's program over the next several years.

New hires versus promoting from within

Matthew Bidwell at University of Pennsylvania's Wharton School of Business substantiates SAIC's decision. "Despite the fact that external hires underperformed those who are promoted, they were also paid around 15 percent more," Bidwell explains, based on his recent research. "In part, this difference reflected the hiring of more experienced and educated workers than those who were promoted."

"The less that you know about a potential employee, the stronger the curriculum vitae you are likely to demand," Bidwell acknowledges. "The difference between hires and promotes likely reflects new hires concerns about the job. They know less about what they are getting themselves into, as evidenced by their higher rates of voluntary and involuntary turnover.

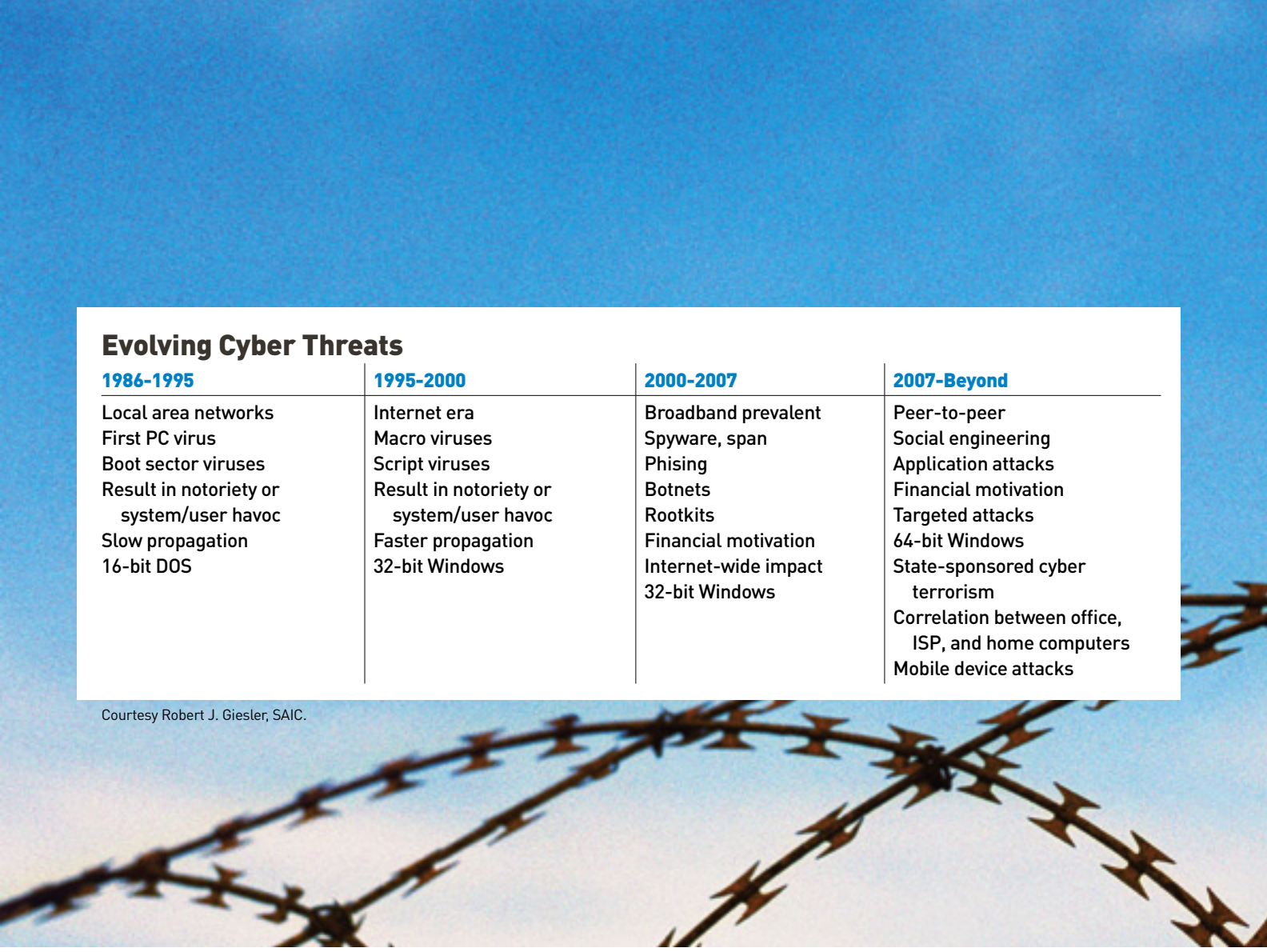
Inadvertent mistakes are better avoided when consistent and specific training is given to non-IT staff regarding the dangers their everyday activity can incur.

"Either way," Bidwell concludes, "compensation of external hires is substantially more than for workers promoted from within the firm. And that gap declines very slowly. There is also evidence that the increased pay of new hires ultimately leads firms to raise the pay of all workers in the group, further raising costs to the firm."

Bidwell's research also showed that performance evaluations for external hires were lower than those promoted into the same jobs for up to three years after they started the job, even taking supervisor bias into account.

By recognizing resource constraints and the timeframe in which they need to bring employees up to speed, Giesler found that by educating existing employees, the company would alleviate the problems of finding top-secret–eligible candidates to emerge as strong cyber cops at a digestible cost.

SAIC has introduced a two-tiered approach. Those with the right skills are enrolled in top-ranked graduate programs. For others, the company engages commercial vendors such as the computer-security training company SANS Institute with classes for personnel in niche areas. For the near and long term, SAIC's objective—and equally the goal at other organizations whose business depends on protecting client networks—is to build an army of cyber warriors.



Evolving Cyber Threats

1986-1995	1995-2000	2000-2007	2007-Beyond
Local area networks	Internet era	Broadband prevalent	Peer-to-peer
First PC virus	Macro viruses	Spyware, span	Social engineering
Boot sector viruses	Script viruses	Phising	Application attacks
Result in notoriety or system/user havoc	Result in notoriety or system/user havoc	Botnets	Financial motivation
Slow propagation	Faster propagation	Rootkits	Targeted attacks
16-bit DOS	32-bit Windows	Financial motivation	64-bit Windows
		Internet-wide impact	State-sponsored cyber terrorism
		32-bit Windows	Correlation between office, ISP, and home computers
			Mobile device attacks

Courtesy Robert J. Giesler, SAIC.

Negligent employees

Most of us are unaware that the biggest and most pervasive attacks are caused by negligent employees clicking on invasive files embedded in messages from beyond company firewalls. Despite strenuous efforts by most companies to alert personnel to email and Internet behavior that opens up firms to invasion, employees continue to do foolish things.

Mobile devices make networks particularly vulnerable. "As more access is given to the end user by means of mobile computing, cyber-crime prevention has to be a top priority. The corporate landscape requiring protection is multiplying at very quick pace," cautions Marc Sachs, vice president of National Security Policy at Verizon.

Sachs has also seen a significant increase in embedded malware within hardware equipment purchased by U.S. companies. "Many companies just don't understand how vulnerable they are in areas they never would expect there to be flaws, such as hardware purchasing," says Sachs. Inadvertent mistakes are better avoided when consistent and specific training is given to non-IT staff regarding the dangers their everyday activity can incur.

Online learning as global bonding

A major global financial institution also has made the strategic decision to educate its worldwide IT global workforce with graduate degrees to ensure protection against threats. "We decided to enroll key employees in NYU-Poly's cyber-security graduate program because of the global nature of cyber within our firm," remarks the chief information security officer. "We see this program as a bonding experience among global executives—one that will connect them through online collaboration long after they've earned their degrees."

NYU-Poly's cyber program is delivered online, allowing global companies to enroll its worldwide security staff without disrupting work and family responsibilities. Professor Nasir Memon, head of NYU-Poly's security program, is alarmed by the increasing sophistication of attacks as well as the speed at which they occur.

"It is not uncommon for large organizations to receive thousands of attacks each day," says Memon. "Our program is aimed, not only at dealing with attacks as they occur, but equally with how a cyber specialist can be proactive in this invisible warfare."

SAIC and other company employees enrolled in NYU-Poly's cyber courses enter the school's virtual lab, where they safely simulate attacks and defenses in an exact replica, mirroring an actual network. At the conclusion of their rigorous online coursework, they earn full master's degrees, typically in two to

Photo by Veer

The Numbers Behind the Threats

The Booz Allen Hamilton study "Cyber IN-security: Strengthening the Federal Cybersecurity Workforce" recommends that agencies adopt the following best practices for onboarding and successful retention:

- Develop onboarding programs for all new employees, but also have special programs for new cyber-security employees to acclimate them, introduce them to colleagues and immediately familiarize them with the agency's cyber-security work.
- Implement training and development programs, including rotations to different parts of the agency that do cyber-security work, to grow skills and knowledge, and include a career path with opportunities to earn appropriate certifications.
- Make new employees feel connected to the mission by using them in recruiting and outreach programs at universities and high schools.
- Identify financial and nonfinancial incentives to help retain employees, including student loan repayment and tuition reimbursement for continuing education.
- Encourage networking across the agency's cyber-security workforce (including field locations) to build loyalty and help create a framework where all cyber-security resources can be mobilized if needed.

Source: Booz Allen Hamilton, http://bit.ly/k2Zlxa

three years, depending on their day-to-day workload and how quickly the company needs them in place.

No company can be passive

As pervasive as cyber attacks now are, no company can be passive. Attacks are targeted at utilities, banking and financial services, healthcare, insurance, chemical, telecommunications, and many other industries, even your local the supermarket's supply chain at a nearby mall.

As long as there are cyber criminals ready to strike, your company remains vulnerable. Vigilant cyber-security training and education must be your company's top priority.

Bank of America/Merrill Lynch's Vice President of Securities Fraud Cassandra Chandler knows this all too well. "As cyber criminals continue to expand and gain access to even more financial information, we continue to evolve our capabilities and expertise to ensure that our customers are protected," says Chandler. "We continue to make tremendous strides in this area."

A recently published study by computer security firm McAfee and Purdue University reported that in 2008, cyber theft topped $1 trillion. The study was based on responses from 800 CIOs worldwide. McAffee CEO David DeWalt says, "The report is a wake-up call, and the trillion-dollar figure is actually a conservative estimate."

Organizations must provide sophisticated training to in-house experts to ensure the integrity of internal and client systems. They must also offer instruction to their entire workforce to avoid cyber minefields surrounding us all.

Simple, yet effective, training must be provided to personnel for general awareness, while graduate education is now globally available to specialists to gain the high level of expertise your company requires. As long as there are cyber criminals ready to strike, your company remains vulnerable. Vigilant cyber-security training and education must be your company's top priority.

Jay VanDerwerken *is managing director of business development at NYU Polytechnic Institute; jvanderwerken@poly.edu.* ***Robert Ubell*** *is vice president of enterprise learning at NYU Polytechnic Institute; rubell@poly.edu.*

T+D

TRAINING + DEVELOPMENT

YES!

I would like to subscribe to ***T+D*** magazine—12 monthly issues that keep me at the forefront of workplace learning and performance.

❒ Individual rate $150 ($216 outside the U.S.)
❒ Institutional rate $300 ($366 outside the U.S.)

TD0833

Order Information

Name: _____

Title: _____ Company: _____

Address: _____ City: _____

State/Province: _____ Zip/Postal Code: _____

Country: _____ Email: _____

Phone: _____ Fax: _____

Check One:
❒ $150 (Individual USA)
❒ $300 (Institutional USA)
❒ $216 (Individual Outside the US)
❒ $366 (Institutional Outside the US)

❒ VISA ❒ MasterCard ❒ Amex ❒ Discover ❒ Check (USD) (Payable to *T+D*)

Card Number: _____ Expiration Date: _____

Signature: _____

Fax this form to 1.205.995.1588 OR Mail to:

American Society for Training & Development
Subscription Office, P.O. Box 11806
Birmingham, Alabama 35202-1806, USA

Order online at **store.astd.org**
Phone: 1.866.802.7059

Orders processed within three business days.
If you have questions, please contact **td@subscriptionoffice.com**

Prices valid through 12/31/2010. If you should wish to cancel your subscription for any reason, you will receive a refund on all unmailed issues. Your subscription to *T+D* may be a tax deductible business expense. Please allow 6 to 8 weeks to receive your first issue.

T+D is published by the American Society for Training and Development (ASTD)

090938.63250

ASTD
WORKPLACE LEARNING & PERFORMANCE