ARMOR™

BETWEEN YOU AND THE THREAT

# Re-imagining the cyber warrior of the future

**CLOSE THE GAP TODAY, WIN THE FIGHT TOMORROW** | CSO VANTAGE POINT

JEFF SCHILLING | **CHIEF SECURITY OFFICER | ARMOR**

# The war is real

Perhaps James R. Clapper, U.S. Director of National Intelligence, said it best in a February 2015 statement to the U.S. Senate Armed Services committee.

"Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication and severity of impact; the ranges of cyber threat actors, methods of attack, targeted systems and victims are also expanding," Clapper stated, as reposted by The Washington Times.

To quantify the issue, the Ponemon Institute reported that the average cost of a data breach jumped 23 percent in 2014.

The study, "Cost of Cyber Crime Study," commissioned by HP, found that organizations worldwide spent $7.4 million, on average, cleaning up after a breach. These organizations also require more time to resolve a data beach, "climbing to 45 days, up from 32 days in 2013."

While that may be a conservative average, a successful breach can easily span into the hundreds of millions. For example, Target's breach recovery efforts have cost the Minnesota-based retailer more than $160 million.

While attack types, vectors and enemies grow in scale, number and veracity, the tools to combat and defend are extremely limited. Most unsettling, the No. 1 asset in countering attacks is also the most scarce: cybersecurity professionals.

> "Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication and severity of impact; the ranges of cyber threat actors, methods of attack, targeted systems and victims are also expanding."
>
> JAMES R. CLAPPER
> U.S. DIRECTOR OF NATIONAL INTELLIGENCE (DNI)

## 209,000 … and climbing

This deficiency in cybersecurity talent has skyrocketed to more than 209,000 unfilled jobs in the United States alone (up 74 percent), according to a recent PBS story.

This need was further reiterated during President Barack Obama's cybersecurity summit at Stanford in February 2015, where cybersecurity experts and government leaders cautioned many times the critical shortage of skilled cyber warriors.

In a perfect world, CSOs would pick up the secure red phone for a direct line to the cybersecurity training factory. Instantaneously, 200,000 cybersecurity professionals would be produced to quickly meet demand.

Would you be able to successfully train a doctor in a year? It may be a simplification of the issue, but good cybersecurity professionals require years of training. Given the current shortage, it's easy to see the dire nature of the situation. This will not be an easy or fast fix.

Unfortunately, the current situation is dire. Many senior-level executives — even experts who work in the cybersecurity field — lack much-needed understanding of what traits are most important when recruiting or hiring cybersecurity talent.

What compounds this challenge? Most education programs, at colleges and universities, can't offer the experience-based training required to fill the widening talent gap.

So, what do you look for in cybersecurity talent? How can our educational system work with industry leaders to accelerate the output of trained security professionals?

## Directing the searchlight

Cybersecurity vendors and agencies can't discover and hire talent fast enough — particularly in the current threat landscape.

At Armor, we average 50 to 60 resumes each week from prospects wanting to join the Armor security team. Of those, maybe 5 percent meet our standards. Why? In short, colleges and universities do not prepare students for success in the cybersecurity field. This is my opinion based on three-plus years of post-military cybersecurity recruiting.

When I do find a talented prospect with the right skillset, I rarely notice if they even have a degree. I value talent and experience. Cybersecurity is a skills-based profession — one that's rooted in capability, experience, practice and aptitude.

From my experience, universities — and to an extent technical schools — fail to mimic complex security environments, even for small- to medium-sized businesses.

### So, where are the cybersecurity specialists of the future?

"Most education programs, at colleges and universities, can't offer the experience-based training required to fill the widening talent gap."

JEFF SCHILLING
CSO | ARMOR



ARMOR™

# Decipher: 3 critical job functions

The obvious conclusion: Hire and recruit talent away from companies where they are currently — and successfully — performing on the job.

This strategy, however, has driven up the cost of skilled labor. It's no longer an option for most security teams. As a result, many vendors and security-conscious organizations are opting to discover and train their own talent.

There are three major functions for providing IT service: host and application administration; computer programming; and network engineering. All three IT functions can directly pivot to a cybersecurity discipline: host forensics, malware analysis and network forensics, respectively.

The critical data that a security analyst has to understand when detecting threat activity relates to these three IT and security functions. When I screen resumes for security prospects, I look for experience in one or more of these fields of work, either as an IT specialist or security specialist.

In fact, if I had to choose between a university-educated cybersecurity graduate or an IT specialist who is strong in sys admin, networking or programming, I will pick the IT specialist every time.

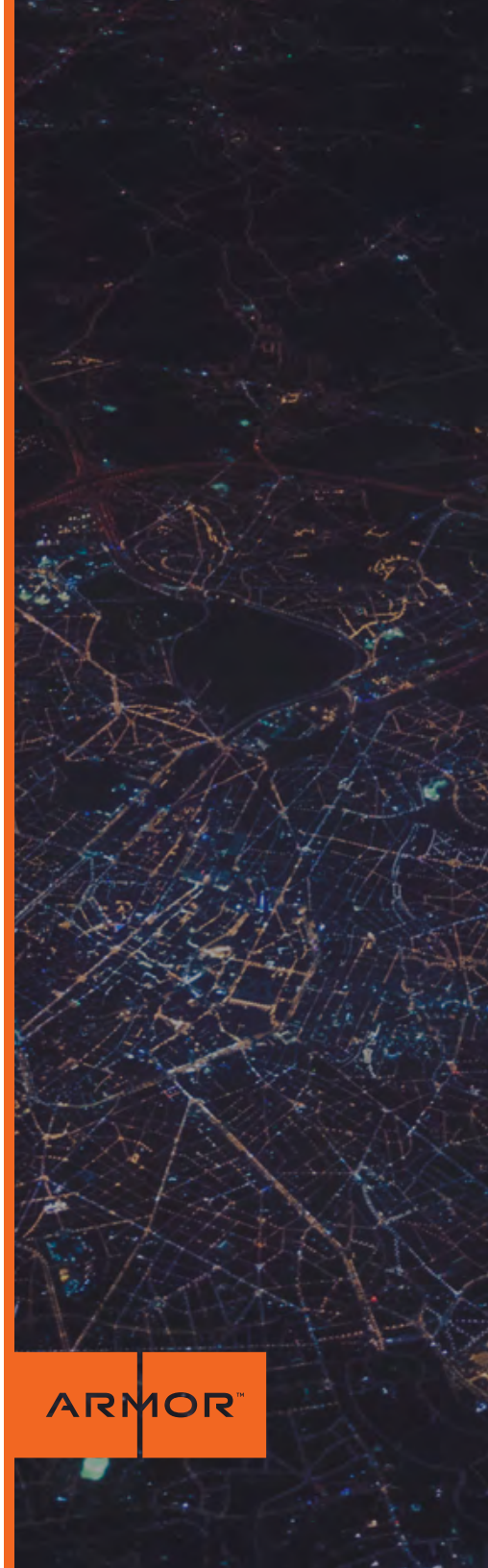
The ideal prospect is often an individual who oversees a small IT shop, where they manage and execute in all three functions.

A model cybersecurity pro must understand how the IT infrastructure works before they can understand how to protect against and find threat activity.

## Map the roles

Trouble filling cybersecurity jobs? Review this simple breakdown on how standard IT jobs map to cybersecurity disciplines.

| IT function | | Cybersecurity discipline |
|---|---|---|
| Host & application administration | → | Host forensics |
| Computer programming | → | Malware analysis |
| Network engineering | → | Network forensics |



## Are certifications valuable?

Are certifications a valid indicator of talent? Yes and no. When you're able to successfully align related certifications with relevant job experience then, yes, certifications are significant.

It's not always that clear, however. Many security prospects possess certifications but no track record of real experience related to those certifications. In these cases, certifications are not a good judge of talent.

My trick is to look at an applicant's experience, then see what level of certifications they have been able to achieve. In this way, I use certifications as a validation that the prospects not only have experience, but also have passed a benchmark to demonstrate their skills and abilities.

A red flag may rise when someone has many certifications that don't inherently go together. We call these individuals "badge finders."

"A model cybersecurity pro must understand how the IT infrastructure works before they can understand how to protect against and find threat activity."

JEFF SCHILLING
CSO | ARMOR



## Reform for higher education

This first suggestion is actually quite provocative: Eliminate cybersecurity undergraduate programs. In my opinion, security should be required and integrated into all computer science and engineering undergraduate programs.

As we train our future sys admins, programmers and network engineers, we need to remain diligent in teaching the principles of cybersecurity. This approach will provide future cybersecurity pros a vast understanding in how IT infrastructure works — and before they decide to specialize.

This change also will have the inverse effect of ensuring our IT service providers are better rounded in security. This gives cybersecurity directors, managers and leaders, who are looking for entry-level security professionals, a broader group to assess. When needed, we may then leverage graduate and doctorate programs for specialization in security.

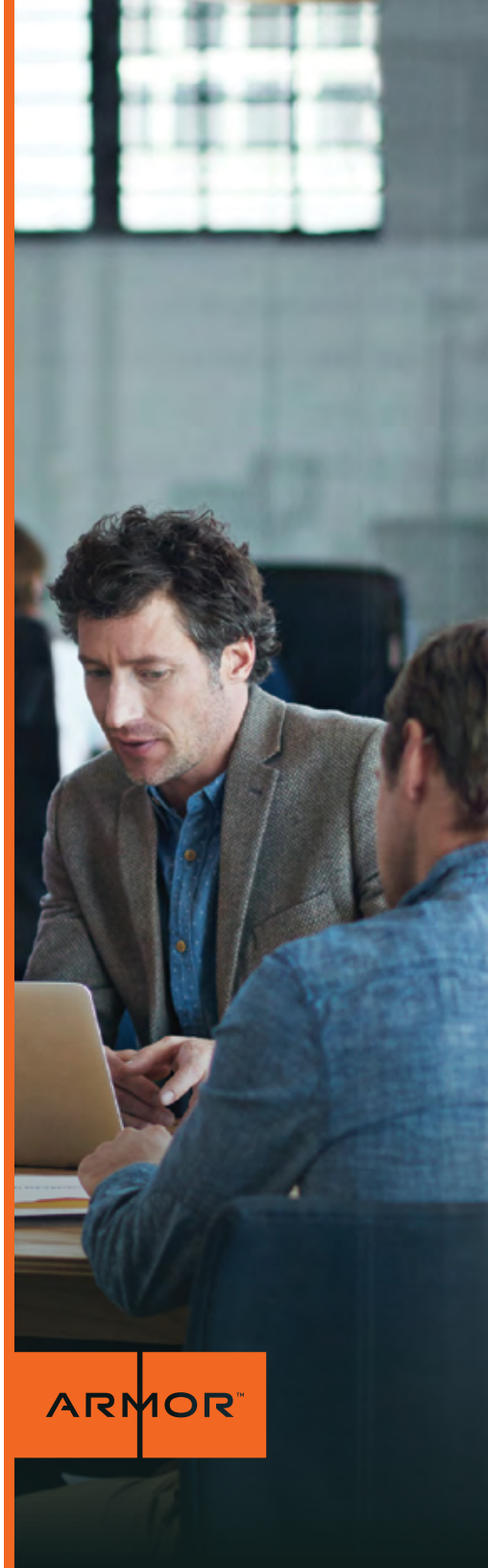
## Teaching technical trades

The second solution is not nearly as proactive. We are critically short on security personnel with hands-on technical skills in managing security infrastructure — a skill that does not take four years to learn and does not require a live environment to become proficient.

What does this entail? Typically, it's the management of devices in a security stack (e.g., firewall, IPS/IDS, WAF, etc.). These talents are great opportunities for vendor-managed training programs and technical schools.

The programs exist today, but we are not placing enough students into proper courses. Could government grants drive more students to look for this opportunity? Perhaps.

It would also be advantageous for more vendors to work directly with technical schools to provide equipment and training packages to facilitate producing more cybersecurity wrenchturners for gear they hope to sell.



## Return of the apprentice

My last suggestion is core to classic professional training models that date back to the middle ages: Establish a master-apprentice framework for cybersecurity.

In fact, I set up this model when I wished to accelerate the progression of forensic college hires in an incident response practice.

The good news? We severely underestimated the success we would achieve in this mentoring program. Our forensics specialists were doing advanced work — within just six to eight months.

These recommendations, however, are moot unless implemented in a timely manner. Until a thoughtful, strategic plan is employed to change how industries find, train, educate and pair professionals to appropriate security jobs, there will remain a major shortage of specialists with the skills to help defend the dynamic cyber landscape.

"Placing security training at the core of all computer science and IT tracks is the first step in evolving how we prepare to properly defend valuable assets, information and digital identities. But it's only a start."

JEFF SCHILLING
CSO | ARMOR



# About Jeff Schilling

Jeff Schilling (Ret. Col., U.S. Army) is Armor's chief security officer and is responsible for the cyber and physical security programs for the corporate environment and customer-hosted capabilities.

Schilling retired from the U.S. Army after 24 years of service in July 2012. In his last assignment, Schilling was the Director of the U.S. Army's global Security Operations Center under U.S. Army Cyber Command. In this position, he was responsible for synchronizing the global security operations/monitoring and incident response for over 1 million computer systems, on 350 wide-area networks, supporting all U.S. Army organizations in more than 2,500 locations.

Previous to this position, Schilling was the Director of the Department of Defense's (DOD) global Security Operations Center with Joint Task Force Global Network Operations, where he managed security operations and global incident management for over 4 million globally connected computer systems.



US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167



ARMOR™
BETWEEN YOU AND THE THREAT