Cybersecurity: The Talent Challenge
Companies Struggle to Compete for Skilled Workers

By BEN DIPIETRO

Peter Metzger, a headhunter, tells his corporate clients he can find them the most accomplished and experienced cybersecurity workers but then moves to discuss a competitive salary and benefits.

“I say, ‘I know them and their compensation looks something like this,’ and I hand them a piece of paper with the number and they gag, and I say, ‘Where is your limit?’” said Mr. Metzger, a vice chairman and cybersecurity and business-risk expert at DHR International Inc., a global executive-search firm. He categorizes the worker shortfall as “somewhere between serious and acute.”

It’s not just the top talent that is being sought out by companies trying to fill a growing number of cybersecurity jobs. A report from consulting and services firm Booz Allen Hamilton Inc. and the Center for Cyber Safety and Education forecast a world-wide shortfall of 1.8 million cybersecurity workers by 2022, an increase of 20% from the group’s previous shortfall prediction made in 2015. A survey of IT executives and managers by cybersecurity firm Trustwave found 57% said finding and recruiting people to work in cybersecurity is their biggest challenge.

Many of those who have jobs in cybersecurity don’t have the requisite skills, another sign companies are scrambling to find people. A survey of cybersecurity professionals by Isaca, an advocacy group for information security professionals formerly known as the Information Systems Audit and Control Association, found 25% said cybersecurity job candidates lack the technical skills needed, while 45% said candidates don’t understand the business of cybersecurity. Any cut in the number of H1-B visas that allows companies to bring in tech talent from overseas—something the Trump administration is considering—could exacerbate the problem by shrinking the available talent pool even further.

“New people entering the workforce are not at the numbers we need, nor do they have the level of technology and operational capabilities we need,” said Patrick Gorman, head of strategy for CyberGRX, a cyber risk management firm.

During his time as chief information security officer for Bank of America Corp., Mr. Gorman said close to 2,000 cybersecurity people were hired by the bank. “All we were doing is raiding each other. If they were at another big bank, I would raid them and they would raid my people,” he said.
SHORTAGE BOOSTS SALARIES
That competition is driving salaries higher. A bulletin put out in March by SilverBull, an IT cybersecurity recruiting and staffing company, found the median average salary for a chief information security officer was $223,000, up from the $204,000 the company posted in a bulletin two months earlier. The number is higher for CISOs in major cities, with those in San Francisco getting an average salary of $421,000 and those in New York $406,000.

But raiding and competing for the same limited pool of people doesn’t solve the larger question of how to get more people trained to work in cybersecurity. A pipeline is beginning to develop as universities launch degree and certificate programs in cyber-related fields and more people enroll in such programs. The military and government remain robust training grounds where people can acquire advanced skills and then transition to the corporate world and a higher paycheck.

Dave Mahon, chief security officer at telecommunications company CenturyLink Inc., said former military people are in demand because they have a more holistic view of cybersecurity that comes from their military training. In the military they had to consider issues not just from a technology or cybersecurity view but had to factor in political considerations and geopolitical concerns, giving them a broader perspective for the implications of taking certain actions.

“I love to recruit from the military,” he said. “There are ways to recruit them, and certain headhunting firms specialize in transitioning military personnel to corporate America.”

Some companies are taking existing workers and retraining them to work in cybersecurity roles, and other firms are hiring outside companies to oversee their cybersecurity—or reducing their need for additional manpower by relying on machine learning, artificial intelligence and other automated tools to monitor and react to any cyberthreats.

“Companies are always looking for good people” and that will still be the case even amid growing use of non-human resources, said Nathan Burke, vice president of marketing at Israel-based cybersecurity firm Hexadite Ltd. “Even if you have a bunch of analysts and start using automation, you wouldn’t lay them off but would make them work on something more interesting.” And even if companies could rely on AI and other technologies to handle their cybersecurity, they still would need people to run those systems, said Eran Barak, chief executive at Hexadite. And if there aren’t enough people trained to work in that area? “Then we will have a real serious problem,” said Mr. Barak.

Mr. Mahon agreed, saying while it’s “going to be substantial to have technological solutions,” employees also are going to need better training to give them a more well-rounded view of what cybersecurity entails. “The profession has to evolve. There was a time when you could be a good accountant with a two-year degree; now you need to be a CPA, combining certifications and training to be a more holistic thinker,” said Mr. Mahon. “That’s where the cybersecurity industry has got to move.”

OTHER WAYS TO COMPETE FOR STAFF
For companies trying to retain their cyber staffers, especially those with small budgets that can’t compete on dollars alone, all is not lost. Ron Sanders, a vice president and fellow at Booz Allen Hamilton who previously worked as an associate director of national intelligence at the Office of the Director of National Intelligence, said many people are attracted to the cybersecurity profession by the challenge of the work and to the mission of fighting bad guys, and government departments and companies can use that to their advantage.

“Surveys show, and our own ground-level experience validates, that money is not the only thing and not the most important thing in many cases,” said Mr. Sanders, especially for Millennials and military veterans. Organizations that can’t compete on pay need to focus on a “value proposition” that appeals to a person’s sense of mission, highlights the cutting-edge nature of the work they will be doing and emphasizes opportunities for advancement and the chance to work on different projects. Even then, many will leave for other opportunities.

Mr. Metzger said offering flexible work hours, the ability to telecommute and generous vacation and time-off perks can go a long way to convincing young people to take a job with lower pay. “Don’t rely compensation alone; find other ways to attract people,” he said. “People want to come where it’s cool, where they have cool projects, cool tools and technologies.”

In the old days, companies would invest in an employee, send them to school, move them around to various jobs to hone their skills and, in return, would expect that person to work for them for 15, 20 years or more. “But we know Millennials just don’t do that and employers had to learn that it’s OK” to provide opportunities even if an employee doesn’t stay married to them for their entire career, said Mr. Sanders. “In the case of a cybersecurity workforce, a rising tide helps all boats.”

Another area where companies can do better to recruit and train the next generation of cyberworkers is focusing on women, minorities, veterans and older workers, said Mr. Sanders. A report from PwC released in March found women make up 11% of all information security workers globally. “Employers have some obligation to partner with high schools and colleges...if nothing else it helps the kids realize how exciting and lucrative cybersecurity career can be,” he said. “Companies and government agencies can collectively put the spotlight on cybersecurity careers. Universities at the undergraduate and graduate levels—even at the community college level—need to do a better job of providing graduates with real hands-on cyberskills.”
Hiring Ex-Spies Requires More Than Just High Pay

By JEFF STONE

U.S. companies struggling to find and hire the employees they need to protect their organization's information security are looking to Washington, particularly the intelligence community, to remedy the skills shortage.

Soaring cybersecurity salaries—one recent poll found that top earners take up more than $400,000 annually—have made it almost impossible for cash-strapped small and medium sized firms to hire experienced chief information and chief information security officers, creating a job shortage of an estimated one million unfilled positions. Even Fortune 500 companies have struggled to retain the top talent in this field, in part because professionals working in major cities are contacted regarding a new position at least once a week, according to a December 2016 study from the Enterprise Strategy Group research firm.

But security professionals and the bosses trying to hire them agree that the best way companies can dip into the talent pool is to wade into the military and intelligence community. By recruiting veterans from the National Security Agency, Federal Bureau of Investigation, Central Intelligence Agency, and others, corporate America can at least double a government worker's salary, and attract a new employee who might have invaluable experience from the front lines of cyberwar. Some hires could also facilitate meetings between companies and potential government clients.

But even if companies can easily outspend the government, they're also competing with each other, which makes it essential to appeal to security experts in other ways, too.

“For true hackers, if they're bored at work, that's just a death knell,” said Patrick Wardle, the director of research at the...
penetration testing firm Synack Inc., and a former NSA staffer. “They thrive on creativity and solving hard problems. A lot of the companies I talked to when I was making the transition [to the private sector] were companies that were really making a difference.”

Money is certainly a factor, Mr. Wardle said, but it’s not the only selling point for a new job. Government workers were paying attention to the technology industry’s reaction to the leaks from former NSA contractor Edward Snowden. Many of the prominent companies named in the leaks publicly criticized the NSA for its surveillance tactics, a stance that roiled many in the intelligence community, Mr. Wardle said.

“If you’re a company that has an us versus them mentality, and I’m from ‘them,’ it’s very hard to forget that,” Mr. Wardle said. “But it’s just what your culture aligns with. If a company takes such a black and white approach to something, it could create complicated issues.”

**MARKETING SKILLS ENHANCEMENT**

There’s also a heavy burnout factor in the industry, so security professionals look for a culture where they’re rewarded for independent efforts to improve themselves, experts agreed. Jon Oltsik, a senior principal analyst at the Enterprise Strategy Group, a market research firm, polled IT workers to find that top security experts prioritize almost constant training. For many, that means employers should allow chief security officers, CISOs, and their teams to foot the bill for penetration testing, for example, travel to conferences, research forums, and the like.

“I tell companies that want to recruit and retain talent, ‘Market yourself as a place of cybersecurity excellence,’” Mr. Oltsik said.

That desire to continue achieving can not only yield a higher salary, experts say it’s related to a “mission first” mentality. It’s a personality trait that keeps the best and brightest motivated to learn more, and keep focused on a valuable tasks. It’s also something many intelligence community veterans remember after leaving government.

With that mindset, perhaps it should be no surprise that former digital spies move to startups, Silicon Valley, or into the world of private contracting, where they can keep their MISSION FOCUS while DOUBLING OR TRIPLING a government salary, after Washington.

For many job candidates, “mission first” means keeping as many users as safe as possible, said Jeremy King, founder of the headhunting firm Benchmark Executive Search LLC. Mr. King explained that when he’s recruiting job prospects on behalf private intelligence companies, advanced technology manufacturers, or other companies working in national security, he first scours ex intelligence officers with the assumption they will be most interested because of the industry’s similarity to the military.

The challenge is that many hiring managers are thinking the same thing.

“It’s a very aggressive environment for talent,” said Tim Estes, chief executive at Digital Reasoning Inc., an artificial intelligence company that uses software to scan messages at financial institutions to detect potential fraud incidents. “You can think you have a great person, then someone else drops in and doubles the salary offer at the last minute.”

Digital Reasoning announced in February it appointed Al Tarasiuk, the former chief information officer at the Office of the Director of National Intelligence and the chief security officer at Deutsche Bank AG, as a board member. In this government role, Mr. Tarasiuk developed a desktop program that enabled officials across the intelligence community to share information faster.

It’s not the company’s first foray into the intelligence community—Mr. Estes said Digital Reasoning employed a former senior Department of Homeland Security official, among others—but Mr. Tarasiuk’s ongoing employment at Deutsche Bank highlights the difficulty of finding candidates without existing opportunities.

“‘They just know what tools can be used, and how they can be applied when it comes to key missions,’” said Mr. Estes, on what makes candidates like Mr. Tarasiuk so attractive.
Tighter Immigration Laws Will Limit Cybersecurity Options

By ADAM JANOFSKY

aced with a shortage of cybersecurity talent, many companies have come to rely on hiring foreign experts to fill their security gaps. But stricter immigration policies will likely tighten this workaround for the foreseeable future, according to immigration lawyers and cybersecurity professors.

New immigration policies that focus on “extreme vetting” will inevitably make it harder for foreign cybersecurity professionals to find work at American companies.

“Anyone who is involved in sensitive technology that might require an extra layer of scrutiny will have extra review,” said Angelo Paparelli, a partner at Seyfarth Shaw LLP and founder of the Alliance of Business Immigration Lawyers. “Cybersecurity experts would be at the top of the list.”

Businesses and universities saw the first signs of this when President Donald Trump signed an executive order in January that suspended entry of immigrants from seven countries: Iran, Iraq, Libya, Somalia, Sudan, Syria, and Yemen. In the cybersecurity world, Iran is seen as a hub for computer engineers.

After the order was blocked in federal court, the White House issued a narrower travel ban that removed Iraq from the list of countries and exempted green card and visa holders. That order also faced a setback on March 15 when a federal judge in Hawaii blocked it from taking effect nationwide.

In the wake of these orders, hundreds of academics involved in cybersecurity research posted job opportunities outside the U.S. for those affected by the travel ban.

Tim Güneysu, a computer engineering and IT security professor at the University of Bremen in Germany, said his department is expecting to receive a surge in international applicants this year as a result of stricter U.S. immigration policies.

“We typically receive quite a number of applications from highly skilled and clever Iranian students,” said Prof. Güneysu, continued on page 7 >
“We typically receive quite a number of applications from highly skilled and clever Iranian students...The U.S. is definitely MISSING THESE OPPORTUNITIES now.”

—Tim Güneysu, computer engineering and IT security professor at the University of Bremen in Germany

adding that German companies and universities—like their U.S. counterparts—are experiencing a shortage of cybersecurity experts. “The U.S. is definitely missing these opportunities now.”

Companies are also bracing for a tightening of the H-1B visa program, which has been used extensively by technology firms to recruit high-skilled workers from abroad.

President Trump’s immigration plan targeted the visa program for reform, arguing that Americans “have been passed over in favor of the H-1B program.” Hundreds of businesses, including Apple Inc., Google, and Anthem Inc, use the program to fill security roles, according to public databases.

Although President Trump has yet to push for specific changes, he took what was seen as a first step on April 18 when he signed the “Buy American and Hire American” executive order, which called for a multiagency review on the changes needed for the H-1B program.

The former Director of U.S. Citizenship and Immigration Services Leon Rodriguez said overall allotments of H-1B visas may be driven down in the near future, which would limit the ability to hire foreign cybersecurity workers. “When you’re talking about cybersecurity, you’re talking about high-end expertise—it’s a boutique niche,” said Mr. Rodriguez, who now works as a partner at Seyfarth Shaw.

Although the fate of the H-1B program remains uncertain, there are some alternative options for recruiting cybersecurity talent from abroad, according to Mr. Paparelli. The EB-11 and O-1 visas can help a company bring in a worker of “extraordinary ability,” who has generally risen to the top of their field. In some cases, these visas can be prioritized when the person’s job is in the national interest.

For firms that are affiliated with overseas operations, the L-1 visa may be an option to transfer a cybersecurity employee to the U.S. The visa generally requires that the American and foreign entities are tied by a common owner.

Additionally, a narrow group of companies can also use E-1 and E-2 visas to recruit cybersecurity experts from abroad. To qualify, the business needs to be at least 50% owned by someone from a treaty nation. An E-3 visa is specifically designated for Australian specialty workers. “Australian cybersecurity experts can come in with a two year grant without much trouble,” said Mr. Paparelli.

For now, companies may take solace in the fact that immigration policy is generally seen as a slow and incremental process. President Trump’s original executive order, for example, was quickly challenged by states and civil liberties groups.

But the Trump administration has already latched onto immigration as a key priority, and has a variety of ways to independently tighten programs like H-1B and Optional Practical Training, which gives foreign technology graduates the right to seek employment in the U.S. for up to three years.

“‘The new administration has really jumped right into it,’” said Mr. Rodriguez.
Criminals are Diverse—Employees Should Be Too

By KATE FAZZINI

Pop culture offers plenty of stereotypes about hackers: a hoodie-wearing outcast with the skillset of a thousand criminals; a lone, troubled girl with elaborate piercings and a dragon tattoo; a “400-pound” man skilled at cracking government servers, possibly all while sitting in bed.

But time and again, conventional wisdom about cybersecurity is just wrong. Hiring for skills, knowledge and instinct is critically important in cybersecurity. Diversity of all kinds is important to the industry because, as one expert put it, criminals are male and female, of all ages and races and come from all manner of backgrounds, globally.

“Diversity is very important, because the adversary knows no gender or racial boundaries,” said Phyllis Schneck, who most recently served as deputy under secretary for cybersecurity and communications at the Department of Homeland Security. Earlier this week, Ms. Schneck started a new role leading the cybersecurity practice at consulting firm Promontory Financial Group, an International Business Machines Company. “If we are going to solve problems and be good scientists, then we need diversity, which brings a much broader perspective and more creative solutions,” she said.

According to a study by PwC, just 14% of the U.S. cybersecurity workforce is women; a study by U.K.-based cybersecurity testing firm CREST International put the global figure even lower, at 10%. Both studies showed that despite efforts to increase the participation of women and girls in fields related to cybersecurity, the numbers haven’t changed significantly in the past decade. While there are few such diversity studies conducted on criminal organizations, the huge prevalence of fraud and crime perpetrated from leading malware producers like China, Brazil, Russia, as well as nations in West Africa, Eastern Europe and Central America point to a diverse global enterprise.

As the chief cybersecurity official within DHS, Ms. Schneck worked with a number of initiatives to help support technology and cybersecurity education for young girls and women. She credits her own success in the industry to early inspiration around technology and computers—her father was a computer programmer for NASA who “brought moon rocks home from work,” and her mother was a mathematician.

Such inspiration is important, said Ms. Schneck. She underscored her point by relating the story of actress Hedy Lamarr, who In

continued on page 9 >
1942, patented Spread Spectrum Technology, a radio signal protocol that is still used today, underpinning Bluetooth, WiFi and the mobile radio signal CDMA (Code Division Multiple Access).

Ms. Lamarr, famous as an actress, isn’t remembered for this still-relevant, “disruptive” cryptologic innovation, a good example of an inspirational story of women in technology that has stayed under the radar, so to speak. Girls may not be gravitating toward cybersecurity careers because they still don’t see themselves in that narrative, nor are they getting comfortable enough with technology early in their education. “My sense is it’s culture,” Ms. Schneck said.

DIVERSITY HELPS CRITICAL THINKING
Ron Kornfeld, a senior business development manager with recruiting firm Mitchell Martin, works to help fill cybersecurity roles at a number of large firms. The issue of diversity in cybersecurity is clearly on the minds of his clients, he said, but what is perhaps most important is the fact that it is simply so hard to fill open positions in the field.

Mr. Kornfeld pointed to a study by the trade group Information Systems Audit and Control Association, which showed around half of all cybersecurity positions get no more than 10 applicants. According to the study, around 27% of companies are entirely unable to fill their open cybersecurity positions, and of the handful of applicants received, 64% of companies said more than half of applicants are unqualified.

Firms that tend to attract more women into cybersecurity roles, he said, have the benefits and perks that appeal to everyone job hunting—better work/life balance, quality of the company brand, career-building opportunities and consideration for family life.

Ms. Schneck said work/life balance may be a reason for some women to hesitate in joining the cybersecurity workforce, but she said this hasn’t created as high a gender disparity in other time-demanding careers, like medicine or law. She emphasized the need for educating girls in computer science much earlier, getting them comfortable with coding and engineering so these career options seem natural later on.

Ms. Moskites emphasized that diversity generally, not just in gender, is a critical component of the evolving cybersecurity workplace.

“Diversity matters for any position that requires critical thinking and problem solving,” she said. “This is especially crucial in cybersecurity because the problems and the technology solutions are in a constant state of change.”

“Fixing Computers in a Skirt”
Early in her career, Tammy Moskites helped an employer link together a fledgling network of computers, part of an actuarial department at a health-care company where she was working to analyze health care trends. She was promised a new job that would be more IT-focused after completing the work, but was surprised when her manager gave the job to a male colleague.

“You know Tammy...we can’t have you fixing computers in a skirt and have you climbing under desks,” she recalled him saying.

Ms. Moskites was inspired nonetheless, and went on to hold high-level technology positions, including the top information security roles at Huntington Bancshares, Home Depot Inc. and Time Warner Cable. She now serves as chief information officer and chief information security officer of cybersecurity company Venafi, a company that helps protect, manage and automate cryptographic keys.

Ms. Moskites said hiring in the cybersecurity field is difficult in general—finding qualified candidates is a challenge and her job requires that she “find the most qualified candidate for the job.” Companies can inspire employees by showing they value merit-based contributions, that skills and attention to detail matter and that they are willing to work with exceptional candidates who are strong in some areas but need training in others.

Qualifications, however, go beyond technical degrees and certificates, she said. Many job seekers, including women, may have highly relevant skills to the industry already. She learned many foundational elements of cybersecurity from starting with her health care actuarial work, “calculating the average
Some Businesses Seek Out Cheaper Security Alternatives

Small businesses that don’t have computer experts on staff or the resources to hire a designated cybersecurity officer are also finding it easier than ever to outsource their security.

Muneer Baig, founder of cybersecurity consulting firm SYSUSA Inc. and a former information security specialist at Microsoft Corp., said he saw a business opportunity for this after reading a 2012 report from the National Cyber Security Alliance that said 60% of small companies that experience a cyberattack go out of business within six months.

Mr. Baig started offering clients an option to hire a “virtual information security officer.” For a fee, a cybersecurity expert would remotely take over a business’s security program, design a customized plan, and recommend tools to minimize risks. He said similar programs are now offered by many other firms.

“It’s not a Cadillac solution, but it meets your business’s needs at any point of time,” said Mr. Baig, who said it’s an especially attractive alternative for small businesses that would otherwise pay over $100,000 a year to hire a chief information security officer.

The cheapest solution for many businesses is leveraging free tools from companies such as Qualys Inc., Hewlett-Packard Enterprise Co., and Tenable Network Security Inc., according to Mr. Baig. When necessary, a company can pay a security expert a small fee to walk them through the reports and identify security gaps.

Ms. Parsons said she relies on affordable software and services from large, public companies, such as Zendesk Inc., QuickBooks (a subsidiary of Intuit Inc.), HubSpot Inc., and Amazon Web Services (a subsidiary of Amazon.com Inc.). “They put security and privacy at the very top of their priority list,” she said.

Another cheap tool for businesses is working with bug bounty programs and so-called “white hat” hackers, who help companies find flaws in their information systems. “Every company should have a way for security researchers to contact them if they find a vulnerability,” said Justin Calmus, vice president of Hacker Success at HackerOne, a bug bounty platform. Mr. Calmus suggests companies set up a “security@” email address that goes directly to the firm’s chief technology officer or chief operations officer.

Mr. Calmus said many researchers try to spot vulnerabilities as a hobby and ethical service, and don’t expect payment for reporting them. “But if it’s something you feel is valuable, absolutely pay for it—you may want to hire that researcher down the road,” he said.
The Chief Security Officer in a hyper-connected world

Finding the talent to secure digitally connected products is becoming a critical job.

By AILEEN ALEXANDER and JAMEY CUMMINGS, Korn Ferry

First it was your credit card. Then your Facebook account. Now hackers have found a way to steal your car. In a well-publicized case, hackers found a way to locate, unlock, and start one automaker’s brand. The maker promptly corrected the problem—but not before adding yet a new layer of high tech jitters.

Welcome to the Internet-of-Things era, where, according to one estimate, there will be nearly 21 billion products and parts sharing information and data with each other by 2020. In theory, this will make the world a more productive, healthier, and better place. But all that potential comes with an ugly underside: the ability to hack once-ordinary physical objects just because they’re connected to the internet. Keeping IoT-enabled products secure will likely shift how corporate security leaders think of their own role and, as importantly, how they create a top-performing security team.

Chief Security Officers and Chief Information Security Officers are long used to thinking about securing networks, PCs and intellectual property. But now they will need to bring products under their umbrella, too. “Some CSOs don’t want anything to do with the product/service side,” said Malcolm Harkins, chief security and trust officer at Cylance, a computer security company. “Even if it’s not a direct reporting relationship, there needs to be a relationship between the two sides, so we are looking at things holistically.”

When a security breach does happen, it can put companies in the embarrassing position of having to explain why they weren’t better prepared. Repairing the damage often ends up costing a lot more than taking proper precautions would have in the first place. Viewed this way, security is just another type of insurance. “What you are insuring against is protecting your reputation from a data breach,” said James Stansberry, SVP and head of Samsung ARTIK’s Stansberry, SW and head of Samsung ARTIK Smart IoT Platform, a division of the Korean electronics giant that makes IoT security and cloud solutions. “People just have to decide how much insurance they want.”

Meeting the talent challenge

Of course, security leaders will need a team of highly-skilled talent to keep a company’s products secure. But recruiting top IoT security talent won’t be easy. Cybersecurity talent already is in short supply, and today’s modern security challenges require a different perspective. Beyond the usual technical know-how, digital security professionals also need good business acumen and strong communications skills. “Security folks tend to want to solve the problem like security folks, when we actually have to think like business people,” explained the top security officer at a medical device manufacturer.

This executive looks for people who don’t give up on finding an answer to a problem. “It is the person who goes through all the scenarios and is looking for that needle in a haystack. And not being that know-it-all security person, but to be able to listen, work, and collaborate,” the executive said. Cylance’s Harkins also stresses the importance of understanding the business. “If you haven’t spent time on the product-creation side, you are going to have to overcome that experience gap pretty quickly,” he said.

Develop alternative talent pools

One way to locate good talent is to look outside the usual sphere. Even though his firm works primarily with technology products, Samsung ARTIK’s Stansberry looks for people in the financial industry, because finance has been working on tough security issues for a long time. “Standards committees are another good source of recruits,” he said. “They become useful when you are trying to secure an ecosystem.”

When the medical device firm executive was looking to build a product security department, he wasn’t sure what was needed. So the executive recruited two employees to study security in other industries. “I sent them out for a year to find out what everybody else was doing, and then in a DevOps model, we helped build and define our own program,” this executive said.

Another CSO hires good technologists and then trains them internally. “I can teach security, but I can’t teach technology,” this executive said. “When you hire, your expectations need to be, ‘I’m not going to find skilled labor in the market. I need to develop it myself,’ so you need your own training process internally. Hire someone two years out of school, train them for two years, and they are good to go.”

A lot of money, time, and effort goes into training someone for a security role. Rather than watch that person hop to a new job six months later, smart CSOs look for ways to make sure they get a return on investment. Martin Bally, CSO at manufacturing firm Diebold Nixdorf, looks for people who are in it for the long haul. “The market is so hot that people can easily jump ship and take a 10%, 15%, 20% bump in pay,” he said. “We look for loyalty, longevity, and a culture fit.”

One strategy Bally uses to make sure potential hires are a good fit is to have them meet with as many people as possible. He also looks for creative ways, such as job rotations, to expose employees to different experiences and a variety of skills, because a good salary isn’t the only thing people care about. They also have to be stimulated in their work.

New possibilities; new responsibilities

The IoT-era is not only creating new types of products but a new type of security leader. This new breed of CSO will need to draw on a new set of skills themselves for when they need to negotiate with product-line leaders, CEOs and other company executives. And they will need to recruit new kinds of talent in order to meet the growing challenges of our increasingly connected world.

AILEEN ALEXANDER and JAMEY CUMMINGS are senior client partners at Korn Ferry and co-leaders of the firm’s Global Security Practice.

Korn Ferry is the preeminent global people and organizational advisory firm, helping leaders, organizations, and societies succeed by releasing the full power and potential of people.

Contact information

AILEEN – 202.055.0931 / aileen.alexander@kornferry.com
JAMEY – 214.665.3055 / jamey.cummings@kornferry.com

Sponsored by
Meet The WSJ Pro Cybersecurity Team

BEN DIPIETRO is an editor and reporter for Risk & Compliance Journal. He worked previously as online editor at seafood industry news service Intrafish and as a reporter with Associated Press and Pacific Business News in Hawaii.

Write to Ben at ben.dipietro@wsj.com

KATE FAZZINI writes for WSJ Pro Cybersecurity. She has held roles in cybersecurity at Promontory Financial Group and JP Morgan Chase & Co., and is an adjunct professor of cybersecurity at the University of Maryland, teaching cybersecurity for business and government.

Write to Kate at kate.fazzini@wsj.com

ADAM JANOFSKY writes for WSJ Pro Cybersecurity, with a speciality in small business. He previously worked at Inc. magazine, Bloomberg News, and managed the WSJ's startup blog.

Write to Adam at adam.janofsky@wsj.com

JEFF STONE writes for WSJ Pro Cybersecurity. He previously covered privacy, international hacking groups, bug bounties, and a range of related topics at media outlets including the Christian Science Monitor and the International Business Times.

Write to Jeff at jeff.stone@wsj.com

Copyright © 2017 by Dow Jones & Company, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, and information storage and retrieval systems—without the express written permission of Dow Jones & Company, Inc. Contents are based on information from sources believed to be reliable, but accuracy and completeness cannot be guaranteed. Dow Jones & Company, Inc., its officers, employees, or agents may hold positions in any of the securities mentioned herein.

PHOTO CREDITS - p2: Africa Studio/Shutterstock.com; p4: saul loeb/Agence France-Presse/Getty Images; p5: stefano carniccio/Shutterstock.com; p6: Rena Schild/Shutterstock.com; p7: Tashatuvango/Shutterstock.com (flags); Scott Olson/Getty Images (President Donald Trump); p8: Rawpixel.com/Shutterstock.com (lineup), 4 Girls 1 Boy/Shutterstock.com (lineup background); p9: LeoWolfert/Shutterstock.com; p10: napocska/Shutterstock.com