SOLVING YOUR CYBERSECURITY TALENT SHORTAGE

By Mike Cobb

OCTOBER 2016 | US$25 | S051016

Channel Partners™

SOLVING YOUR CYBERSECURITY TALENT SHORTAGE

By Mike Cobb

OCTOBER 2016 | US$25 | S051016

Channel Partners™

TABLE OF CONTENTS

Channel Partners™

ABOUT THE AUTHOR

@thehairyitdog

MICHAEL COBB, CISSP-ISSAP, is 20-year veteran of IT security with a passion for making industry best practices easier to understand and implement. As an adviser on security controls and information handling practices to companies and government agencies large and small, Cobb has helped numerous organizations achieve ISO 27001 certification and successfully migrate data and services to the cloud. Cobb also has worked with CESG, the Information Security arm of Britain's Government Communications Headquarters agency, to promote security best practices in government. A renowned author and presenter, Cobb has written numerous technical articles and webcasts for leading IT publications as well as the book "IIS Security." He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS).

SOLVING YOUR CYBERSECURITY TALENT SHORTAGE

By Mike Cobb

THE CYBERSECURITY SKILLS GAP IS REAL. WHILE IT MAY BE DIFFICULT TO PROVE THAT HEADLINES LIKE "One Million Cybersecurity Job Openings in 2016" don't sensationalize the problem, there's no denying that cyberattackers are outpacing and outflanking your and your customers' defenses.

A major reason why we're losing the war: People trained and experienced in cybersecurity are rare and expensive.

In 2011, C-level executives didn't even rank cybersecurity as a top 10 risk, so there was little incentive for colleges and universities to develop programs to churn out defenders. Fast forward to 2016: Big data breaches and bigger regulatory fines have created a surge in demand for cybersecurity experts. Firms must compete with the likes of Amazon, Facebook and Microsoft as well as thousands of cool Silicon Valley startups flush with venture capital cash. Forget being able to hire top new talent — most shops are just trying to hold on to the security pros they already have.

A study of the international shortage in cybersecurity skills by the Center for Strategic and International Studies shows the extent of the problem. Fully 82 percent of respondents reported a shortage of cybersecurity skills, with 71 percent saying that this shortage causes direct and measurable damage. Hackers will definitely search out organizations they suspect of being short of cybersecurity skills; one in four respondents said insufficient cybersecurity staff has damaged their organization's reputation and led directly to the loss of proprietary data through cyberattack. It certainly makes it difficult for solution providers offering cloud-based services to expand while still maintaining security standards, and it's leaving businesses and government agencies vulnerable to organized cybercriminals, small-time hackers and attacks from various nation states.

So what's the answer?

Plenty of organizations hope that information security technology will plug the skills gap. More than half of respondents believe that, in five years, cybersecurity solutions will be able to meet the majority of their organizations' needs.

This is alarmingly optimistic thinking. Even if new technologies can turn the tide against cybercriminals, organizations still need people who understand when, where and how to deploy and manage these solutions. Cybercriminals, malware, application vulnerabilities and plain old human error are always going to be clear and present dangers. So, yes, improving security technologies will help mitigate some of these risks. But skilled people will always be needed to ensure the remaining weak spots are taken care of.

Data Security by the Numbers

A recent survey by Dataguise of 100 senior IT decision makers, including CxOs, VPs, directors and managers, showed some interesting trends:

73% report that data security concerns terminate or delay data-driven business initiatives

82% use network monitoring — no wonder some are afraid to make fuller use of data

47% are confident that sensitive data throughout the organization is safe

47% said the CEO or board of directors would be on the hook for unauthorized access to sensitive data versus 88% who say that the IT/security team would face scrutiny

Source: Dataguise

The message for most customers is that outsourcing cybersecurity functions is a more realistic approach than relying on some future killer technology. More than 60 percent of survey respondents work at organizations that already outsource at least some cybersecurity work, although in the United States this figure is only just over 50 percent.

For partners that want to provide security services to customers, the key is to be selective as to what you handle in-house. Lean on vendors for security functions that lend themselves to automation, like 24x7 threat detection and network monitoring. Specialized providers can deliver these better and more cost-effectively than you can.

Then decide on which strategic added services you want to focus.

Currently, the high-value security skills that are in really short supply are intrusion detection, secure software development and attack mitigation. While it will take time to bring even talented employees fully up to speed in these areas, the profit potential is such that any or all are worthwhile investments. Ongoing education for customer end users to reduce instances of ransomware is another hot offering.

BUY SOME, GROW SOME

It's certainly possible to hire security experts to spearhead these offerings now, given the fiscal will, and the supply will continue to increase. A 2014 report by RAND Corp. suggested that relying on market forces to fix the problem would mean at least a five-year lag. Educational institutions have taken note of the demand, and we're seeing more graduates.

Still, information security is a highly specialized and knowledge-intensive profession. While higher compensation will draw more people into the sector, it can't reduce the time it takes to train them to their full potential. Implement a program to grow your own experts, promoting from within. Someone with deep knowledge of a programming language or the ability to develop and deliver effective training is already halfway to becoming a secure software development or end-user security education specialist.

Educating employees is expensive, of course. Who makes a good security pro, and what skills do they need to serve your customer base? How do you identify people with the potential to become cybersecurity experts, and then get them up to speed?

One thing is certain: You must take a different approach from how you normally recruit or internally promote employees.

Most HR guidelines prefer candidates with degrees and various other must-have attributes, but this is too restrictive in the current climate and potentially prevents people with valuable KSAOs (Knowledge, Skill, Ability and Other) from being selected.

One key recommendation in the CSIS survey is that employers should rely less on a degree as evidence of suitable skills for entry-level positions. A good cybersecurity team needs a diverse mix of skills and personalities, and widening the range of potential candidates is an opportunity to create a more varied talent pool. There is currently a particular dearth of women and minorities in the cybersecurity industry; an (ISC)² study in 2013 of 14,000 professionals in cybersecurity revealed only 11 percent were women.

Bringing in people from different fields and backgrounds can challenge existing preconceptions and outdated processes and lead to innovative thinking in how to tackle recurrent security issues.

Ideally, recruits should show not just an interest in security but also a desire to make a real contribution to how your organization delivers security services. Does an employee really care about customer outcomes and have a good understanding of the business processes and drivers that make the customer's business succeed? An ability to grasp how technology and security together can drive the business forward is important.

Look for individuals with strong interpersonal abilities. In most surveys of what makes a good security expert, the single most important attribute is communication skills — ranked ahead of even a university degree, according to managers.

Another important competence is analytical skills, particularly when designing and developing new systems and services.

Remember, it's not just budding technical security expertise you're looking for. You need people who like looking at the big picture, a requirement for managing the suppliers, processes and technology involved in a fast-changing security landscape. Plenty of security vendors will supply people to tap away at keyboards and stare at banks of monitors.

Testing 1, 2, 3

There are plenty of free online courses and tests that can be used to prescreen employees and rate their security skills potential. FutureLearn offers a free **Introduction to Cyber Security** and the Open University provides a free **Network Security** course, while **Cybrary** provides a wide range of cybersecurity education.

Big gains can be made in any customer's security posture, without the need for highly trained experts, by focusing on behavior-based strategies to minimize human error — still one of the biggest factors behind data breaches. Training someone to be a security evangelist and deploying them to run Lunch & Learn sessions will raise the knowledge level of security procedures and good hygiene practices throughout the customer's workplace. A great place to start is the SANS Securing the Human training modules.

SPEED TRAINING

Once you've talent-spotted specific individuals, what is the best way to bring them to a level where they can play effective roles?

Although more universities are now offering cybersecurity courses, CSIS survey respondents rank hands-on experience and professional certifications as better ways to acquire cybersecurity skills than a degree. Development programs should therefore focus on practical training in the form of labs and certification courses. Hacking contests and capture-the-flag exercises certainly play a role in developing technical expertise as well.

There are plenty of bodies offering certifications in different aspects of information security — think ISACA, (ISC)² and GIAC — as well as industry-specific qualifications and supplier-specific programs. Look for those courses that provide the skills your organization is short of, and work with those employees committed to developing their security skills to help them fit in the necessary study time to achieve certification.

MVP Security Certs

Foote Partners LLC recently reported on the skills that brought the biggest gains in value since the beginning of 2016 — we're talking pay increases of 18 to 50 percent. Among the top 10, six (noted in yellow) are security-related:

- **GIAC Enterprise Defender (GCED)**
- **GIAC Certified Firewall Analyst (GCFW)**
- **EC-Council Certified Security Analyst (ECSA)**
- **Linux Professional Institute Certification (LPIC-Level 3)**
- **EC-Council Computer Hacking Forensic Investigator (CHFI)**
- **CompTIA Server+**
- **Microsoft Certified Professional Developer (all)**
- **PMI Program Management Professional (PgMP)**
- **Certified Cyber Forensics Professional (CCFP)**
- **Certified Forensics Computer Examiner (CFCE)**

Source: Foote Partners LLC S051016

Note that there are dozens of computer security certifications, ranging from general to very specialized. Due to the constantly evolving nature of cybersecurity, look for certs that require members to regularly update their knowledge and skills. Providing continued learning is not only vital to stay abreast of the latest attack techniques and security technologies, it can you help retain your homegrown talent. The 2015 (ISC)² Global Information Security Workforce Study by Frost & Sullivan found that an absence of training is often a significant factor in people's decisions to seek alternative employment; paying for professional security certification expenses was considered more effective at retaining staff than improved compensation packages. In addition:

Spread the knowledge: Partners, who often have experience monitoring their workforces for the certifications required by various vendors, know how critical it is to ensure customer offerings are not reliant on one or a few employees. Rotating daily tasks not only makes jobs more interesting but creates a wider knowledge base within the security team.

Lean on vendor partners: Most commercial security solution vendors provide comprehensive programs that give in-depth training on how to configure, deploy, maintain and use their products. Take advantage of these to keep a range of employees abreast of the latest features and updates to the products used within your own network.

Invest in threat intel: Effective security requires not only a knowledge of hardware, software, networks and applications, but also an understanding of the threats and vulnerabilities a specific customer faces and what cyberattacks are prevalent. Investing in services to keep employees up to speed in these areas will produce a security team with an in-depth understanding of the infrastructure and business processes they are protecting — an ideal scenario.

How Dire Is the Situation?

Various industry experts and education advocacy groups have for some time predicted a shortage of trained IT security pros, warning that it will put online systems and services at risk.

On the face of it, these concerns seem valid. The U.S. Bureau of Labor Statistics estimates that 1.24 million security-related jobs will need to be filled by 2020. However, the problem may be more about finding or retaining qualified individuals at what are considered "reasonable" salaries, rather than a shortage of actual candidates.

For example, in the U.K., more students have begun computer science courses than physics, chemistry and mathematics combined in each of the last six years. However, of undergraduates who qualify across all higher education subjects, computer science has consistently had the highest rate of unemployed graduates. Despite supposedly unprecedented industry demand for their skills, some 13 percent of computer science students are still unemployed six months after graduating.

The raw talent is out there. Partners should take advantage of their unique ability to expose employees to a variety of companies and technologies. In addition, in 5 Ways to Crack the Skills Ceiling, channel experts offered 10 tips on hiring and retention.

5 Pro Tips: Hiring

■ **Don't dawdle or go on a unicorn hunt.** Consider accelerating the hiring process to avoid losing top candidates.

■ **Don't get hung up on paper.** Someone with general technical acumen, a willingness to learn and a great personality is often a better bet than someone with a string of certifications.

■ **Do concentrate on soft skills.** Before hiring, ensure potential employees can present on and document their work and that you'd feel comfortable with them talking to a customer's CEO.

■ **Don't lowball.** Before beginning to interview, research going rates in your area.

■ **Consider agencies along with master agent and distributor partners.** The keys are selecting an agency partner with knowledge of your industry sector and geography and then letting it be proactive.

5 Pro Tips: Retention

■ **Set a policy on training and counteroffers.** How much will you invest in training and retraining staff? Is tuition reimbursement open, or will you pay only for courses relevant to the employee's current role? Will you counteroffer to keep a top employee?

■ **Be creative with incentives.** It's not all about the money, especially for millennials and older workers looking to scale back.

■ **Be transparent on compensation.** PayScale recommends issuing total compensation statements that show employees exactly how much the company spent on health and wellness benefits, retirement savings, educational costs and any other benefits on top of regular salaries and commissions.

■ **Spend on employee education beyond just certifications.** Succession planning is important as well, so employees can visualize a career ladder, not just a path.

■ **Specialization may allow you to charge customers a premium, and pay accordingly.** In a complex world, expertise is currency.

CAN MACHINE LEARNING SAVE US FROM CYBERCRIMINALS?

By Mike Cobb

ALMOST NINE OUT OF 10 RESPONDENTS IN A RECENT CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES SURVEY SAID THAT CYBERSECURITY TECHNOLOGY could help compensate for skill shortages, with just over half believing that, in five years, cybersecurity solutions will be able to meet the majority of their needs.

That's a lot of optimism, and potential sales.

To cash in, most vendors are pinning their hopes on big data analytics, machine learning and artificial intelligence to give their products the edge over cybercriminals. These features are being added to many top-end security solutions, and are being heavily marketed by vendors as an effective strategy to reduce the time it takes to detect and respond to cyberattacks, thanks to automated detection and remediation.

The problem: Experience tells us that attackers adapt their tactics whenever new security controls are introduced. Can these technologies really change the threat landscape, alleviate the cybersecurity skills gap and win the war against cybercriminals?

Traditional security solutions rely on signatures, rules, filters and blacklists to stop malware and attackers from taking over a network. This approach is effective at detecting known malicious code and activities but is increasingly ineffective against modern attacks. Advanced analytics and neural networks have been used by banks to detect fraud for more than 20 years, and this form of analysis has recently been harnessed to protect enterprise computer networks and data.

Even so, more advanced detection techniques are needed, and data security requires more than algorithms that can check byte and packet counts to spot if someone is suddenly working outside of office hours.

Machine learning — giving computers the ability to learn without being explicitly programmed — is viewed by many as the most efficient and effective way to detect attacks and risky behavior, and overcome the limitations of older security information and event-management products. Automated and iterative algorithms allow a program to probe data for obscure structures and use predictive analytics to recognize potential threats that would go unnoticed using human analysis alone.

The amount of data and events generated by security systems today is beyond the capacity of human experts to parse, but machine learning systems can actually benefit from very large volumes of data — with an important caveat.

Security solutions that incorporate machine learning still have various places where improvement is needed and, surprisingly, one is the same problem faced by human analysts: the sheer amount of data, particularly unstructured and hybrid data sets. Even small networks generate millions of logged events every day that need to be stored and analyzed. Many attacks are carried out over several months through discrete steps, often concealed in the guise of legitimate requests and commands. This means analysis has to reach back over huge amounts of historical data to find and correlate attack-related events. Analyzing this amount of data for prolonged periods of time can introduce performance issues unless only a small set of attributes is examined. Attackers understand this and can adopt their tactics to slip through the analysis and findings.

Another problem is that to determine if there is a suspicious deviation in network usage, the system needs a clean baseline, and the current hypothesis is that most networks are already compromised. Even baselining a "clean" network is no easy matter. Network traffic is constantly changing and evolving, making it difficult to gauge whether activity is normal or malicious.

The main argument so far against security solutions powered by unsupervised machine learning, though, is that they spit out too many false positives, resulting in alert fatigue and missed critical events.

These difficulties make relying entirely on new security technologies like big data analytics, machine learning and artificial intelligence to spot and prioritize complex attacks impractical. But human analysis-based solutions clearly can't keep up with the huge volume of data that needs to be analyzed. What's the answer?

HYBRID TIME

Reducing the high rates of undetected attacks and delayed responses demands a combination of human effort supported by machine learning to automate the process of recognizing patterns hidden in increasingly large and complex datasets.

MIT's Computer Science and Artificial Intelligence Lab (CSAIL) is developing a system called AI2, a cybersecurity platform that combines machine learning and the experience of security experts to continually improve its ability to find real breaches while reducing false positives. AI2 works by analyzing security logs and flagging anything it "thinks" is suspicious. This filtered data is passed on for human analysis, with legitimate threats generating feedback to AI2.

This approach is proving to greatly improve detection rates and reduce false positives compared with unsupervised anomaly detectors.

For full visibility into emerging threats, we can't rely just on data gathered from endpoints and network traffic, either. A lot of clues and pointers exist in unstructured data like social media posts, news stories and research reports. To capture that, IBM is looking to use the natural language processing capabilities of its artificial intelligence platform Watson to hunt through and learn from unstructured data to identify new threats.

Hopefully these types of projects will lead to improved attack-detection techniques and security solutions. However, no security technology can stop all cyberattacks. Malicious hackers will continue to use social engineering to circumvent even the most advanced analytic security systems, just as they have circumvented fraud systems in the banking world. However, advances in machine learning and its application to information security should decrease the time to detection, which at the moment is woefully slow.

We need to do something, and soon. The growth of the Internet of Things is creating more data, more attack vectors and more attacks. Security teams already can't cope, so machine learning technology will play an important role in not only reducing workloads but providing better-quality information from which to prioritize activities.

Machine learning systems certainly won't replace humans, but they will make people far more efficient, and make life harder for the enemy.