

<http://www.darkreading.com/threat-intelligence/curbing-the-cybersecurity-workforce-shortage-with-ai/a/d-id/1329617?>

8/18/2017

10:00 AM



Deborah Golden

Curbing the Cybersecurity Workforce Shortage with AI

By using cognitive technologies, an organization can address the talent shortage by getting more productivity from current employees and improving processes.

It may seem counterintuitive, but close to 0% unemployment in an industry is not a good thing. Little to no unemployment means there aren't enough cybersecurity professionals to fill open positions; there's a high demand for existing talent, resulting in salary inflation and high turnover; and hiring of underqualified workers is more likely. But this is the situation for cybersecurity, and it's unlikely to get better soon — more than 1.5 million job openings are anticipated globally by 2019.

No matter how hard organizations try, they won't be able to hire enough college graduates, recruit enough skilled professionals, or reskill enough of the existing workforce to reduce, let alone erase, the shortage. But there is another way: cognitive computing — systems that learn, think, and interact with humans. By using cognitive technologies such as artificial intelligence, machine learning, advanced analytic techniques, and automation, an organization can address the cyber workforce shortage by getting more productivity from the existing employees and optimizing the supporting processes.

The premise is simple: cognitive computing allows an organization to make better use of the time and skills of its cybersecurity talent and improve security in the process. Instead of having the workforce spend the bulk of its time reacting to potential threats or on mundane administrative tasks, it can now focus on proactive security and complex investigations.

For example, cognitive technologies can help address the workforce shortage by improving the organization's workflow. One leading investment firm noted that by

automating routine activities, tasks that used to take cyber professionals about 40 minutes were now accomplished in 40 seconds, and analysts' productivity tripled. That's the value of automation — not spending too much time on mundane tasks, when time and talent is already in short supply.

In addition to saving time, it saves money. A [recent study](#) found that organizations spend about 21,000 hours investigating false or erroneous security alerts at an average cost of \$1.3 million annually. These alerts could be handled by cognitive systems, which would only notify cybersecurity personnel when more investigation is warranted.

But automation is just the beginning. One of the more powerful newer applications is the use of advanced analytics. This technique uses supercomputer processing power to sift through large sets of data to identify behavioral patterns, malicious code, and network anomalies that may not be readily apparent. This can help cyber professionals predict where threats are most likely to occur and then prevent them before they do.

Consider the [case](#) of a large cable and Internet service provider that was receiving more than 500,000 network security alerts every day. It implemented a behavioral analytics application that allowed analysts to baseline network activity, identify and correlate security alerts to isolate the most threatening, and refine security thresholds. The results: six months later, the provider saw a 99.8% reduction in alerts and its cyber professionals were now spending their time investigating the highest-priority alerts that required human ingenuity to solve.

How It's Used

The applications for behavioral analytics are endless. Banks can use this technique to identify suspicious online account activity that deviates from an individual user's typical profile, thereby stopping theft, fraud, or further network penetration before it begins in earnest. Cybersecurity firms can use it to detect a new virus or unknown attacks and stop the malicious behavior before damage happens, permitting responses at machine-speed.

The use of analytics is one of cognitive technologies' greatest advantages for cybersecurity in that it allows organizations to take a proactive approach. The ability to wade through massive amounts of network traffic to quickly identify irregular behaviors is an enormous security advantage. Being able to predict where threats are most likely to occur, and then prevent them before they do, can change fundamentally change security.

Another way cognitive technology addresses the cybersecurity workforce shortage is by helping to reduce employee turnover, which can occur when employees feel unsatisfied with the work. A typical workday filled with uninspiring tasks or activities that aren't challenging can prompt employees to seek professional fulfillment

elsewhere. According to a [report](#) by the Society of Human Resource Management, 48% of employees reported that the work itself was very important to job satisfaction.

Naturally, there are concerns that cognitive computing means that the "robots are taking over" or that the efficiency of cognitive technologies may be so advantageous that humans may be out of work. But this fear is overblown. When grocery stores brought in self-checkout kiosks, cashiers feared they'd no longer be needed. The advent and widespread adoption of ATMs caused many to believe that bank tellers were on the brink of becoming passé. But the number of [grocery store cashiers and bank tellers actually grew](#) over time. In cybersecurity, there remains a place and an overwhelming need for human interaction and ingenuity that a machine cannot fulfill.

The key is to not compete against the machine but to compete with it. Cognitive technologies can manage rote security tasks, predict malicious attacks, and help retain employees. These capabilities allow companies to address workforce shortfalls by reassigning existing personnel without needing to rely solely on hiring new and experienced talent, while also improving processes and adding rigor to decision making.

But they can't do everything. When these insights are combined with an organization's knowledge of its own network, cybersecurity professionals can identify the network's weak points, characterize the type of attacks the network is susceptible to, and prioritize addressing the pertinent vulnerabilities. In this way, human-machine teaming can produce better outcomes in less time.

http://www.darkreading.com/author-bio.asp?author_id=4803

Profile of Deborah Golden

Principal, Deloitte & Touche, and Federal Cyber-Risk

LeaderNews & Commentary Posts: 1

Deborah Golden is a principal in Deloitte & Touche LLP's Advisory practice, with over 20 years of information technology, security, and privacy experience encompassing various industries, with a specialization in Cyber-Risk Services, as well as within the Federal, Life Sciences & Health Care, and Financial Services industries.