Alexander Hughes
EXECUTIVE SEARCH CONSULTANTS

# Companies need talent to beef up cybersecurity

## With malware attacks on the rise, companies must be creative to recruit, train and retain cybersecurity experts because they are in short supply

**By Michael NEUMANN Managing Partner of Alexander Hughes Germany**
**And Benoît CEILLIER Client Partner at Alexander Hughes Paris**

In May and June, hackers crippled companies around the world with ransomeware known as WannaCry and then Petya.

The malicious software, or malware, blocked access to data until a ransom was paid to the cyber-criminal. It affected companies from UK chocolate giant Cadbury to Danish shipping giant Maersk and Russian oil producer Rosneft, and it temporarily shut down banks, the airport and metro system in Kiev, Ukraine.

The attacks must be a wake-up call for corporate leadership and their recruiting strategies. Companies need more cybersecurity professionals to protect their data – and customer information – because the attacks are going to become more frequent and increasingly costly.

Juniper Research, a UK market research firm, forecasts that criminal data breaches will cost businesses $8 trillion over the next five years.

Companies are taking steps to ward off the attacks. Cybersecurity spending is poised to surpass $100 billion in 2020, a compound annual growth rate of 8.7% from an estimated $81.7 billion in 2017, according to International Data Corporation, a U.S. research firm.

But will they find the experts to protect their crucial data as cyber criminals become more aggressive and organized?

### Talent Shortage

It won't be easy to build a security team. This is for two reasons. The first is that there's already a deficit of such talent – and it's expected to reach 1.8 million positions by 2022, according to the International Information System Security Certification Consortium, or (ISC)2, a U.S. non-profit organization.

To fill these positions, Millennials will be critical. They've grown up in the era of the internet, mobile phones and social media. This has made them more agile than previous generations in their capacity to quickly acquire and process knowledge and skills, and to innovate and adapt to changes.

But it's a hard generation to pin down. "Millennial workers are more likely to change employers than other generations," not out of low job satisfaction but the lure of better perks, (ISC)2's report found.

## Deficient Education

The second reason for the difficulty in finding cybersecurity professionals is that the traditional education system is not doing enough to supply them, according a report by the U.S. nonprofit Center for Strategic & International Studies (CSIS) and Intel Security, a U.S. tech company. Only 23% of those surveyed for the report said education programs are preparing students to enter the industry. This is critical. Without sufficient and skilled cybersecurity workers, companies are "more desirable hacking targets," according to a third of those surveyed for the report.

CSIS also found that companies are coming to understand how important it is to train their cybersecurity team with hands-on experience and professional certifications. In the survey, 97% said their boards now view cybersecurity as a major concern, when it didn't register in the top 10 of prioritized risks only five years ago.

To undercover the talents of their generation in the field of programming and to do so, on a broad scale, Xavier Niel with several partners including Nicolas Sadirac founded 42, an innovative computer programming private school. Training on the two official campuses - Paris, France and Fremont, California- is free, open and accessible to all.
This forward-looking approach to the talent shortage remains one of the most daring response to the challenge of information technology skill development, as well as a source of innovation for the future.

## Continuous Training

To equip cybersecurity teams, continuous, on-the-job training is a must so that workers can gain experience and skills as fast as – or faster than – cyber criminals. The top skills include attack mitigation, intrusion detection and the ability to develop secure software.

To build these skills, companies can put their workers through certification programs and community college courses, and arrange mentorships. They can also hold hacking competitions for developing the talents to spot and defend vulnerabilities in a computer system.

As important are curiosity and analytical and critical thinking, as these help cybersecurity teams to react and work quickly when an attack happens, no matter the professional qualifications.

Indeed, on the day of the WannaCry attack, Marcus Hutchins, a 22-year-old web security researcher, not a corporate professional, found out how to halt the spread of the ransomeware – all rather by accident while working out of his room at his parent's house in England.

Such young people should be brought into the fold to teach the cybersecurity staff – and the entire workforce – because they tend to be at the forefront of what's going on in the fast-changing world of hacking, more so than senior executives and teachers.

## Widening the Search

The CSIS survey suggests that hiring people who have hacked before can be beneficial for beefing up security, and the stigma against them should be relaxed. Another way to find more security workers is to widen the search beyond the traditional career fairs at universities, and to hire more foreigners, minorities and women.

IBM, a U.S.-based technology company, is taking a fresh approach to filling cybersecurity positions. It's mining its own ranks and other lines of business for candidates. Marc van Zadelhoff, IBM's general manager of security, calls these "new collar" jobs, and says that the best workers to fill them may not be the IT college graduates but people who are curious, ethical, motivated to learn and keenly interested in solving problems and understanding risks.

"Businesses should open themselves up to applicants whose nontraditional backgrounds mean they could bring new ideas to the position and the challenge of improving cybersecurity," said Van Zadelhoff.

These recruits, whether from the entertainment, law or retail industries, can pick up the cybersecurity skills on the job, he said.

## A Talent Pipeline

Companies, too, should team up with high schools and colleges to develop apprenticeships and training programs to create a talent pipeline. This will make it possible to keep the "cybersecurity team staffed into the future," Van Zadelhoff said.

Senior leadership must also understand that cybersecurity is every executive's job. That's the exhortation of Bill Sweeney, chief technology officer for the Americas at BAE Systems, a London-based aerospace, defense and security company.

"Executives need to personally know how strong their company's cyber defenses are, as well as the expected responses for attacks or breaches," he said.
To improve these defenses, he called on executives to work closer with their chief information security officers, or CISOs, by making them a part of the top leadership team. That will make it easier for them to warn C-suite executives of any weakness in a company's software and what can be done to reduce the threat of a cyber-attack.

"The CISO should be included on new business initiatives early on so that security is baked in rather than bolted on afterward," Sweeney wrote.

These strategies will keep companies to keep ahead of the curve – and not always trying to catch up after cyber criminals have found the next vulnerability to exploit. Companies must invest today in recruiting and training a cybersecurity team to defend assets against tomorrow's attacks.

***Follow Alexander Hughes on LinkedIn!***

More about us: www.alexanderhughes.com
Media contact: Valeria Brancato – v.brancato@alexanderhughes.com
Réjane Campisi-Barea - r.campisi@alexanderhughes.com