Beat the security talent shortage: How analytics can upskill your team

As businesses confront a vast, global cybersecurity talent shortage, what can organizations do to rapidly upskill their workforce?

Cybercrime is never far from the headlines. Whether it's a major company being hacked or another security threat striking fear into the hearts of IT professionals everywhere, criminals are taking advantage of inadequate defenses among global businesses.

In fact, 2018 saw several breaches that caused international disruption, including those at Under Armour's MyFitnessPal app, Ticketmaster UK and social media giant, Facebook.

Yet globally, there is a distinct lack of IT professionals available to strike back, with the shortfall in the cybersecurity workforce estimated at just under three million globally.[1] It's a figure that exposes the skills gap at the heart of the mayhem. An ESG survey suggests that 51% of organizations [2] have a 'problematic' shortage of cybersecurity skills, while the lack of personnel has become the top job concern for cybersecurity professionals.[3]

"We're seeing more sophisticated attacks, even at the basic level," says Ian Glover, president of the Council for Registered Ethical Security Testers (CREST). "We need to keep our cyber hygiene standards up to date to make sure they replicate the current threat environment."

"51% of organizations have a 'problematic' shortage of cybersecurity skills."

- ESG Research 2018 [2]

Fighting back against cybercrime

Cybercrime is estimated to have cost as much as $608 billion globally in 2017 [4], according to research from the Center for Strategic and International Studies (CSIS). Predictions for the future are even more stark, with researcher and publisher Cybersecurity Ventures estimating that cybercrime damages will cost the world $6 trillion a year by 2021. [5]

"Cybercrime damages will cost $6 trillion a year globally by 2021."

- Herjavec Group 2017 Cybercrime Report [5]

There are many reasons for the escalation, ranging from difficulties in making prosecutions to the rise in 'cybercrime as a service' – where criminals run lucrative businesses by marketing their abilities and allowing customers to easily (and cheaply) acquire the tools of this particularly dark trade.

Challenges associated with the proliferation of devices and operating systems entering the workplace, and the corresponding hike in entry points for potential security breaches, only makes the headache worse for security staff.

IT centralization is one way to tackle this challenge. With better cloud management and data visualization through analytics, it's far easier to see what's going on in a business. This increased visibility can help identify weaknesses, isolate breaches as they occur and deliver clear intelligence on the risks of any outdated technologies and processes.

Building the right security skills

Awareness of what's happening across the organization is an essential part of strengthening defenses. Yet improved insight through analytical tools is only part of the solution because – as always – people are key.

Verizon's 2018 Data Breach Investigations Report [6] – exploring over 53,000 security incidents around the globe – revealed that a quarter of cyberattacks were committed by insiders. And 17% of these were caused by human error, which included sending an email to the wrong person and misconfiguring web servers. The report also found that 4% of employees are falling for phishing campaigns.

A recent survey by PwC found similar results, revealing that internal actors were a third more likely than external parties to be the perpetrators of the most disruptive frauds. Despite this, the survey also found that a decreasing number of organizations have a formal business ethics and compliance programme in place, dropping from 82% to 77% in the last two years.[7]

"We need to change cybersecurity training programs into cultural change programs," says Glover. "We need to work with a wider audience, and you need cultural change to make people more aware."

"17% of internal cyberattacks were caused by human error over the previous 12 months."

- Verison 2018 [6]

Work is also being done in education to close the skills gap, but James Hadley, founder and CEO of Immersive Labs, says more effort is needed to promote the variety of roles available.

"Most developed countries are spearheading a number of initiatives to increase the amount of people that see cybersecurity as a career, starting with children in school," he says. "It's not just about hacking, but because the industry is often depicted in this way it's difficult to get new people into the field, especially women. More needs to be done to remove the gender imbalance."

"If an individual has attributes – such as analytical thinking, problem solving, trouble shooting and perseverance – they're likely to excel in cybersecurity."

- James Hadley, founder and CEO of Immersive Labs

Developing expertise within the business

However, building a pipeline of new talent takes time, and with such an immediate threat to contend with, businesses are looking for alternative solutions to help build resistance without the need to hire specialists.

Upskilling an existing workforce is one clear way to help fill the void. As Hadley explains, organizations have a real opportunity to transition their people into cybersecurity roles.

Interestingly, he says that a person's academic background has little influence on their potential.

"It's qualities and attributes such as analytical thinking, problem solving, trouble shooting and perseverance," Hadley says. "If an individual has those attributes, they're likely to excel in cybersecurity."

As more centralized data-driven tools emerge to provide a truly holistic view of the business, more control is placed in the hands of employees to interpret and act upon the results. It all starts with having the ability to spot breaches early which helps organizations take security to the next level.

"The monitoring that comes with TechPulse helps IT employees take a variety of proactive actions to reduce cybersecurity threats to their business. In turn, these IT pros can develop and mature new analytics skills of their own."

How HP DaaS can help upskill your workforce

Having a clear understanding of the health and usage of mobile devices, desktops and workstations – whether company-wide or on an individual basis – can improve the likelihood of making crucial decisions in areas such as security compliance and data protection. Managed solutions such as HP Device as a Service (DaaS) can help with this.

The HP offering is unique in that it provides predictive analytics and insights with HP TechPulse – powered by company-specific data and HP's broader expertise in the latest cybersecurity threats. This kind of monitoring – and the dashboards that come with it – helps employees take a variety of proactive actions to reduce threats to the business. In turn, this can help individuals develop, mature and develop new skills.

HP DaaS Proactive Security shares detailed findings on attempted and blocked attacks to enhance security intelligence, giving employees the information to better respond to threats. The one-stop dashboard function adds visibility for insights across the entire device environment, including cybersecurity, which can build a greater understanding of analytics among IT teams.

Whether spotting vulnerable devices, automatically installing the latest patches across the suite, or identifying risk implications in the way devices are being used, security employees can analyze their infrastructure on an individual and overarching basis and use that data to put themselves back in control.

Discover HP DaaS

Other useful links:

Blog:
Technology

HP Device as a Service

1. ISC2, Cybersecurity professionals focus on developing new skills as workforce gap widens, 2018

2. ESG, ESG Research Suggests Cybersecurity Skills Shortage Is Getting Worse, Jan 2018

3. ISC2, Cybersecurity professionals focus on developing new skills as workforce gap widens, 2018

4. Center for Strategic and International Studies (CSIS), Economic Impact of Cybercrime, Jan 2018

5. Herjavec Group, 2017 Cybercrime Report, Oct 2017

6. Verizon, 2018 Data Breach Investigations Report, 2018

7. PwC, Pulling fraud out the shadows: Global economic crime and fraud survey, 2018

4AA7-3855ENW, February 2019