BEAT THE CYBERSECURITY TALENT SHORTAGE:

HOW TO USE UPSKILLING AND ANALYTICS TO BOLSTER YOUR TEAM'S CYBERSECURITY CAPABILITIES

BUSINESSES ARE CONFRONTING A GLOBAL IT TALENT SHORTAGE. WHAT CAN YOU DO TO GET YOUR WORKFORCE UP-TO-SPEED?

85%

OF ORGANIZATIONS REPORT A SHORTAGE OF CYBERSECURITY SKILLS[2]

Cybercrime is never far from the headlines. It seems as though every few months, another security threat creates costly headaches for IT professionals everywhere.

And those threats don't come cheap, at least for the victims. The average cost of a breach is $8.7 million in the US and $3.86 million globally. Add in the many remote endpoints involved in today's hybrid-work environment, and costs swell even higher.[1]

The losses aren't just in the form of missed revenue from system downtime; they also include other, hard-to-quantify effects, such as increased customer turnover and the cost of working harder to acquire new business after suffering a damaged company reputation.[1]

If security breaches are a problem, the obvious answer is to hire more specialists to protect the organization. However, one of the greatest barriers to effective endpoint defense is a lack of skilled IT security personnel.[2]

In part, that is a market problem. There's a distinct shortfall of cybersecurity professionals, lacking just over 3 million workers globally.[3] However, despite increasing attacks and 85% of organizations reporting a shortage of cybersecurity skills,[2] they are actually hiring fewer cybersecurity pros.[3] You may want to hire more cybersecurity staff—but you can't find experts you can afford.

CYBERTHREATS ARE GROWING

102 MILLION

NEW MALWARE THREATS EACH MONTH[4]

60%

# OF ORGANIZATIONS HIT BY ATTACKS SPREADING FROM 1:MANY EMPLOYEES[5]

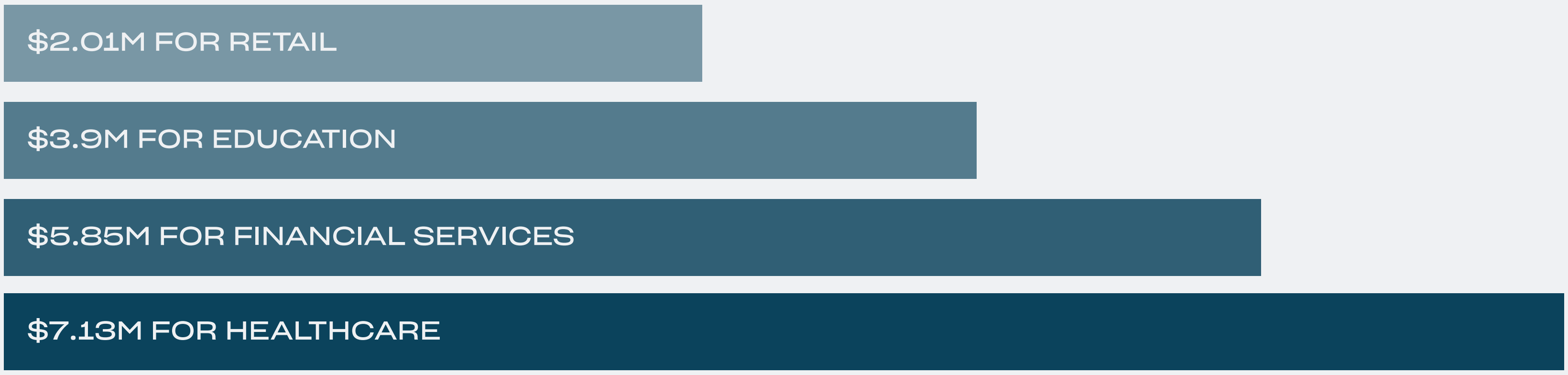
+58%

PHISHING ATTACKS OVER THE LAST YEAR[5]

+63%

PHISHING CAMPAIGNS AND FAKE SOCIAL MEDIA POSTS RELATED TO COVID-19[6]

AVERAGE COST OF A DATA BREACH:[1]



WHY IT'S HARD TO BUILD A CYBERSECURITY TALENT POOL

Cybersecurity skills are specialized, and not every computer science program devotes dedicated attention to imparting that knowledge. While IT education providers are working to close the cybersecurity skills gap, building a pipeline of new talent takes time. Cybercrime Magazine reports that in the US, only 3% of bachelor's degree graduates have cybersecurity-related skills.[7]

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 number of people that see cybersecurity as a career, starting with children in school," Hadley 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."

In the meantime, here are some practical options for organizations that know they need cybersecurity experts.

MINE YOUR EXISTING TALENT

IT'S QUALITIES AND ATTRIBUTES SUCH AS ANALYTICAL THINKING, PROBLEM-SOLVING, TROUBLESHOOTING, AND PERSEVERANCE THAT MATTER.

Don't overlook a natural source of talent: existing employees who can be strategically trained in hard-to-find skill sets such as cybersecurity. Look at the hidden potential of existing staff, then upskill them for new responsibilities.

Organizations have a real opportunity to transition their people into cybersecurity roles, if they know where to look for talent. Hadley points out that academic background has little influence on an individual's potential. "It's qualities and attributes such as analytical thinking, problem-solving, troubleshooting, and perseverance that matter," he explains. "If an individual has those attributes, they're likely to excel in cybersecurity."

There are other advantages. Retraining personnel can fine-tune the instruction to the company's particular needs. Employer-paid training also builds loyalty.[8] It engages employees who aim to bolster their credentials, add new skills to their résumés, and improve potential earning power.

DEPLOY AUTOMATION AND ANALYTICS

Another way to empower existing IT teams—even those with less security-specific expertise—to fight cyberattacks is with comprehensive, always-on technology solutions. Let automation do what it's good at, and permit humans to focus attention where it matters.

Organizations that have deployed artificial intelligence, machine learning, and analytics in their security strategy experience far lower losses than those who have not yet deployed these technologies. The average cost of a breach at organizations with fully deployed security automation was $2.45 million, compared to $6.03 million at organizations with no security automation.[1] It's no wonder that up to 43% of organizations say they prefer these more advanced IT security solutions.[2]

Solutions that use centralized, cloud-based management let IT teams see and control what's going on with device security, from the basics to more advanced metrics. Pairing always-vigilant protections with better data visualization through analytics makes it far easier for them to identify weaknesses, contain breaches, and get clear intelligence on the risks of outdated hardware and patches.

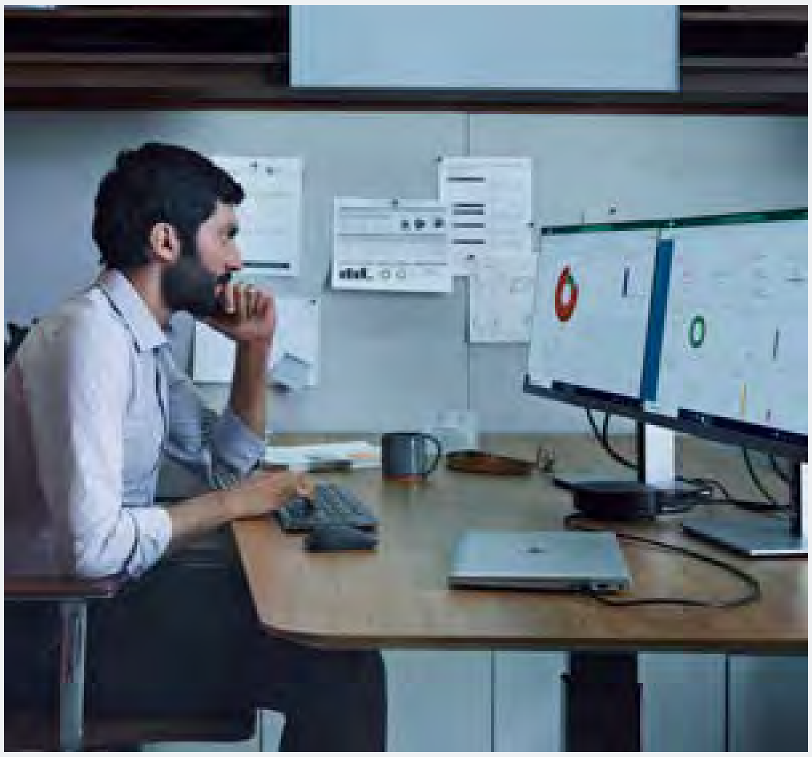
HP TECHPULSE[9] HELPS I.T. PROS DEVELOP AND MATURE NEW SKILLS OF THEIR OWN

CLOSE YOUR CYBERSECURITY SKILLS GAP WITH THE WORLD'S MOST ADVANCED ENDPOINT SECURITY SERVICE[10]

Now you can defend endpoint devices and develop IT skill sets at the same time. HP Wolf Pro Security Service[11,12] provides small and medium businesses with enterprise-grade protection—no in-house security expertise required.

GET COMPREHENSIVE, WORRY-FREE ENDPOINT SECURITY MANAGEMENT:

- Reinforced layers of government-grade protection and advanced, AI-based antivirus capabilities go beyond traditional tools,[13,14] so your company data, credentials, and devices stay safe.
- Timely, actionable insights on the entire device environment, including attempted attacks and potential threats, through a single cloud-based dashboard.
- Cybersecurity expertise[15] delivered as-a-service, so your in-house IT teams can develop and mature new skills.



DON'T LET A SKILLS GAP BECOME A BREACH POINT.

Learn more about HP Wolf Pro Security Service

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to the Customer at the time of purchase. The Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with an HP product.

[1] 15th Annual 2020 Cost of a Data Breach Study: Global Overview from IBM Security and Ponemon Institute, July 2020

[2] CyberEdge 2020 Cyberthreat Defense Report, March 2020

[3] (ISC)² Cybersecurity Workforce Study, April 28, 2019

[4] AV-Test SECURITY REPORT 2019/2020, August 26, 2020

[5] Mimecast The State of Email Security 2020, June 2020

[6] The Impact of the COVID-19 Pandemic on Cybersecurity, ISSA, July 30, 2020

[7] https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/

[8] https://applied.economist.com/articles/a-route-map-for-retraining-workers

[9] HP TechPulse is a telemetry and analytics platform that provides critical data around devices and applications and is not sold as a standalone service. HP TechPulse follows stringent GDPR privacy regulations and is ISO27001, ISO27701, ISO27017 and SOC2 Type2 certified for Information Security. Internet access with connection to TechPulse portal is required. For full system requirements, please visit .com/requirements.

[10] Based on HP's internal analysis of isolation backed, deep learning endpoint security services including SaaS and managed services. Most advanced based on application isolation and deep learning endpoint protection on Windows 10 PCs as of July 2020.

[11] HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

[12] HP Wolf Pro Security Service is sold separately. For full system requirements, please visit http://www.hpdaas.com/requirements. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

[13] HP Sure Click is available on select HP PCs and requires Windows 10. See https://bit.ly/2PrLT6A_SureClick for complete details.

[14] HP Sure Sense is available on select HP PCs and is not available with Windows10 Home.

[15] Security Experts available in the Proactive Security Enhanced plan only.

4AA7-3855ENW, Rev 1, April 2021