ALERT LOGIC™

WHITEPAPER

Six Practical Approaches to Bridge the Cybersecurity Talent Shortage

Monitoring for Suspicious Activity and Emerging Threats 24/7 for Better Cybersecurity

Ask a sampling of business leaders about their chief concerns and one particular subject is likely to rise to the top: cybersecurity. In fact, over 74% of organizations voted data security as their top IT priority in 2020.[1]

As the number of security breaches increases each year, so too does the financial impact. Studies have shown that the total cost of cybercrime is rising 12% year over year (an increase of 72% in the last five years).[2]

Cyberattacks and data fraud/theft are **2 of the top 5 risks** CEOs are most likely to face.[4]

In the face of such daunting business risks, many organizations are investing in security technologies to stay ahead of cybercriminals. According to a forecast from IDC, worldwide spending on security-related software would reach US $38 billion in 2019.[3] Yet, a major issue stands in their way: the worldwide cybersecurity talent shortage.

Realistically, the notion of a skilled talent shortage is nothing new

Pundits have been talking about it at least as far back as the early 2000s, when an article in Computer World recommended that companies seek out IT staff who demonstrate a unique combination of technical acumen and softer skills, "including a positive attitude, diplomacy, patience, attention to detail, tenacious abstract problem-solving ability and a strong will."[5] Mind you, this was back when Information Security was a less-than $5-billion-a-year business and security talent and skills shortages were lumped in with ever-present IT shortages.

But the talent shortage we're experiencing today is different

While businesses have never been more dependent on digital tools, services and systems for growth, many executives report that their organizations are adopting new and emerging technologies faster than they can address related security issues.[6] This exposes their data and systems to greater threat of cyberattacks, which are happening with increased frequency and are made all the more serious because criminals are targeting end users with phishing, ransom and malware attacks and other breaches[7] that can lurk for months before discovery. In addition, the accelerated pace of digital transformation, which is seeing organizations increasingly adopting "cloud-first" strategies, has led to a wider

attack surface that's ripe for infiltration by industrious cybercriminals. The situation is further exacerbated by the industry's skills and resources gap, with more than 4 million positions open around the world[8] and too few academic institutions and professional programs offering comprehensive training to develop and cross-train new security practitioners to detect and prevent cyberattacks.[9] In fact, computer science programs struggle to offer adequate cybersecurity courses for the next generation of technologists, and many schools lack trained teachers or course materials in cybersecurity[10], including the top 50 computer science programs in the U.S., only 42% of which offer three or more information security-specific courses for undergraduates.[11]

The cybersecurity workforce gap by region

Lastly, new and far-reaching cybersecurity and data privacy legislation (e.g., GDPR in Europe) enacted over the last five to ten years have driven an increase in demand for staffing who are knowledgeable about data and systems security and protection.

Taken together, these issues present a decidedly pessimistic impression of the future of the cybersecurity industry. However, at Alert Logic, we believe that the current gap in skills and resources presents a powerful opportunity for businesses as well as institutions, including government bodies, schools and associations, to band together in a coordinated effort to provide the expertise, tools and resources required to combat cybercrime on a global scale. .

Six Practical Approaches to Bridge the Cybersecurity Skills and Resources Gap in Your Organization.

We've been offering cutting-edge threat intelligence and expert defence against cyberattacks since 2002, and in that time, we've seen plenty of recommendations come up and just as quickly get dismissed to address and repair the skills and resources gap in the cybersecurity industry. Yet, digital technology continues to transform all levels of the global marketplace, and any practical solutions put forth need to consider—and require accountability from—all levels, too.

Here are six approaches that combine technological and human intervention to bridge the multi-million-person cybersecurity talent shortage experienced by organizations worldwide:

1. Re-envision your hiring and retention strategies to include exploring alternative sources for candidates like universities, job fairs, technical association meet-ups [e.g., Information Systems Security Association (ISSA)], and getting creative with compensation and benefits.

   PROS: Best approach to affect longer-term change in your organization.

   CONS: Requires executive education and buy-in, which can be a challenge for many lean organizations.

2. Look outside your organization, enlisting consultants and/or augmenting staff using third-party outsourcing firms.

   PROS: Effective temporary measure to bridge potential gaps in skills or resources.

   CONS: Can be costly, and when the added resources leave, they often take their expertise with them.

3. Offshore cybersecurity work.

   PROS: Inexpensive, potentially long-term solution.

   CONS: Helps to bridge resources, but often doesn't solve the skills gap.

4. Invest in new technical solutions that are built for automation, integration, and streamlined security operations.

   PROS: Reduces the administrative burden, allowing personnel to focus on responsibilities that require their expert skills and insights. Also, most of today's leading-edge solutions come as SaaS that can flex to meet each organization's particular security needs.

   CONS: Can be costly to implement and requires some system upkeep.

5. Enlist a Managed Security Services (MSS) or Managed Detection and Response (MDR) service to supplement your internal cybersecurity protocols and processes.

   PROS: No need to staff up, as these firms combine expert threat intelligence with proprietary technology to proactively hunt for, investigate, and provide support to eliminate cyberthreats as they come up. Plus, MDRs like Alert Logic offer fully managed service packages to suit any organization—regardless of size or budget—and not only uncover the security issues but also help to remediate, so you're far less likely to experience attacks in the future.

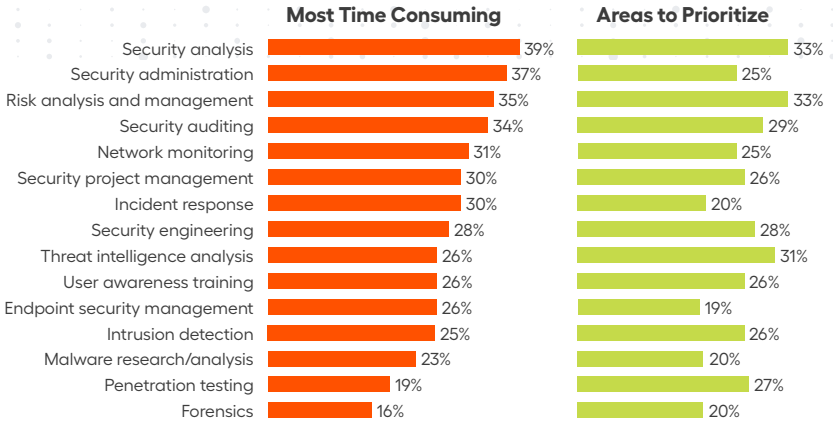
   CONS: If your business requires in-house security solutions and staffing, outsourcing won't work for you.

1. 1 2020 Netwrix IT Trends Report https://www.netwrix.com/2020ittrendsreport.html
2. Accenture Annual Cost of Cybercrime Study, developed jointly with the Ponemon Institute LLC https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
3. IDC "Worldwide Semiannual Security Spending Guide," 2019 https://www.idc.com/getdoc.jsp?containerId=prUS44935119
4. World Economic Forum, The Global Risks Report 2019, 14th Edition http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
5. Companies Need Security Pros With More Varied Skills, July, 9, 2001 https://www.computerworld.com/article/2581991/companies-need-security-pros-with-more-varied-skills.html
6. Accenture, "Securing the Digital Economy: Reinventing the Internet" https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy
7. Cyberattacks Skyrocketed in 2018. Are You Ready for 2019? https://www.industryweek.com/technology-and-iiot/article/22026828/cyberattacks-skyrocketed-in-2018-are-you-ready-for-2019
8. (ISC)2 "2019 Cybersecurity Workforce Study" https://www.isc2.org/Research/Workforce-Study#
9. Information Age, "Cyber security training: Is it lacking in the enterprise?" Sept. 4, 2018 https://www.information-age.com/cyber-security-training-123474550/
10. CNBC.com, "A serious shortage of cybersecurity experts could cost companies hundreds of millions of dollars," March 6, 2019 https://www.cnbc.com/2019/03/06/cybersecurity-expert-shortage-may-cost-companies-hundreds-of-millions.html
11. Marten Mickos, "The Cybersecurity Skills Gap Won't Be Solved in a Classroom," Forbes (online), June 19, 2019 https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#41fe65291c30

6. Implement continuous training and encourage cybersecurity personnel to participate in professional organizations, such as the SANS Institute, the Information Systems Security Association (ISSA), the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS), many of which offer free or low-cost resources, educational tools, and more.

PROS: Keep staff from all areas of your business—not just IT—up to date and ready to combat the latest cybersecurity developments.

HOW CYBERSECURITY PROS ACTUALLY SPEND THEIR DAY VERSUS WHERE THEY'D LIKE TO FOCUS



CONS: Takes initiative from internal stakeholders, including participating staff members, to pursue skills up-leveling.An option quickly gaining popularity is Managed Detection and Response (MDR). This option delivers immediate threat detection, response and monitoring capabilities, delivered as a service, to help organizations save time, money and frustration. Without getting caught up in the care and feeding and ongoing commitment of a SIEM platform, you get accurate, actionable threat insight and remediation advice, aligned with today's threat environment, delivered at a predictable cost which is typically a fraction of the cost of purchasing and maintaining a SIEM.

The Cybersecurity Talent Shortage Doesn't Necessarily Mean the Downfall of Tech as We Know It

Most articles that deal with the global cybersecurity talent shortage paint a dire picture of an industry that's too overloaded with security threats and too under-resourced with skills and tools to keep up. And, while it's true that the rate of attacks continues to rise and a shortage of grassroots talent continues to undermine security strategies, we contend that solutions do exist to combat the persistent shortage of skills and resources in our industry.

Ultimately, organizational leaders must take proactive and persistent steps to bolster internal cybersecurity mandates, enlisting a combination of technological and human intervention to bridge the talent shortage and better weather the inherent risks in the years ahead.

Experiencing the effects of the cybersecurity talent shortage in your company?
Let's talk about how we can bridge the skills and resources gap together.

Contact us today