Coping with the cybersecurity skills gap

How to do more with less

Global Shortage of Cybersecurity Talent

- 82% of IT professionals feel there is a shortage of cybersecurity skills within their organization
- There are 1 million cybersecurity job vacancies worldwide

At this point in history, it's fair to say that our reliance on the internet has developed much faster than our ability to defend it.

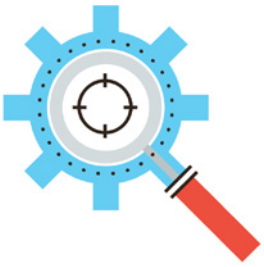
We create more data than ever (2.5 quintillion bytes of it every day1), and we've reached a point as a society where the material expense of a single instance of IT downtime is nearly $9,000 per hour on average[2], while the immaterial cost is crippled business and millions of inconvenienced people.

Yet, according to the Identity Theft Resource Center, more data breaches were confirmed in 2016 than in any year prior[3]. Meanwhile, zero-day threats are on the rise. Internet of Things malware is creating botnets from unsecured digital devices. Ransomware has become a billion-dollar industry. Data leaks, such as the recent dump of the CIA's digital arsenal of zero days and malware, are being announced left and right. Hackers' willingness to go the extra mile for illicit gain is not surprising; but the fact that they continue to succeed is.

Hackers' success stems from the morphing network topology that requires new, more dynamic tools for defense. However, it has been made clear in the past few years that the cyberthreat landscape's squalor is due in large part to a well-documented shortage of cybersecurity experts. According to a recent study from Intel, 82 percent of IT professionals believe there is a shortage of cybersecurity skills in their organization[4]. Cisco corroborated these findings in a separate study, noting that 1 million cybersecurity job vacancies exist worldwide[5]. That number is expected to reach 1.8 million by 2022, according to yet another study[6].

---

1. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html
2. http://searchdatacenter.techtarget.com/news/4500272147/Minute-by-minute-data-center-outage-costs-stack-up
3. http://www.idtheftcenter.org/2016databreaches.html
4. https://newsroom.intel.com/news-releases/global-study-reveals-businesses-countries-vulnerable-due-shortage-cybersecurity-talent/
5. http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf
6. http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
7. https://www.varonis.com/study-finds-employees-security-hygiene-getting-worse-just-as-ransomware-exposes-insider-negligence/



Again, the problem is apparent: There is a severe cybersecurity talent gap, and it's hindering our ability to protect our most important digital assets. It's the solution that may not yet be clear to organizations, and it's the solution that we will spend the rest of this white paper discussing.

Start by fostering an organization-wide cybersecurity culture

Be more selective of IT hires

The average salary of a security analyst is approximately $100,000, and according to Karnam, effective management of a security operation center (SOC) requires more than one of these professionals. The fact that they are in high demand makes it difficult for small and medium-sized businesses to attract and retain this talent – let alone provide these experts with the tools they need to do the job well. That said, Karnam argued that you can still create what he calls a "Frankenstein SOC" using carefully selected IT ops professionals. Ideally, these candidates should exhibit strong hygiene in the IT network space (i.e. knowledge for how to limit attack surface areas). You can then train these professionals using online tools, and nurture that talent.

Appoint a CISO to nourish top-down security culture

Company-wide appreciation for security hygiene doesn't begin with IT or with the lines of business, according to Karnam. It originates at the top, and most often as a directive spearheaded by a chief information security officer (CISO). Ideally, all business decisions should be made with information security in mind. But in the past, cybersecurity was largely an afterthought – an add-on that was expected in support of a business process. This put pressure on IT staff to manage a security strategy for which they had neither the resources nor the expertise. The CISO – in addition to making sure IT isn't burdened with unrealistic expectations – is responsible for providing the security point of view for all high-level business decisions. That perspective trickles down to senior managers, to mid-level managers and so on, until it pervades all business operations from the top down.

As an additional consideration, simple bi-weekly or monthly cybersecurity seminars for the lines of business can go a long way toward improving company-wide security culture. In 2016, a report from the Ponemon Institute found that security hygiene was actually getting worse among the lines of business[7]. This is a problem that, while difficult to permanently eliminate, can be ameliorated by teaching employees best practices from "the break room to the boardroom."

---

7. https://www.varonis.com/study-finds-employees-security-hygiene-getting-worse-just-as-ransomware-exposes-insider-negligence

Leverage third-party cybersecurity expertise

Company-wide best practices are not substitutes for a SOC, and neither is the aforementioned "Frankenstein" approach to security. Granted, both are orders of magnitude above putting complete faith in out-of-the box security or an IaaS vendor, but they aren't ideal by themselves. Furthermore, the longer you nourish cybersecurity talent within your organization, the harder it becomes to retain those IT professionals. Given the quantity of cybersecurity vacancies, home-grown security experts will invariably be courted by competitive new opportunities that SMBs may struggle to match.

These roadblocks have driven many organizations toward MSSPs. The benefit of MSSPs is that they can manage advanced security solutions purchased by the customer, which significantly slashes security overhead. The drawback to an MSSP is that it puts the tool that a company thinks it needs in the hands of a third party. In other words, the client still doesn't gain access to the dedicated cybersecurity expertise that it would have through an in-house SOC. That opens the door to what is perhaps the most important question for our intents and purposes: If a business can outsource the skill needed to manage a specific solution, why can't it outsource the skills needed to build a SOC?

MDR is the component of a SOC-as-a-Service offering that focuses holistically on improving an organization's security posture.

According to Gartner, a recent cybersecurity offering known as managed detection and response (MDR) was born precisely for the purpose of answering that question[8]. MDR is the component of a SOC-as-a-Service offering that focuses holistically on improving an organization's security posture. This is achieved by assigning a dedicated team of security engineers to do the following:

- **Provide ongoing, cyberthreat detection** in real-time
- **Work with the customer** to create incident response plans
- **Continually analyze threat intelligence** to improve security controls
- **Conduct frequent vulnerability scans** and risk assessments to test security posture.

Building an in-house team of professionals and then arming them with the tools they need to accomplish all of the above would easily cost millions of dollars annually – assuming it's even possible to lock down the requisite cybersecurity talent. MDR does all of this at a fraction of the cost.

8. https://cybersecurity.arcticwolf.com/acton/media/18124/gartner-mdr-marketguide?Referrer=Blog

Help us close the cybersecurity gap, one organization at a time

Globally, there is a lot of work to be done before the cybersecurity skills gap is closed, and based on current projections, the situation will likely get worse before it gets better.

Nevertheless, by leveraging the information in this white paper, organizations will have a template for closing the cybersecurity talent gaps that exist within their ranks. In turn, this has the cumulative impact of making the global digital ecosystem just a little more secure. That may not be the singular crushing blow to the cybercriminal community that exists only in our dreams, but we'll take it for what it's worth – one small step in the right direction.

ARCTIC WOLF Layer 7 Data Solutions

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com