by MIT Technology Review Custom, in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc.

Close the Talent Gap, Secure the Future

The shortage of in-house cybersecurity skills is a major challenge for executives who fear their organizations are ill equipped to prevent, detect, and respond to cyberattacks. For that reason, many turn to external partners for security expertise.

It's no secret that finding, hiring, and retaining top cybersecurity talent has always been challenging. But today's cyberthreats are becoming both more numerous and more sophisticated, making those tasks tougher than ever before.

The complexity of information-security environments is escalating in response to the fast-evolving cyberthreat landscape—and the ramifications are widespread: recent breaches at Target and Sony Entertainment, among others, led to high-profile resignations as business leaders bore the blame. But with the intense competition for highly in-demand skills and increased turnover in cybersecurity positions, the race to find—and keep—top talent is more difficult than ever to win.

40%

Percentage of business and IT leaders surveyed ranking "lack of in-house expertise" as their top information-security challenge

Source: *Cybersecurity Challenges, Risks, Trends and Impacts Survey,* MIT Technology Review Custom in partnership with Hewlett Packard Enterprise Security Services and FireEye Inc., 2016

With intense competition for highly in-demand skills and increased turnover in cybersecurity positions, the race to find – and keep – top talent is more difficult than ever to win.

"This is one of the biggest challenges facing security leaders—recognizing there is a significant capability gap in terms of people, process, and technology," says Andrzej Kawalec, who is chief technology officer of Hewlett Packard Enterprise Security Services. Without the right combination of those resources, he warns, "your organization isn't able to respond adequately to cyber-risk."

The struggle to find the right people to hire, develop, and retain weighs heavily on chief information-security officers (CISOs) and other executives. In a February 2016 survey conducted by MIT Technology Review Custom in partnership with HPE and FireEye, nearly 40 percent of respondents cite the lack of in-house expertise as their top challenge.

In that same survey, fewer than 6 percent of the 225 business and IT business leaders who participated believe their organizations are "extremely well prepared" to respond to a security breach involving a major loss of information.

As they scramble to shore up their security teams, CISOs are also grappling with wider-ranging responsibilities than ever before. In the past, information-security heads were accountable for the technology and systems. Now their jobs might include high-pressure tasks as well, such as finding exactly the right professionals to staff critical, highly specialized roles, such as forensics.

Build a Resilient Cybersecurity Team

"Desperation." That's the word Kawalec uses to sum up the mood among organizations looking to hire cybersecurity talent. Hiring executives struggle to fill available positions because there are simply too few experienced candidates trained to face constantly changing threats and increasingly sophisticated attacks. "Demand massively outstrips supply," Kawalec says. "Internal teams aren't able to match the rate or type of change needed to address the cyber-risks organizations face today." As a result, the talent shortfall disrupts, or threatens to disrupt, security operations at many organizations worldwide.

Organizations need to build "cyber-resilient" environments with security teams that can grow and adapt as the world changes, Kawalec adds. That requires hiring some of today's most in-demand security professionals, often with packages involving premium salaries and benefits—or working with expert partners who can help them overcome the skills gaps they may not be able to close on their own.

53%

Percentage by which demand for cybersecurity jobs is expected to grow by 2018

Source: Peninsula Press/U.S. Bureau of Labor Statistics

> "The right person might come from the military, from police work. I don't think there is a recipe for the best people. The skills shortage demands you cast a wider net."
>
> **— Chris Leach, Chief Technologist, HPE Security Services**

The reality: More than 209,000 cybersecurity positions went unfilled in 2015 in the United States alone, and job postings were up 74 percent from 2010 to 2015, according to an analysis of data from the U.S. Bureau of Labor Statistics by Peninsula Press, a Stanford Journalism Program project. The demand for security-related positions is expected to grow by 53 percent through 2018, according to the analysis.

"The longer these jobs remain open and unfilled, the longer you wait to build your team, the more desperate you get," says Kawalec.

More than half the MIT Technology Review survey respondents say their organizations lack adequate forensics skills to lead so-called "hunt teams." Kawalec explains: "These are people who can perform a 'Sherlock Holmes' type of investigation around a breach or a compromise. These are not skills that you get just a couple of years out of college." Such crucial skills include incident response, monitoring, and risk management—all of which are enriched with experience.

Create Cybersecurity Career Paths

Not only is it difficult to find the right people with the right skills, expertise, and experience, it's also a challenge to develop them and to keep them engaged and on your team. The job tenure for high-caliber security talent is often short—18 months at most, Kawalec says.

However, an organization that can offer a specific cybersecurity career path may have an edge when it comes to retaining the best professionals, says Chris Leach, HPE's chief technologist. "You can't just offer a generic career path from HR; it has to be a well-defined map for cybersecurity," says Leach, himself a former corporate CISO. Dangling a coveted prize, such as a position on the hunt team, is one way to entice your best people to stay, he adds.

In addition, it pays to be open-minded and creative when recruiting talent in the first place. An ideal cybersecurity team includes members from distinctly untraditional backgrounds. For instance, Leach once hired a former poker player, who combined good instincts with dogged follow-through, as a security analyst. "He was one of the best," Leach says.

Earning a college degree in computer science isn't the only way to enter the cybersecurity field, Leach notes: "The right person might come from the military, from police work. I don't think there is a recipe for the best people. The skills shortage demands you cast a wider net."

IT experience alone isn't enough to guarantee successful information-security leadership, says

> "A strong technical background will always be critically important, but security pros know that security is ultimately about people, not just computers." **— Grady Summers, Chief Technology Officer and Senior Vice President, FireEye Inc.**

Grady Summers, CTO and senior vice president of FireEye Inc., a global cybersecurity company. "Sometimes organizations say, 'This person was successful in other big IT roles, so they can lead a security team as long as they've got technical experts under them,'" Summers notes. "While I've seen this work in some places, it tends to be unsuccessful."

Cybersecurity roles are also becoming more multidisciplinary and cross-functional, Summers adds. "I'm seeing people with deep security expertise who are taking psychology or law classes, or learning new languages so that they can do their jobs better," he says. "A strong technical background will always be critically important, but security pros know that security is ultimately about people, not just computers." To have a successful security career today, employees must be able to work closely with other functions in the enterprise—HR, legal, public relations, and marketing, for instance.

The entire cybersecurity industry has suffered from a lack of specialized education and training. "There isn't enough targeted, quality education aimed at preparing people to work specifically in cybersecurity," says Kawalec. Toward that end, HPE has partnered with Coventry University in the United Kingdom to offer a cybersecurity-oriented MBA. The program is a direct response to growing demand for training security leaders "as managers able to work with their C-level counterparts," says Jason Ferdinand, the university's course director. Similar degree programs are emerging elsewhere, as well. In the United States, the Florida Institute of Technology, Excelsior College, and Concordia University, St. Paul, are among the schools offering combined cybersecurity–MBA programs.

Consider Partnering to Fill the Gaps

Amid the struggle to find cybersecurity talent—and with the situation unlikely to ease in the foreseeable future—many organizations are seeking external partners to buttress their in-house capabilities. In fact, Leach recalls that in his corporate CISO role, he often looked to third parties to augment his staff.

"A trusted partner brings enhanced capabilities that you aren't in a position to develop in-house," says Kawalec. "You need a team of people with special training who do this every day, giving you expert advice at the point of need."

HPE and FireEye are uniquely well equipped to offer exactly that kind of rapid, hands-on support. With a combination of more than 5,000 cybersecurity specialists and 10 security operations centers globally, serving some 10,000+ customers in more than 60 countries, the two companies' ongoing alliance offers a new level of cybersecurity expertise to organizations worldwide—and helps them close the expertise gaps on their in-house teams. "There is an active, relentless, and dynamic threat from attackers deliberately trying to steal intellectual property and assets, and most organizations aren't able to maintain the continuous staff investment needed to combat these threats," Kawalec says. "Essentially, it's an arms race. Put the burden on us and benefit from the level of protection we maintain."

To learn more about how digital transformation can bolster your cybersecurity, please explore this HPE–FireEye resource website.

About MIT Technology Review Custom

MIT Technology Review Custom produces world-class print, online, and live-event solutions that align clients with a trusted 116-year-old brand. www.technologyreview.com/media