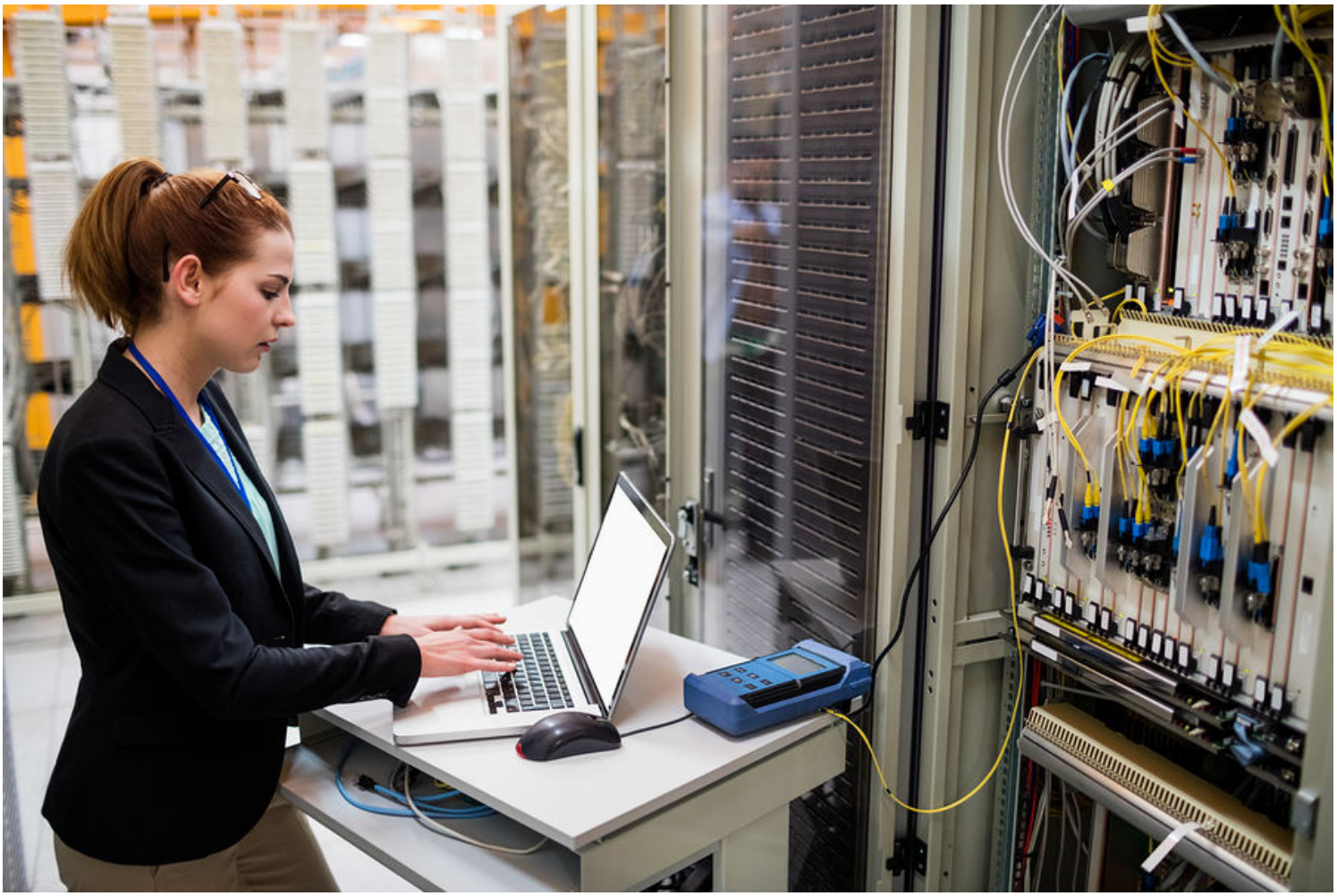
SLAYTON SEARCH PARTNERS

Hiring for Cybersecurity in the Finance Sector



Were you one of the 143 million Americans impacted by the 2017 Equifax data breach? How about one of the 4.6 million people affected by the 2015 Scottrade hack? Or the 76 million households impacted by the 2014 cyberattack against JPMorgan Chase? These are just three of hundreds of known cyberattacks on financial institutions, with thousands more affecting the financial data of businesses across every industry.

Cybercrime is reportedly a $445 billion business, and it's ever-growing, with a 36 percent increase in ransomware attacks across the globe. There's no surprise, then, that demand for cybersecurity professionals is skyrocketing across every industry. This is especially true in the financial sector. IBM Security Services sees 65 percent more attacks on its financial services clients than any other client. And yet, only 21 percent of IT leaders report being "very well" prepared

for these attacks.

Beyond the risk of malware, ransomware, and other cyberattacks, a PwC survey reveals these top five cybersecurity challenges:

- Assessing security procedures of vendors
- Dealing with complex technologies
- Protecting sensitive customer information
- Understanding and complying with regulation
- Developing and administering employee training

Unfortunately, exponential demand is met by an extremely limited supply of professionals. Analysts forecast as many as 1.5 million cybersecurity positions will go unfilled by 2020. In a field where the unemployment rate is effectively zero, how can organizations hope to stem the risk of cyberattacks and protect against vulnerabilities?

Hiring for a Unique Skill Set

Successful cybersecurity professionals have a unique set of skills. Because it is next to impossible for any company to avoid 100% of human error in every project, let alone one complicated by the nuances of cybersecurity, their soft skills are integral to the role. Not only have these professionals built the necessary technical experience, but they're also outstanding collaborators who understand the challenge of cybersecurity in the framework of business objectives. They understand risk management, are quick and willing to learn, and choose to really listen before diving in.

Many of these skills and characteristics are unteachable. That means the traditional search for cybersecurity professionals may be somewhat flawed. A more "typical" career path supported by a college degree and appropriate work experience are often the first things a hiring manager looks for when seeking to fill open roles in cybersecurity. But this strategy is unlikely to be successful as the cybersecurity talent shortage continues to grow. Instead, companies need to look for people who are passionate about problem solving and possess a sense of ethics that can't be taught. From there, training and certification programs can fill in the gaps.

IBM is reportedly using this exact approach, developing "new collar" jobs in areas like cybersecurity. They value skills over degrees, providing training and development programs to build employees' technical knowledge. It's a long-term solution that may effectively resolve the cybersecurity skills shortage.

Finally, it's important to recognize how greater diversity can help address the skills gap challenge. A PwC study reveals that just 11 percent of cybersecurity professionals in the US are women, a statistic that has remained flat over the last two years. Ethnic minorities see similar numbers, with less than 12 percent in the cybersecurity workforce. A focus on diversity in the c-suite and across all areas of an organization would greatly benefit companies who struggle with finding talent. Addressing corporate cultures that lack diversity and adjusting hiring strategies to attract a wider audience are ways that invite greater numbers of talented workers.

Other Considerations When Hiring Cybersecurity Professionals in Finance

There is a myriad of state and federal regulations that already aim to help regulate cybersecurity in financial institutions, including the FCRA and a recent policy enacted by the New York State Department of Financial Services. This is in addition to "voluntary" standards, such as those developed by the National Institution of Standards and Technology in its Cybersecurity Framework and the Data Security Standards set by the Payment Card Industry. Furthermore, there have been several propositions at a federal level for a more comprehensive ruling on cybersecurity for financial institutions. All in all, there is no lack of uncertainty for leaders in finance when it comes to protecting their organizations in a legal sense as well as in a cyberthreat sense. Shifting and overlapping regulations can make it difficult to hire the right cybersecurity professionals. As discussed, these workers must have a foundational sense of ethics as well as a clear understanding of how cybersecurity fits into the big picture of the organization.

Beyond regulations, finance executives must also consider the cost of hiring best-in-class cybersecurity professionals. These workers are some of the most sought-after talent in the workforce. It goes without saying that the competition has led to sky-high salaries and wages. The Bureau of Labor Statistics reports that the average annual wage for information security analysts is $92,600. Other cybersecurity roles can see upwards of $160,000 annual salary. Of course, these numbers shift according to region, company size, experience level, industry, and other factors. Companies that are struggling to fill security positions must research and offer market rates for these individuals, or else risk losing talent to the competition. Considering the high risks of leaving cybersecurity positions open, the investment in top talent will be more than worth it.

How is your organization adapting to these trends in cybersecurity?

Related Articles

The Challenge of Hiring Executive Leaders in a Candidate-Driven Market

SLAYTON SEARCH PARTNERS

How HR Should Respond to Retiring Baby Boomer Executives

Exploring the State of Diversity in the C-Suite