5 Strategies to Fill the Cybersecurity Skills Gap For Financial Services Firms

The financial services industry is one of the hardest hit for cyberattacks. With today's ease of transactions via web, mobile, and cloud environments, technical adoption, while convenient and seamless, is unfortunately weakening the attack surface for hackers.

BY THE NUMBERS: CURRENT THREATS FOR FINANCIAL SERVICES

- Raked 1st out of 26 for most attacked industries by a cyber criminal
- $23.6 million lost from cybersecurity breaches in 2013
- 98% of cyberattacks are successful in less than one day
- 72% of firms are unable to detect or remove attacks
- Only 47% of firms are able to restore their business after an attack
- 26% of financial services institutions are most concerned about financial losses from cyber attacks
- 37% of financial services companies believe individual hackers pose the greatest danger

Meanwhile, financial cyber teams struggle to keep pace with the onslaught of threats due to both a lack of manpower, skill development, and expertise. Today, financial services firms are seeing a need to act fast to fill the cybersecurity skills gap so they can better protect trade secrets, compare, and their customers.

FILL YOUR TALENT PIPELINE

- Hire people with different professional backgrounds for a ‘think different’ perspective
- Seek transferrable skill sets [e.g. problem solving, communication]
- Look beyond the technical degree and certificates

LOSE REAL-WORLD EXPERIENCE

- Let candidates describe how they addressed a real attack if experienced in the industry
- Learn about their career path and how they got to where they are today
- Understand their strategies and approach to the position

GIVE THEM A SCENARIO TO PRACTICE YOUR ASSESSMENT

- Give them a scenario to perform to gauge their ability to manage sensitive data confidentiality
- Ensure they undergo a scenario check
- Make a list of qualifications needed for the position

RECOGNIZE CONTINUOUS PROFESSIONAL DEVELOPMENT OPPORTUNITIES

- Invest in active learning training platforms with good feedback to optimize staff skill development
- Ensure staff training regardless of their skill level to prepare them for any cyber attack situation
- Include repetitive, active learning cyber training techniques to keep skills sharp

ADOPT A "PEOPLE CENTERED" APPROACH TO INFO SECURITY

- Don't rely on an advanced technology solution to secure customer data—there must be people placed behind the software
- Set expectations that staff are required to be "a part of the defense of the industry"
- Send out monthly reminders of recent attacks to keep everyone current on the latest threats

"Cybersecurity has to be something that's integrated into the way people think about business opportunities and capabilities. It can't be just something that the technology guys are going to fix." - Joe Reina, US Financial Services, Cybersecurity Leader