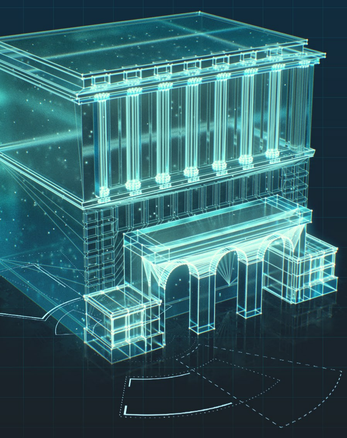
CIRCADENCE

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

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

BY THE NUMBERS: CURRENT THREATS FOR FINANCIAL SERVICES



- **Ranked #1** out of 26 for most attacked industries by a cyber criminal
- **$23.6 million lost** from cybersecurity breaches in 2013
- **88%** of cyberattacks are successful in less than one day
- **79%** of firms are unable to discover attacks
- **Only 40%** of firms are able to restore their business after an attack
- **36%** 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 lack of man power, skill development, and expertise. Today, financial services firms are taking a hard look at how to fill the cybersecurity skills gap, so they can better protect and defend their companies and their customers.

1 FILL YOUR TALENT PIPELINE

- Hire people with different professional backgrounds for a "fresh" perspective
- Seek transferrable skill sets (e.g. problem solving, communication)
- Look beyond the technical degree and certificates

2 LOOK FOR REAL-WORLD EXPERIENCE

- Let candidates describe how they've addressed an attack if experienced in the industry
- Learn about their career path and how they got to where they are today
- Understand their strategic approach to the position

3 USE DATA TO INFORM YOUR ASSESSMENT

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

4 PROVIDE CONTINUOUS PROFESSIONAL DEVELOPMENT OPPORTUNITIES

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

5 ADOPT A "PEOPLE-CENTRIC" APPROACH TO INFO SECURITY

- Don't rely on advanced technology alone to secure customer data—there must be people behind the curtain
- Set expectations that staff are required to be "students of the industry"
- Send out monthly roundups of recent attacks to keep everyone current on the latest threats

"Cybersecurity has to be something that's ingrained into the way people think about new business opportunities and capabilities. It can't be just something that the technology guys are going to fix."

- Joe Nocera, US Financial Services Cybersecurity Leader

PROJECT ARES®

LEARN HOW PROJECT ARES HELPS FILL THE SKILLS GAP

303.413.8800 • www.circadence.com • sales-cyber@circadence.com

HEADQUARTERS Boulder, CO 80302
ADVANCED RESEARCH & DEVELOPMENT FACILITY Tupelo, MS 38804
CENTER FOR CYBER AUTONOMY San Diego, CA 92123
WASHINGTON D.C. SALES McLean, VA 22101

CIRCADENCE

©2018 Circadence Corporation. All rights reserved.
Circadence, the Circadence logo, Project Ares, and the Project Ares logo, are trademarks or registered trademarks of Circadence in the US and other countries.
Statistical references sourced from https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/financial-services/DUP_Digital-transformation-in-financial-services.pdf