Who is your Next Security Hire?
Where to look outside of information security

In addressing the skills gap in cybersecurity, CISOs and their human resource counterparts now engage in creative tactics to recruit and retain employees to join their teams. Here we look at other industries where the next great cybersecurity professional might be found.

CATEGORY: TRIED AND TRUE

1. LAW ENFORCEMENT AND MILITARY

Type Casting: Professionals in these industries are generally astute forensic investigators, and shrewd when it comes to identifying suspicious activity.

The State of Their Industry: The Bureau of Labor Statistics reports that employment of police and detectives is projected to grow 4% from 2014 to 2024, which is slower than average compared to other occupations in the United States. However, the contract defense industry is projected to grow rapidly as the United States defense budget increases, after years of steady decline. Military veterans interested in staying in the defense industry will find opportunities there.

Fit Factor: Based on statistics of CISOs we have featured in our magazine, roughly 30% are veterans of the armed forces.

Learning Curve: Technical and engineering degrees are not generally required for employment in law, so these cross-over hires may need additional training on technology.

2. IT GENERALISTS AND NETWORK ENGINEERS

Type Casting: Employees who already understand the systems, networks and applications that need protecting are obvious candidates. According to Digital Guardian, 59% of CISOs came up through the IT ranks.

The State of Their Industry: According to a recent report in USA Today, this year, there are 627,000 unfilled IT jobs in the United States. Many IT professionals might decide to transition into information security to broaden their skillsets.

Fit Factor: There is a reason most CISOs come from IT - a strong knowledge of technology is important to protecting a company's vital assets, and IT workers possess that knowledge to great degrees.

Learning Curve: Familiarity with technology can help IT professionals hit the ground running in information security, but sometimes these tech-savvy contributors need education and training to understand business goals and to communicate security to business users.

CATEGORY: WHERE COMPLIANCE MEETS SECURITY

1. LAWYERS

Type Casting: Increasing industry and government regulations, the importance of security policy and the introduction of tools such as cyber risk insurance, have all made a law degree highly-valuable for specific strategic roles on the information security team. There is also a spike in organizations adding Chief Privacy Officers to their executive teams.

The State of Their Industry: Young lawyers may be on the hunt for non-traditional roles. Recent graduates of law schools are 5% less likely to be employed in their field than they were in 2007, according to the National Association for Law Placement.

Fit Factor: A prospect with a law degree may be a good fit for a CISO's e-discovery and forensics team, and has the ability to help navigate compliance and customer and employee privacy issues.

Learning Curve: Lawyers will be naturals at dealing with corporate privacy concerns and the legal ramifications of non-compliance. They will be adept advocates for sound security policies. They likely will not come with a technical background.

2. ACCOUNTANTS

Type Casting: An accountant's time-tested skill in

performing audits will make them a natural fit for the compliance and audit group within an information security organization.

The State of Their Industry: According to the Bureau of Labor Statistics, the accounting industry is projected to grow 11% from 2014 to 2024.

Fit Factor: Accountants are skilled in investigations and capable of understanding complex laws and regulations. Tax accountants have a reputation as detail-oriented, ethical and diligent employees.

Learning Curve: While a natural fit for audit and compliance teams, they may lack the skills and training to work on the technical side of information security, or the appetite to work in threat detection.

CATEGORY: THE COMMUNICATORS

1. BUSINESS ANALYSTS

Type Casting: Business analysts are the bridge between IT and business users, tasked with taking business requirements and helping developers and engineers create systems that meet the needs of the user.

The State of Their Industry: Business analysts often grow into positions of project management within the IT department. To advance beyond middle management, analysts must pick a field of focus, such as information security.

Fit Factor: Business analysts are skilled in communicating in both business and technical language, a core attribute CISOs seek in their team members.

Learning Curve: Most business analysts have some technical knowledge, although an IT degree is not a necessity for the role. Business analysts will be comfortable in outward-facing security roles, as

well as performing testing, systems monitoring and investigations as a security analyst.

2. TRAINING MANAGERS

Type Casting: Training and internal communication professionals are experts in delivering complex information in easy to understand ways.

The State of Their Industry: According to PayScale, the average salary of a training manager is $66,000, and the average salary of a mid-level information security professional is over $100,000. Training jobs are readily available, the salary increase may make a jump to information security very appealing.
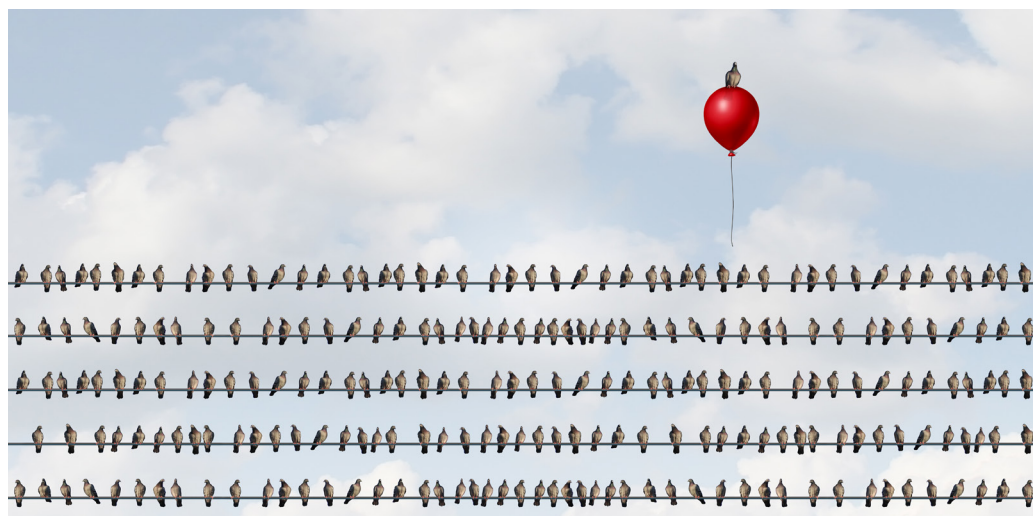
Fit Factor: Business user training and effective communication skills are crucial among CISOs' reported challenges. These professionals are creative thinkers adept at presenting information in articulate ways, making them expert liaisons between the business and more technically-savvy information security professionals. They may also be enlisted to deliver important end-user training, assist in writing clean policies and run security ambassador programs.

Learning Curve: It is likely corporate trainers or internal communications professionals will need to be trained in information security specifics.