CYBERSECURITY HELP WANTED

The Framework to Improve Your Workforce Strategy and Manage the Looming Security Talent Crisis

northhighland
WORLDWIDE CONSULTING

NORTH HIGHLAND INSIGHTS

The following report draws on our experience leading workforce development programs for clients across various industries, and the results of two North Highland-sponsored surveys conducted in October 2017 and April 2018. The surveys identified the top strategic priorities for business leaders in 2018 and emerging trends in how organizations are managing the challenges of cybersecurity and security talent shortages. This report utilizes those insights to spotlight opportunities for organizations to emulate what's working, compare themselves to industry averages, and differentiate in the margins.

Survey Participants

Business Leader Mindset/BEACON
More than 600 senior-level employees in energy, financial services, healthcare, retail, and media, entertainment, and telecom companies surveyed in October 2017.

Technology & Digital
More than 300 director-level and above employees with leadership responsibilities in technology/digital categories at global companies with revenues in excess of $1/£1 billion surveyed in April 2018.

Key Takeaways

- **The problem:** Security talent is a defining asset and the top priority for leaders in 2018, however a growing gap between available qualified cybersecurity professionals and unfulfilled positions will reach 1.8 million by 2022.[1]

  Moreover, 70 percent of organizations aren't highly confident that in-house IT workforces have the right security skill sets to deal with today's cybersecurity challenges.

- **The analysis:** This talent-confidence gap can be applied to develop a security talent supply chain strategically aligned to organizational priorities and your industry averages.

- **The solution:** Understanding your unique talent challenges and security employee reinvestment rates is key to defining and correcting the talent problem through a custom counter-offensive based on the following framework:

  - A skills-based approach with skills mapped to security disciplines
  - A plan designed around industry-specific requirements
  - Creative employee hiring, training, and retention practices focused on meaningful human engagement

In the summer of 2017, the social security numbers, birth dates, and addresses of 143 million Equifax customers were exposed in one of the most significant data breaches in recent memory.

Before he stepped down, Equifax CEO Richard F. Smith reported to Congress that "human error and technology failures" were to blame[2], referring to an "individual" in Equifax's technology department who had failed to heed security warnings and did not ensure the implementation of software fixes that would have prevented the breach, which could cost the company upwards of $600 million.

Over the last decade, many organizations have made multimillion-dollar investments in security technologies, processes, and talent to meet shifting regulatory requirements and prevent an Equifax-esque nightmare. In our October 2017 survey of more than 600 senior-level employees across a variety of industries, cybersecurity was the number one priority in 2018 for all respondents, with 46 percent reporting they believe its importance will continue to increase this year.[3]

While security technology and processes have become increasingly available and heavily marketed, increased competition for associated security talent has created a frightening gap.

Frost & Sullivan predicts that the growing gap between available qualified cybersecurity professionals and unfulfilled positions will reach 1.8 million by 2022.[4] Because of this global skills shortage, nearly half of all cybersecurity professionals are solicited to consider other jobs at least once per week.[5]

In North Highland's April 2018 survey of more than 300 leaders in the U.S. and U.K., only 30 percent "strongly agree" their in-house IT workforces have the right security skill sets to deal with today's cybersecurity challenges and demanding landscape; challenges expected to cost global businesses over $8 trillion over the next five years.[6]

In a rapidly shifting security ecosystem, one constant has emerged. Cybersecurity workforce acquisition, development, and retention must become laser-focused on establishing right-size, right-time staffing models – even amidst the steady knocking of competitors with job offers and cyber criminals with malicious intent.

It's important to learn what we can from the Equifax breach, and to recognize that every day cyber criminals are working to score a bigger payday. Experts agree it is only a matter of time until a new company takes Equifax's infamous place in the spotlight. Grounded in the belief that everything begins and ends with humans, this piece is intended to empower IT and technology leaders – and the human resource departments that serve them – to establish a workforce strategy that makes people their first line of cyber defense.

OF LEADERS "STRONGLY AGREE" THEIR IN-HOUSE IT WORKFORCES HAVE THE RIGHT SECURITY SKILL SETS TO DEAL WITH TODAY'S CYBERSECURITY CHALLENGES

THE THREATS: FOUR EMERGING CHALLENGES IN CYBERSECURITY WORKFORCE MANAGEMENT

Security talent is a defining asset for IT security organizations, and in the field of cybersecurity a unique set of challenges make securing this talent even more expensive and critical.

Understanding these unique challenges is an important first step towards defining, developing, and implementing talent management programs and practices that drive business results and promote employee engagement, development, and retention.

> **IN A MARCH 2018 SNAP POLL OF WALL STREET JOURNAL CIO NETWORK MEMBERS, MORE THAN HALF OF RESPONDENTS AGREED THEY ARE "SECRETLY WORRIED THAT THEIR FIRMS DON'T HAVE THE IT TALENT THEY WILL NEED TO COMPETE."[7]**

1 CYBERSECURITY THREATS ARE EVOLVING FAST.

There are two types of companies in the world today: those that know they've been hacked, and those that don't. As companies collaborate with a wider network of partners and digitize to offer 24/7 operations and greater transparency, the scope, scale, and impact of cybersecurity risks grow in concert with rapidly evolving technologies. The expanding universe of Internet of Things (IoT) devices is particularly vulnerable to exploitation as companies may not update them after installation, and many devices are not able to receive security update patches, according to AIG.[8]

Our research found that while 45 percent of respondents strongly agree that "my employees understand the risks associated with cyberattack," only 30 percent strongly felt that their organization "has the in-house security talent and skills needed to deal with cybersecurity priorities over the next three years." This difference represents a **talent-confidence gap** that will constrain organizations over the near-term as they attempt to make security improvements against their priorities.

INDUSTRY INSIGHTS: The Talent-Confidence Gap

- In the finance and manufacturing industries, this talent-confidence gap appears narrow, with respondents signaling a gap of less than seven percent.
- However, in the IT/telecom industry, where cybersecurity threats have arguably the most direct impact to operations, the gap is considerable at 25 percent between understanding and skills.
- For the healthcare and retail industries, the talent-confidence gap is still substantial at 15 percent.

The damage of a data breach goes well beyond the immediate bottom-line impact of settlements and clean-up. Customer trust is often inexorably damaged, with a whopping 70 percent of consumers reporting that they would stop doing business with an organization if it experienced

a data breach.[9] Increasingly, consumer trust in an organization's cybersecurity is emerging as a competitive advantage.

2 CYBERSECURITY TALENT SHORTAGES REQUIRE WINNING COMPANIES TO MAKE ABOVE-AVERAGE INVESTMENTS OF TIME AND MONEY.

It takes a heavy investment of time and money to get (and keep) cybersecurity employees up to speed; if they leave, those investments are lost. And time in particular is painfully short: 40 percent of cybersecurity leadership reports spending most of their time focused on day-to-day critical threats,[10] rather than developing and executing long-term security and workforce strategies.

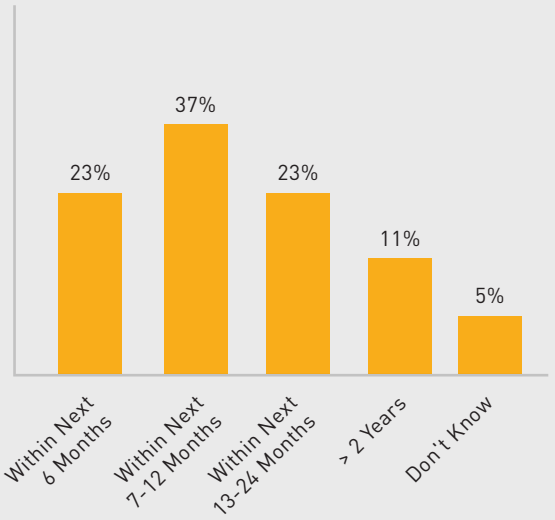
Finding the right people to be passionate advocates for security programs requires ongoing commitment to skill set improvement and education for key employees. Yet our research shows that only 23 percent of organizations plan to make significant investments in their in-house security talent (including the hiring and training of talent and investing in tools and strategies) in the next six months.

Moreover, while only 13 percent of respondents perceive a near-term talent shortage, 60 percent are planning to make significant investments (>five percent of annual IT budget) in in-house security talent within the next year (i.e. hiring, training, retention bonuses). Examining the difference between these two metrics can help us infer the ratio of near-term investment focused on human capital spending beyond hiring — **a security employee reinvestment rate.** This metric helps quantify respondents' level of recognition that keeping

NORTH HIGHLAND INSIGHTS

FUTURE INVESTMENTS IN IN-HOUSE SECURITY TALENT

Are you planning to make significant investments (>5% of annual IT budget) in your in-house security talent in the near future?



their existing team will require a holistic plan backed by significant financial resources.

INDUSTRY INSIGHTS: Security Employee Reinvestment Rates

- Overall, the 47-point gap between significant near-term talent investments and admission of in-house talent gaps signals that for every dollar spent on hiring security talent to meet shortages, $3.50 will be spent to train or retain the existing workforce.
- This average security employee reinvestment rate of $3.50 appears to hold steady when zeroing in on the healthcare and IT/telecom industries (retail is marginally higher at $4.68).
- However, in the finance industry, where confidence about in-house talent is above average, the ratio of security human capital spending beyond hiring jumps to $10 for every dollar spent on hiring – almost triple the average. This could be an indication that many organizations within the finance industry are fighting to protect their existing security teams amidst above-average levels of competition for talent within the industry.

3 CYBERSECURITY TALENT IS ON THE BRINK OF A BURNOUT, AND THAT INCREASES SECURITY RISK.

Talent shortages mean employees are overworked, and their burnout directly contributes to increased risk: 84 percent of data breaches are at least in part attributable to human error.[11]

Employee burnout is a compounding challenge. Elevated risk means more emergency response, less time for long-term strategy and talent development, and less engagement and satisfaction as employees are further denied opportunities to learn and grow.

When it comes to developing these strategies, our research shows that less than half of organizations (49 percent) have formal workforce strategies in place that include security talent supply/demand analysis. When compared to the data referenced previously regarding significant near-term investments on in-house security talent (60 percent), we reveal a disconnect between having funding for a plan versus having a plan for that funding.

INDUSTRY INSIGHTS: Near-Term Investment vs. Long-Term Strategy

- The finance industry appears to have the largest positive differential between planned near-term security talent investment (63 percent) and formal security workforce strategy (43 percent), resulting in a 20 percent positive gap.
  - This indicates that a more detailed approach to security workforce planning could improve return on investment (ROI) on security talent spending, and may also indicate underinvestment in existing workforce supply/demand analysis activities.
- In IT/telecom (17 percent), retail (15 percent), and manufacturing (14 percent) we see similar positive gaps in security talent investment to talent planning numbers.
  - Again, these responses suggest gaps in security workforce planning and probable low ROI for existing security talent spending.

- In the healthcare industry the numbers tell a different story. Planned near-term security talent investment (56 percent) trails the number of respondents indicating an active security workforce strategy is in place (62 percent), resulting in a six-point negative gap. The healthcare industry leads all other industries in workforce strategy planning (13 percent above average).
    - Combining these insights suggests that the healthcare industry's significant investment in workforce strategy is helping keep security talent investments aligned to capacity to effectively plan for near-term spending.

4 CYBERSECURITY PROFESSIONALS HAVE A PRICE MOST ORGANIZATIONS AREN'T PREPARED TO PAY.

Recruiting and retaining a modern cybersecurity workforce requires organizations to incentivize beyond a salary. While financial compensation topped the list of job satisfaction drivers (42 percent), "support and training to advance IT security careers" and "business management expressing a commitment to strong cybersecurity" closely followed at 38 and 37 percent, respectively, as top satisfaction drivers.[12]

Other non-financial incentives, including flexible work schedules and environments, and opportunities to collaborate cross-functionally, are increasingly important for employers to retain top talent, yet far too many cybersecurity organizations aren't optimized to employ them.

Organizations also need to think about leveraging multiple talent supply channels to augment their internal teams. When driving security strategy, organizations take different approaches to outsourcing talent to management consulting firms and dedicated security companies.

INDUSTRY INSIGHTS: Multiple Talent Supply Channels

- Across all industries, approximately 39 percent of respondents indicated dedicated security companies were most qualified to drive an organization's security strategy, while 18 percent indicated management consulting firms were most qualified. The strongest preference was for internal resources to drive security strategy (44 percent).
- Within the finance industry, there is a stronger preference for internal resources to drive security strategy (54 percent), followed by an even preference (23 percent) for either management consulting or security company support.
- In healthcare (38 percent) and IT/telecom (33 percent), internal resources are believed to be less qualified to drive security strategy than dedicated security companies (44 percent in healthcare and 58 percent in IT/telecom).

CONNECTING UNDERSTANDING WITH SKILLS FOR £10M IN DIRECT RISK MITIGATION

In the aftershock of several Personally Identifiable Information (PII) data breaches, a large UK-based telecommunications provider turned to North Highland to help reconcile their gap between cybersecurity understanding and skills.

Through a seven-week discovery period, North Highland determined that the organization's information policies were outdated, not well understood, or otherwise not taken seriously by the business. It was unclear where PII data was stored, who it was shared with, and what controls protected it. There were also no checks in place to ensure employees and third parties were compliant with policies. Collectively this made it impossible to understand, quantify, and prevent associated risks with customer and employee data.

As a result of this analysis, North Highland identified £10m of direct risk that could be mitigated by a set of recommendations around a new information policy which engaged employees across the organization, and put into place a process to better classify information, explain PII, and align policy with strategy. That process included a way to bring together all information assets, and the implementation of a supplier and information asset register. Moreover, it provided the framework for managing the flow of employee data across 50+ outsourced HR suppliers, and a platform for housing policies, information, and audit processes in one place.

THE COUNTER-ATTACK:

THREE WAYS TO MAKE PEOPLE YOUR FIRST LINE OF DEFENSE

Given the unique cultural attributes of cybersecurity talent, traditional workforce strategies may not be enough to fill the growing cybersercurity talent shortage. Instead, it commands an approach that begins and ends with humans: one that is grounded in a heightened focus on the engagement, skills, and needs of people.

Our research shows that 40 percent of organizations have informal workforce strategies in place, and within that group, 92 percent indicate security talent is a top discussion item. The following offers immediate opportunities to fine-tune those existing workforce strategies to capitalize on emerging opportunities and precisely target efforts for immediate and long-term impact in the uniquely critical cybersecurity field.

THE FUNDAMENTALS OF A CYBERSECURITY WORKFORCE STRATEGY

Starting from nothing is hard. If you are one of the 30 percent of organizations with no formal cybersecurity workforce strategy in place, here are three first steps to get you started:

1. KNOW YOUR LANDSCAPE

Above and beyond the macro challenges listed throughout this piece, understanding the custom micro challenges in your organization is the first step toward creating a meaningful and impactful workforce strategy.

2. IDENTIFY THE PRECISE SKILLS AND TALENTS YOU NEED

By assessing your internal needs and capabilities, you can better plan for the gaps and create sourcing strategies targeted on finding the specialty talent best suited for your organization. If you know which roles need which skills, then you can be strategic about what to outsource and when.

3. ESTABLISH TARGETED EMPLOYEE DEVELOPMENT PROGRAMS

Cybersecurity employee development programs impact short-term success and long-term job satisfaction, both for people who are new to the organization and new to the roles of cybersecurity. An effective workforce strategy includes education and ongoing learning to retain talent, and to ensure talent is equipped to combat rapidly evolving security threats.

1 TAKE A SKILLS-BASED APPROACH MAPPED TO SECURITY DISCIPLINES.

It seems simple, but are you sure you're hiring, retaining, and training for the cybersecurity skills your organization needs most, or will need most in the future?

Right-sizing the skills required for current cybersecurity needs is essential. Understanding how to help cybersecurity professionals grow, and clearly defining growth paths over time can be matched with the SFIA framework, a series of skills leveled 1-7 that identify the common tasks of cybersecurity professionals. Starting with the most basic need of identifying risks and issues and working to remediate (level 1) to influencing policies and business strategy (level 7), the SFIA framework can help organizations determine the right amount of autonomy, influence, and business acumen for each role, as well as provide forward-looking benchmarks for advancement.

Taking the time to map key skills to functional security disciplines (such as Identity and Access Management (IAM), Incident Response, Regulation and Compliance) can help workforce planning efforts zero in on critical skill shortages, or future areas of skill demand.

Strategically determine which disciplines you can outsource or insource based on immediate and long-term needs.

2 BUILD INDUSTRY-SPECIFIC REQUIREMENTS INTO YOUR PLAN.

All industries should customize their talent strategy to forecast, hire, and train for industry-specific needs.

In the utilities industry, for example, security professionals must have a basic understanding of the NERC-CIP regulatory regime to view standard security concepts through a utility-specific lens. In financial services, security candidates with exposure to the Federal Financial Institutions Examination Council (FFIEC) will stand out. And in retail, familiarity with PCI-DSS is central to understanding the controls relevant to industry-specific cyber threats.

3 GET CREATIVE WITH EMPLOYEE HIRING, TRAINING, AND RETENTION.

North Highland research shows that only 24 percent of respondents consider "preparing their culture" as a cybersecurity priority. Yet culture is a critical intangible in keeping your talent amidst the incessant knocking of competitive job offers. Investment in culture requires time and money, but is ultimately likely less costly than sourcing net new talent.

Start by applying your skills-demand findings to design targeted internal skills development programming, total rewards strategies (retention bonuses, flexible work programs, etc.), and succession planning.

Internal resources already know your industry and your company's specific security needs. Keep them fresh on the latest security trends and focused on how those trends apply to your organization. Give them a choice in training topics, and demonstrate how their development choices can propel their upward mobility within the organization.

Lastly, consider non-traditional, "new collar" candidates.[13] Establish apprenticeship opportunities, emphasize certification programs, explore new education models and networking communities, support programs at community colleges or polytechnic schools, and look for talent

OF LEADERS CONSIDER "PREPARING THEIR CULTURE" AS A CYBERSECURITY PRIORITY

in unexpected places, such as threat/intelligence-sharing communities.

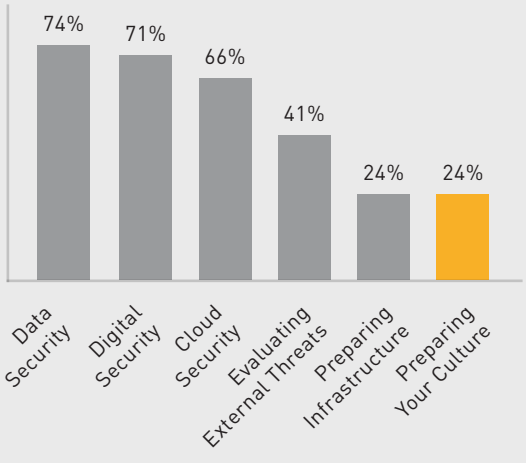
A joint initiative between academia and the private sector in Massachusetts may be a model nationwide. The Cybersecurity Education and Training Consortium (CETC) is working to "collectively address the high demand for talent in the rapidly growing field of cybersecurity"[14] with the creation of 40 new cybersecurity training and degree programs in the region's colleges and universities.

Other burgeoning industries in history have had successfully filled ranks with similar initiatives. In 1951, the U.S. accounting industry was poised for growth, but was predominantly male, with only 500 female certified public accountants in the country. After recognizing the problem, leaders across the accounting field teamed with industry associations and academic institutions to solve the issue through awareness campaigns and hiring initiatives. Today, more than half (61 percent) of all accountants and auditors in the U.S. are women.[15]

NORTH HIGHLAND INSIGHTS

CYBERSECURITY PRIORITIES

Which of the following fall within your top-three cybersecurity priorities this year?



YOUR NEXT MOVE FOR SECURING SECURITY TALENT

Your ability to secure and retain cybersecurity talent will increasingly serve as your core competitive differentiator in the digital marketplace. Understand where you are in comparison to others in your industry: After all, those are the organizations targeting your current talent, and fighting against you to secure new talent. Then move beyond traditional workforce strategies, taking a skills-based, industry-specific, creative approach to not just prevent an Equifax-esque incident of your own, but to create a competitive advantage based on consumer trust through your cybersecurity talent.

---

1 "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," Frost & Sullivan, March 2017

2 "Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says," The New York Times, Oct. 3, 2017

3 North Highland Beacon 2018

4 "The 2017 Global Information Security Workforce Study: Women in Cybersecurity," Frost & Sullivan, March 2017

5 "Cybersecurity skills shortage creating recruitment chaos," CSO, Nov. 28, 2017

6 Juniper Research, April 25, 2017

7 "The Morning Download: Hiring Is the CIO's Top Concern, WSJ Snap Poll Shows," The Wall Street Journal, March 8, 2018

8 "The Internet of Things and Cyber Risk: How You Could Be Victimized," AIG

9 "2017 Data Breaches and Customer Loyalty Report," Gemalto

10 "The Life and Times of Cybersecurity Professionals," ESG and ISSA, Nov. 2017

11 Aug. 2017 Lastline survey of Black Hat USA 2017 attendees, eSecurity Planet, Aug. 23, 2017

12 "The Life and Times of Cybersecurity Professionals," ESG and ISSA, Nov. 2017

13 IBM New Collar, IBM

14 "Closing the Cybersecurity Talent Gap: What They're Doing in Massachusetts," SecureWorld, Feb. 21, 2018

15 "Statistical Tables: Awards/Degrees Conferred by Program (2010 CIP Classification), Award Level, Race/Ethnicity, and Gender – Includes New Race/Ethnicity and Award Level Categories," Completions Survey (2017)

ABOUT OUR TECHNOLOGY & DIGITAL SERVICES

At North Highland, we help organizations drive market gains by aligning technology with strategy and culture, optimizing the types of tools and services that drive informed decision-making, enable internal collaboration, and enable secure, resilient organizations.

As security threats grow in number and scale, North Highland's cybersecurity expertise helps organizations build the human and operational competencies that equip leaders to protect the business, enable employees to recognize their role in security, and inspire collective action to protect the organization. We focus on aligning security strategy, operations, and culture with the digital tools and services that drive security.

ABOUT NORTH HIGHLAND

North Highland is a global management consulting firm known for helping clients solve their most complex challenges related to customer experience, performance improvement, technology and digital, and transformation. We add value and support our clients across the full spectrum of consulting, from strategy through delivery. We bring the big ideas, then we make them real. North Highland is an employee-owned firm, headquartered in Atlanta, Georgia, with more than 3,000 consultants worldwide and 60+ offices around the globe. The firm is a member of Cordence Worldwide (www.cordenceworldwide.com), a global management consulting alliance. For more information, visit northhighland.com and connect with us on LinkedIn, Twitter and Facebook.

For more information about this topic, please contact:

Mark Resnik
Mark.Resnik@northhighland.com

Mark has 18 years of experience in security and business operations and is a leader in North Highland's cybersecurity practice. Mark's experience spans a broad set of industries including financial services, energy & utilities, retail & consumer packaged goods, public sector, transportation, and defense. He holds PMP, CISSP, and ITIL certifications and specializes information security strategy and operations. His work has centered on partnering with clients to design governance, risk, and compliance solutions for their business security challenges.

Kelli Klindtworth
Kelli.Klindworth@northhighland.com

Kelli is an expert change, people, and culture consultant with over 15 years of experience. Her areas of expertise include human capital management, cultural transformation, process improvement, IT implementation, and program and project management. She has worked across many industries including retail, technology, financial services, and education. Kelli passionately believes in the importance of culture to help shape and transform organizations to achieve their highest potential.

northhighland.
WORLDWIDE CONSULTING