COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

The HR Professional's Guide to a Cyber-Secure Workforce

Introduction

Cybersecurity is one of the most important aspects of managing the modern enterprise, with duties and responsibilities extending through every level of the workforce. The central nervous system of any organization[i]—its data, systems and infrastructure—depend not just on secure technology but also on the quality and skills of the people entrusted with managing and operating it. As a human resource (HR) professional, you play a critical role in ensuring that your organization is prepared to manage escalating operational, financial, reputational, and legal risks related to cyber attacks through effective workforce planning and management.

Cybersecurity is no longer just an information technology (IT) issue; it is an enterprise-wide issue with implications for everyone. Cyber risk is now one of the top concerns for board directors and executives as they manage the full spectrum of enterprise risks[ii]. HR has always had an important role in managing risks—from natural disasters to layoffs, lawsuits, and workplace violence—and cyber risk is no different: you have a role to play.

A human capital crisis

The stakes are high. For individual companies, the global average annualized cost of cyber incidents stands at $7.7 million, although in many regions, such as the United States (at $15.4 million), the average costs are higher, and many individual companies must bear costs much greater still[iii], while an estimated 80% of the value of S&P 500 companies is based on intellectual property[iv]—which is often vulnerable to cyber attack. More broadly, the critical infrastructure we all depend upon for daily life—from electricity and water to emergency response services—are increasingly dependent upon interconnected IT, and thus vulnerable. Indeed, cyber attack has risen to become a top national security concern, according to the senior American intelligence official[v]. At the same time, there is a critical shortage of people with the requisite knowledge, skills and abilities to address emerging threats.

The shortage of cybersecurity talent is unique in its intensity, scope and potential impact. The speed at which the world became connected through the Internet—from individuals to organizations—far outpaced the ability to produce professionals who can adequately secure the data, systems and critical infrastructure that is now dependent on it. Traditional sources of professional talent, such as four-year universities, are lagging far behind.

This is a problem of global proportions. There is already a shortage of over one million professionals[vi] worldwide, and the gap is expected to widen to more than 1.5 million by 2019[vii]. In the United States alone, there are nearly 250,000 postings annually for cybersecurity-related jobs, many of which go unfilled[viii]. This shortage is exacerbated by a lack of clarity and consistency in competency models, job descriptions, and certification, training and education standards for cybersecurity professionals. Finding the right talent will be a challenge for years to come.

And the problem is not limited to cybersecurity-specific roles, or even the broader category of IT roles. An organization's greatest vulnerability remains its own workforce[ix], so even if all needed cybersecurity roles were filled, the enterprise would still be open to exploitation. In other words, effectively managing the *entire* workforce with cybersecurity in mind is essential.

As an HR professional,[x] you are the key resource in workforce management, and therefore essential to cybersecurity. You don't need to become a technical expert, but you *can* contribute in a meaningful way. This paper provides an introductory set of guidelines and considerations to help you get started.

What "Good" looks like

It's important to begin with an understanding of what an enterprise looks like when its workforce is optimized for cybersecurity. In a cyber-secure enterprise:

- The people responsible for tools and technology are given *proper (but limited) authorities* to access and protect data and systems
- The organization has the *right governance structure* to balance its business objectives with security needs as part of overall enterprise risk management
- The organization has clear and broad *consensus on the cybersecurity risks* that are most important to the business and industry in which it operates
- Security is a broadly-understood priority, with leaders building a *cybersecurity culture* where the right behaviors are encouraged
- The *right people*—with the right competencies and capabilities—are available to support the enterprise
- These people are deployed to the *right places* within the organizational structure
- The entire workforce is doing the *right things* to be resistant to exploitation of human vulnerabilities, which typically represent the biggest risk to any organization

This can't be accomplished without a close alignment between two frequently disconnected things: workforce management and cybersecurity strategy. HR

professionals like you can leverage your position and apply your expertise in the following ways:

Collaborating with senior management

- Actively participate in the cybersecurity planning process from the outset by attending meetings, observing, and offering input on workforce matters—*this will help you understand what you're planning for and how cyber risk is being addressed*
- Ensure appropriate leaders from IT, operations, legal and finance are involved in the workforce planning that you're guiding from the outset—*this will help you capture the input of the functional areas which impact security*
- Seek the support of senior leadership to drive active participation in this effort—this mitigates the risk of "stovepipe" views of departmental needs which undermines integrated planning
- Establish a cross-functional committee or work group with representatives from key departments and functional areas to integrate their perspectives and address their needs

> ***Key Question:*** *Are you starting at the right place?*
>
> ***Yes,*** *if cybersecurity strategy is the basis for a holistic workforce plan*
>
> ***No,*** *if your plan is based only on the staffing requests of each department*

Taking a holistic approach to workforce planning

- Ensure workforce planning considers *all* roles in the organization:
  - All *technical roles* involved in cybersecurity, regardless of organizational placement—this includes the IT department, as well as technical roles embedded within business units (such as developers or engineers)
  - All *non-technical roles* involved in cybersecurity, regardless of organizational placement—this ranges from procurement managers (who need to buy relevant products and services) to lawyers in the legal department (who need to understand regulatory compliance and privacy protection)
  - *Management* responsibilities—including workforce training and education, security culture and incentives for cyber hygiene (basic behaviors to reduce vulnerability)

> ***Key Question****: Is everyone who is supposed to be involved in cybersecurity included in the plan?*
>
> ***Yes,*** *if a broad mix of technical and non-technical roles from across the enterprise are included*
>
> ***No,*** *if it's mostly an "IT" or "cybersecurity" plan*

- *Partners and suppliers*—this includes roles which oversee the sharing of data and systems (such as procurement or project management applications) with partners and suppliers

- Learn more about workforce planning by exploring the Department of Homeland Security (DHS) resource, *Best Practices for Planning a Cybersecurity Workforce White Paper*

Understanding specific needs

- Build partnerships with cybersecurity professionals (on staff or from external providers) to understand specific staffing needs—including roles, responsibilities and requisite knowledge, skills, and abilities—related to cybersecurity
- Learn the basic needs for certifications and other advanced training by working with your cybersecurity leaders

***Key Question**: Is your plan based on independently-validated best practice?*

***Yes,** if it is based on prioritized actions like the CIS Critical Security Controls*

***No,** if your plan only references compliance regimes, such as PCI and HIPAA*

- Work with your colleagues to assess the competencies and capabilities of the existing workforce against the needs identified above
- Perform a gap analysis to identify the roles and responsibilities which are not appropriately filled already
- Use existing frameworks and toolkits, such as the National Cybersecurity Workforce Framework developed by the National Initiative for Cybersecurity Education (NICE) at NIST, DHS' *Cybersecurity Workforce Development Toolkit*, and the Council on CyberSecurity *Cybersecurity Workforce Handbook*

- Recognize that demand forecasting must be based on an overall enterprise-wide cybersecurity strategy, not merely the sum of staffing requests from various departments, because cybersecurity is not merely an *intra*-departmental function, but an *inter*-departmental, *enterprise-wide* function!

Closing the gap

- Draft a workforce planning map[xi] specific to your enterprise, placing cybersecurity roles where they need to be within the organizational structure and delineating appropriate (and limited) authorities for each role

- Identify positions most critical to enterprise security and which require the most sophisticated technical knowledge and experience[xii]—this list can be used to prioritize budget and talent acquisition efforts
- Work with managers to develop a staffing plan, considering the different sources of talent:
  - Directly hire and manage staff (insourcing)
  - Contract for a set of individuals to be provided by a third party, but managed by the organization's own staff (staff augmentation)
  - Contract for services to be provided by a third party which manages its own capabilities, staff and assets (outsourcing)

> ***Key Question:*** *Do you clearly understand who is accountable for what?*
>
> ***Yes,*** *if job descriptions include specific responsibilities and reporting requirements for data and systems*
>
> ***No,*** *if cybersecurity is assumed or implied*

- Collaborate with other leaders to determine the best mix of talent sourcing, considering financial, operational and other factors
  - For most small and medium-sized businesses, cybersecurity functions will need to be performed by third parties, since in many cases much of the IT infrastructure is outsourced
- Explore creative ways to source talent internally—many of your current employees may have abilities and affinities fit for cybersecurity, and can become productive contributors if provided the right training and development
- Consider a broad range of incentives to hire the best talent—while compensation continues to rise for cybersecurity professionals, many of them are also attracted to other incentives such as training and education subsidies, flexible work arrangements, and leadership development opportunities

> ***Key Question:*** *Do you know who's going to be doing what?*
>
> ***Yes,*** *if you have a clear delineation of what is done "in-house" and what is done by a third party*
>
> ***No,*** *if talent sourcing remains vague*

- Engage the *entire* workforce to secure the enterprise by working with management to drive awareness and increase cyber hygiene as part of a strengthened security culture[xiii]

Becoming a cyber-savvy HR professional

While you don't need to know everything about cybersecurity, you *do* need to be a "smart user" of IT and cybersecurity. To be an effective member of the management team, *all* leaders need to have a foundational understanding of the major functional areas of the business, such as finance, operations, business development, and (of course) HR. The same is now true for cybersecurity, and it applies to you as an HR professional. It also means doing your part to secure data and systems—especially those pertaining to sensitive personal information and employee records. This can be

accomplished through a variety of controls, from restrictive account access (through multi-factor authentication, role-based permissions and least privileged user) to data encryption and regular log reviews.

To implement these controls, and become more knowledgeable in general, you can reference foundational frameworks such as the *Cyber Security Framework* (CSF) developed by NIST, and the *CIS Critical Security Controls*, which are a set of independently validated best practices for securing enterprises. There are also resources specific to workforce management, including the National Initiative for Cybersecurity Careers and Studies (NICCS) portal and the aforementioned *Cybersecurity Workforce Handbook*.

This is an opportunity for you to contribute in a real way to the organization and its leadership. If it hasn't happened already, it's a matter of time before cybersecurity becomes a hot topic at your office. Cyber attacks plague enterprises of all sectors, industries and sizes—a quick glance at the news is evidence enough. Take a proactive approach to help your enterprise operate securely and effectively in the digital world—now and in the future.

About the Council on CyberSecurity: The Council on CyberSecurity is an independent, expert, not-for-profit organization with a global scope committed to the security of an open Internet. The Council is committed to the ongoing development and widespread adoption of the Critical Security Controls, to elevating the competencies of the cybersecurity workforce, and to the development of policies that lead to measurable improvements in our ability to operate safely, securely, and reliably in cyberspace. In 2015, the Council on CyberSecurity integrated with the Center for Internet Security. To learn more please visit http://www.CISecurity.org or follow us at @CISecurity.

Authors & Contributors: This paper was produced by the *Roles & Controls Panel* convened by the Council, a voluntary group of cybersecurity and HR experts from government, industry and academia, representing a diversity of perspectives. Principal authors were Roger M. Callahan, Managing Director, Information Assurance Advisory, LLC; Rebecca Slayton, Assistant Professor, Cornell University; and Maurice Uenuma, Vice President, Center for Internet Security. Contributors and reviewers included Vilius Benetis, CEO, NRD CS; Tom Brennan, ProactiveRISK; Carolyn Comer, Director of Human Resources, Center for Internet Security; Karen Evans, Partner, KE&T Partners, LLC and National Director, US Cyber Challenge; Jeremy Grant, Managing Director, The Chertoff Group; Geoff Hancock, CEO, Advanced Cybersecurity Group; James Harris, EVP/CTO Nelson Harris, LLC; Jim Michaud, Director, Cyber Talent Solutions, The SANS Institute and Adjunct Professor of Human Resources, Michigan State University; Karl Perman, Vice President, EnergySec; John Salamone, Vice President, Federal Management Partners; Benjamin Scribner, DHS Program Director for National Cyber Workforce Development; and Dale Young, Executive Director, Human Resources – Dell Global Services Infrastructure and Cloud Computing.

Support was provided by the Department of Homeland Security, HSARPA, Cyber Security Division, through a cooperative agreement with the Air Force Research Laboratory: This material is based on research sponsored by Air Force Research Laboratory under agreement number FA8750-12-2-0120. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

[i] Throughout this paper, the terms "enterprise" and "organization" are used interchangeably, as the topic applies to government, commercial and non-profit entities across all sectors
[ii] According to "Executive Perspectives on Top Risks in 2015," by North Carolina State University's ERM Initiative and Protiviti, at http://www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2015.pdf
[iii] According to "2015 Cost of Cyber Crime Study: Global" by the Ponemon Institute, at http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/
[iv] Ocean Tomo, LLC, at http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/
[v] As reported by the Washington Times, at http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/?page=all
[vi] As noted in the 2014 Cisco Annual Security Report, at http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
[vii] As noted in the 2015 (ISC)² Global Information Security Workforce Study, at https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf
[viii] According to "Job Market Intelligence: Cybersecurity Jobs, 2015," by Burning Glass Technologies, at http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[ix] As noted in the 2015 Verizon Data Breach Investigations Report, at http://www.verizonenterprise.com/DBIR/2015/
[x] Throughout this paper, the term "HR professional" refers to those individuals whose primary function involves HR competencies such as workforce planning, talent acquisition, training and development, compensation and benefits, labor relations, etc. and is interchangeable with similar terms such as "human capital professional"
[xi] Manpower Map, page 48, Cybersecurity Workforce Handbook at http://www.cisecurity.org/workforce/images/Workforce.pdf
[xii] Mission Critical Functions, at http://www.cisecurity.org/workforce/roles.cfm
[xiii] Security Culture, page 36, Cybersecurity Workforce Handbook at http://www.cisecurity.org/workforce/images/Workforce.pdf