Information Security Forum

BUILDING TOMORROW'S SECURITY WORKFORCE

With a dynamic threat landscape growing in sophistication and intent, expectations on information security are rapidly increasing. With limited personnel to manage the risk, attracting, recruiting and retaining a workforce presents a challenge for providing immediate and sustainable security.

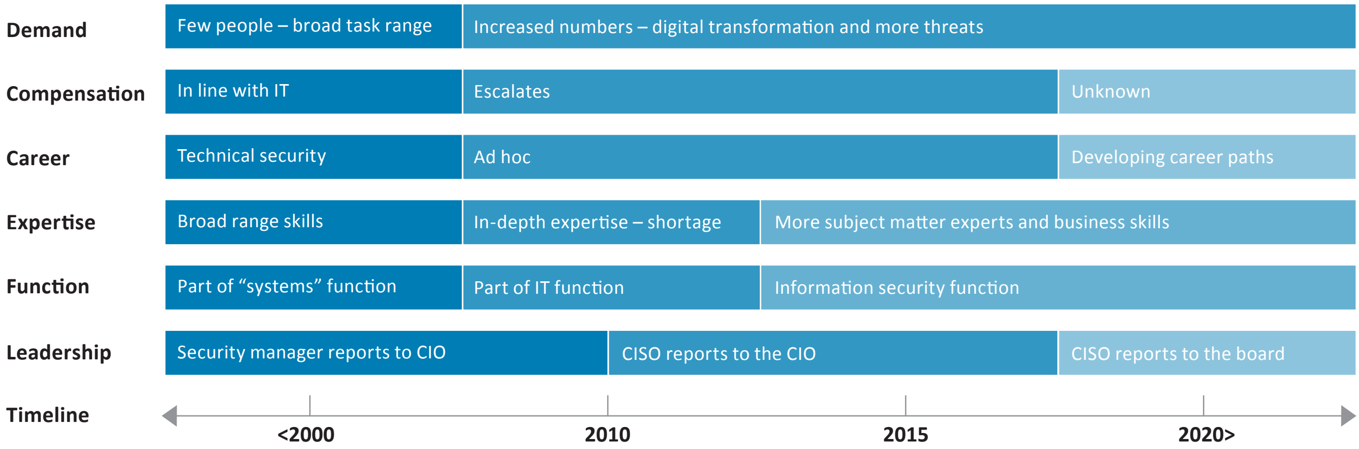
Shortfalls in skills and capabilities are manifesting as major security incidents damage organisational performance and reputation. Building tomorrow's security workforce is essential to address this challenge and deliver robust and long-term security for organisations in the digital age.

EVOLUTION OF THE SECURITY WORKFORCE

The security workforce has evolved rapidly since its inception, typically defined as the personnel responsible for the activities of an organisation's information security function. The information security function often exists only as part of another associated business function, such as: risk, technical IT operations, legal and or audit. It can be identified as information or cyber security, assurance or operational security; it can also report into various business functions, including: finance, risk, governance or IT.

Over the course of its evolution, the lack of an agreed definition of the information security function – its capabilities and workforce – has allowed numerous, disparate components to form an organisation's security workforce (e.g. employees working within threat intelligence, business continuity and security operations). These components rarely convene in one distinct function under a designated leader.

Figure 1: The general evolution of information security functions



Demand	Few people – broad task range	Increased numbers – digital transformation and more threats			
Compensation	In line with IT	Escalates			Unknown
Career	Technical security	Ad hoc			Developing career paths
Expertise	Broad range skills	In-depth expertise – shortage		More subject matter experts and business skills	
Function	Part of "systems" function	Part of IT function		Information security function	
Leadership	Security manager reports to CIO		CISO reports to the CIO		CISO reports to the board
Timeline	<2000		2010	2015	2020>

This paper uses the concept of the security workforce to reflect this diversity – encompassing all individuals who contribute to an organisation's information security, irrespective of functional designation or reporting line.

40% of ISF Members have increased their security workforce over the past two years, as roles and responsibilities within information security – from technical to strategic – expand.[1] However, this demand for staff has led to a predicted global shortage of 3.5 million cyber security workers by 2022.[2] At this juncture, organisations are struggling to align the security workforce with demand for services.

[1] The ISF Standard of Good Practice for Information Security (the Standard) provides a useful landscape of information security responsibilities, available on ISF Live https://www.isflive.org/community/compliance/standard-of-good-practice-for-information-security

[2] Herjavec Group, 2017, 2017 Cybersecurity Jobs Report, Cybersecurity Ventures, https://www.herjavecgroup.com/wp-content/uploads/2018/07/HG-and-CV-The-Cybersecurity-Jobs-Report-2017.pdf

SUPPLY AND DEMAND

Closing the gap between supply and demand is imperative for an enterprise to develop an effective security posture. With only 11% of ISF Members sourcing all information security professionals necessary, it is evident that individuals with the required skills, qualifications and experience are either unavailable or demanding rewards that cannot be met from existing budgets: making regular moves to new employers as they seek out better rewards.

But is this inevitable? Does inflexible demand for candidates with specific skills and qualifications coupled with years of prior experience hinder rather than help? Do uninformed recruitment practices contribute significantly to the perceived shortage? As salaries escalate, organisations are urgently seeking a solution to the perceived crisis in supply and demand of information security professionals.

To address the growing demand, organisations should broaden their approach to recruiting security professionals from a diversity of backgrounds, disciplines and skill sets; focusing on the aptitude and attitude of candidates rather than insisting on a host of specific skills, experience and qualifications that would elude a large proportion of current and potential information security professionals.

3.5 million unfilled cyber security positions by 2021

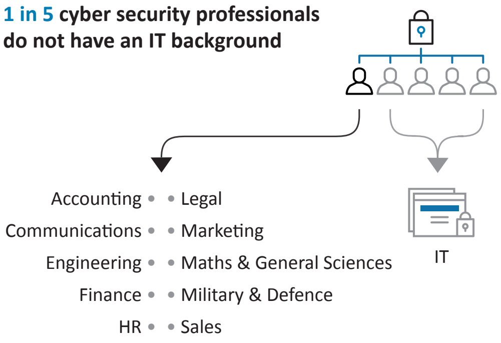
HUMAN-CENTRIC SECURITY

As vendors and tools saturate the market of security solutions, information security has acquired a deeply technical perception among potential employees, leaving functions struggling to recruit from beyond the technical skill set. Organisations are now swiftly recognising that individuals are one of the most valuable security capabilities to possess. A human-centric approach to information security will deliver a workforce that is capable of meeting the challenges presented by digital risk.

To help achieve a human-centric approach, the information security function should collaborate with HR to enable the security workforce to take advantage of well-established HR concepts, helping to efficiently build a diverse workforce with capable individuals.

A human-centric approach coupled with HR concepts provides the structure for a strong workforce culture underpinned with proficient and satisfied information security professionals.

Figure 2: The proportion of professionals with IT vs non-IT backgrounds

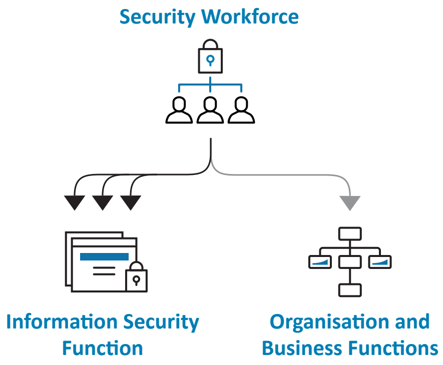


A COLLABORATIVE APPROACH

This paper helps organisations to focus on building the information security skills and expertise necessary to retain employees within a progressive, engaging and collaborative environment that satisfies career aspirations.

The paper also provides guidance on defining future expectations for the information security function, determining the implications on its workforce and positioning the organisation to implement a plan to move forward with confidence.

Figure 3: The security workforce


Security Workforce
Information Security Function
Organisation and Business Functions

Conclusion

Increasing reliance on digital systems coupled with a dynamic threat landscape has made the security workforce core to an organisation's survival. But for many enterprises, building a sustainable security workforce is only an aspiration: the pursuit of experienced, certified security experts has left organisations struggling to attract, develop and retain the necessary skilled individuals.

Organisations need to establish a series of strategic objectives that provide a foundation for building tomorrow's security workforce. With clear direction and leveraging fundamental HR concepts, organisations can develop an approach that formalises the structure of the security workforce, harnessing the appropriate talent and skills to achieve the organisation's security objectives.

As the security workforce matures, embracing the vast amounts of untapped talent with the right aptitude, attitude and experience, the exaggerated myth of a future global security workforce shortage will be debunked. A robust security workforce will also enable organisations to effectively manage future workforce challenges, such as automation, role and functional amalgamation and outsourcing. ISF Members are already demonstrating success, building tomorrow's security workforce with the necessary skills and expertise, developing and retaining employees in a progressive and engaging environment.

A sustainable security workforce is essential if the information security function is to become a partner to the business and effectively manage the increasing security burden.

WHERE NEXT?

The ISF encourages collaboration on its research and tools. ISF Members are invited to join the **People** community on ***ISF Live*** to share experiences and discuss practical approaches for building tomorrow's security workforce.

This is an excerpt from the ISF briefing paper ***Building Tomorrow's Security Workforce***. To purchase the full paper contact:

Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
steve.durbin@securityforum.org
securityforum.org

Building Tomorrow's Security Workforce
September 2018

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

WARNING

This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from the ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION

Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.

Information
Security
Forum

REFERENCE: ISF 18 09 01

©2018 Information Security Forum Limited. All rights reserved.