ISO/IEC JTC 1/SC 27/WG 1 "Information security management systems"
Convenorship: **BSI**
Convenor: **Humphreys Edward J. Prof.**

ISO Article (15th April) Cybersecurity Skills Gap

Document type	Related content	Document date	Expected action
General document / Other		2021-04-23	**INFO**

Description

This article was produced by ISO to support the work of PWI 27109

NEWS

THE CYBERSECURITY SKILLS GAP

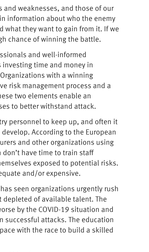
By Clare Naden on 15 April 2021

Why education is our best weapon against cybercrime.

The Internet has been one of the biggest winners in the past year's pandemic, with traffic and transactions reaching unprecedented levels in 2020. Unsurprisingly, the number of malicious attacks and activity has risen with it. According to INTERPOL Secretary-General Jürgen Stock, "cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19".

Coming at a time when estimates state that up to 3.5 million cybersecurity jobs will go unfilled this year, this is bad news. Are we losing the battle? Upskilling those already in the cybersecurity industry and enticing newcomers to join is our best defence, but programmes and schemes are piecemeal, and not enough.

We sat down with world-renowned IT security specialist Dr Edward Humphreys to discuss concerns about the cyber-skills shortage and its potential implications for business and society. Dr Humphreys sits on a number of committees run jointly by ISO and the International Electrotechnical Commission (IEC), including ISO/IEC JTC 1, *Information technology*, subcommittee SC 27, *Information security, cybersecurity and privacy protection*, which has over 200 published standards and a further 77 in development. An expert in his field, he is often quoted as the "father" of the ISO/IEC 27001 family of standards for information security management systems.



Q&A

DR EDWARD HUMPHREYS

Convenor of working group ISO/IEC JTC 1/SC 27 WG 1, *Information security management systems*

Cybersecurity is a constant battle, with demand for cyber talent continuing to rise and outpace supply. Where does the situation stand today?

ISO / DR EDWARD HUMPHREYS

It is useful to quote some ancient wisdom on battle strategy. This quote is often used today in various educational and training settings for professionals in many fields, including management, business negotiations and, of course, cybersecurity.

> If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.
>
> — Sun Tzu, *The Art of War*

The more information we have about our strengths and weaknesses, and those of our enemy, the better prepared we are. We need to gain information about who the enemy is, why, when, how and what they might attack and what they want to gain from it. If we know ourselves and our enemy well, we have a high chance of winning the battle.

Having a cyber-aware workforce with skilled professionals and well-informed employees puts us in a good position. This means investing time and money in cybersecurity education, training and awareness. Organizations with a winning strategy for cybersecurity are those with an effective risk management process and a skilled cybersecurity workforce. Taken together, these two elements enable an organization to assess its strengths and weaknesses to better withstand attack.

There's a drastic worldwide shortage of skilled experts in this area. Why is this?

Technology keeps changing, so it's hard for industry personnel to keep up, and often it requires specialized knowledge that takes time to develop. According to the European Union Agency for Cybersecurity (ENISA), manufacturers and other organizations using Industry 4.0 and Internet of Things solutions often don't have time to train staff adequately before things change again, leaving themselves exposed to potential risks. What's more, the training that is available is inadequate and/or expensive.

Over recent years, the escalation of cyber-attacks has seen organizations urgently rush to recruit skilled professionals, leaving the market depleted of available talent. The need and urgency to take action has been made worse by the COVID-19 situation and the wake-up call resulting from the dramatic rise in successful attacks. The education and training of cybersecurity talent have not kept pace with the race to build a skilled workforce.

The reasons for this shortage are many and various. At the formal educational level (university, college), the take-up to do cybersecurity as a qualification has been steadily growing over the past decade or so, but the numbers graduating still fall way short of industry demand. It takes time to educate and train highly skilled professionals, and time to gain practical working experience. Meanwhile, investment in cybersecurity training has been severely hampered as budgets for items of expenditure not directly related to profits and revenue earning have been cut or reduced.

What does this mean for our future if nothing more is done?

The worldwide shortage of skilled cyber personnel has a direct and significant impact on organizations and their ability to protect themselves. And this collectively adds up to an appreciable threat to a nation's overall economic well-being and, by extension, that of society.

The problem covers at least three areas of concern:

- Skilled professionals to manage, administer and support organizational security and operations
- Skilled cyber-engineers to design security systems and develop secure software and tools
- General cybersecurity awareness at every organizational level so that everyone has a baseline knowledge of the threats and risks, and what this means in the context of each and every individual's job function

The growth in the use of the Internet and online services, the introduction of new technologies and the rapidly changing digital landscape compounds the need for better cybersecurity. The desperate shortage of cyber-skilled professionals will clearly hold back progress in achieving adequate and effective protection.

If the global shortage of a skilled cybersecurity workforce continues, organizations will find it more difficult to be on the winning side of the battle. The future outlook will be one of increasing exposure to cyber-attacks resulting in heavier financial losses, greater disruption to operations, interruption of services and supply chains, compromising of personal privacy and safety, and many other impacts.

What initiatives are underway to try and encourage cyber talent to fill the widening skills gap?

ENISA advocates cross-functional knowledge on IT and OT security and to further the training and education offering. It has placed capacity building as a key objective in its new strategy and is doing lots of awareness-raising activities with consumers to promote safer online behaviour. It is also promoting and analysing cybersecurity education in order to tackle the cybersecurity professional shortfall, which represents an issue for both economic development and national security.

There are a number of cybersecurity career awareness campaigns in countries such as the US and the UK, but the promotion of these campaigns is fragmented and there is nothing that is internationally harmonized.

Some countries have established programmes to consider the problem. These include national awareness campaigns encouraging universities, colleges, schools and training organizations to promote the take-up of cybersecurity as a field of study. In Canada and the UK, for example, cyber education is starting to be introduced in schools for children as young as eight years old. This is reassuring as we need to build future generations of cyber-skilled talent.

You are currently working on a new standard to address education in the cybersecurity industry. How is it intended to help?

One of our working groups has begun developing a technical report for cybersecurity education and training. When it is published, it will outline the why, what and how of cyber education and training to help improve the current situation.

This new technical report will provide insight into why cybersecurity education and training are important and how they are essential to building a well-informed and competent workforce that can protect business and society. It also brings home why cybersecurity education needs to be made a strategic priority in workforce development within organizations and government, across all business sectors.

The guidance will list what is available with regard to national programmes and initiatives, formal education, professional training, standards and guidelines. Thus, it can be used to identify areas for improvement and further development. It will also go into specialist areas of cybersecurity education that are critical to ensure effective cyber protection.

Who is this document aimed at and when can we hope to use it?

The document is intended to be useful to anyone involved in cybersecurity: users, suppliers, certifiers, policy makers and regulators, educationalists, consumers, vendors and manufacturers. We expect to see it published at the end of 2021 or early 2022.

What can organizations do in the meantime to protect themselves?

One of the key actions that organizations must take is to fully understand the risks they face, and to apply a baseline of controls to try and mitigate these risks. ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*, provides a set of controls that are derived from industry best practice; this fulfils organizations' need to build winning capability by understanding themselves better, as I mentioned at the beginning. The more they understand about the attacks they could face and what their weaknesses are, the better they can reduce them. The wisdom of Sun Tzu in *The Art of War* is just as applicable today as when it was first written.

THIS MAY ALSO INTEREST YOU

RELATED INFORMATION

ISO/IEC 27001 — INFORMATION SECURITY MANAGEMENT

Providing security for any kind of digital information, the ISO/IEC 27000 family of standards is designed for any size of organization.

STANDARDS

ISO/IEC 27002:2013
INFORMATION TECHNOLOGY
Security techniques
Code of practice for information security controls

COMMITTEES

ISO/IEC JTC 1 | Information technology

ISO/IEC JTC 1/SC 27 | Information security, cybersecurity and privacy protection

CONTACT

Clare Naden
+41 22 749 0474
naden@iso.org

Tags: Safety, security | Technologies | Business
Topics: Security