Chapter 13
A Holistic View of Cybersecurity Education Requirements

Steven M. Furnell
University of Plymouth, UK and Edith Cowan University, Australia

Ismini Vasileiou
https://orcid.org/0000-0001-6174-3586
University of Plymouth, UK

ABSTRACT

This chapter sets the scene for the book as a whole, establishing the need for cybersecurity awareness, training, and education in order to enable us to understand and meet our security obligations. It begins by illustrating key elements that ought to form part of cybersecurity literacy and the questions to be asked when addressing the issue. It then examines the problems that have traditionally existed in terms of achieving awareness and education, both at the user level (in terms of lack of support) and the practitioner level (in terms of a skills shortage). The discussion highlights the importance of a holistic approach, covering both personal and workplace use, and addressing the spectrum from end-users through to cybersecurity specialists.

INTRODUCTION

From office applications to social media, from electronic business to global communications, the rise of information technology and the Internet has offered numerous benefits to individuals and organizations alike. With all the positives to point at, it is sometimes easy (and certainly convenient) to forget the downside – namely that the technology that we now take for granted (and often depend upon) comes with associated risks. Systems can be attacked. They can fail. Data can be lost or exposed. Users themselves can be targeted. At the same time, cybersecurity is often assumed to be someone else's problem, with the consequence that the very parties that ought to have a stake in it end up distancing themselves from it instead. For example, end users frequently seem to assume that their employer, their Internet Service Provider, or some other party (*any* other party!) is taking care of their security needs. In reality of course,

DOI: 10.4018/978-1-6684-3554-0.ch013

they have a role to play as individuals, because no matter what steps may be taken elsewhere, there will be some threats that reach them directly. So, they will find themselves needing to make security-related decisions, and they clearly need a level of awareness and understanding in order to do so. Meanwhile, organizations may look at their employees and assume that they should already have acquired a level of general cybersecurity awareness from somewhere else. While this nicely excuses the organization from taking responsibility, it is often an entirely unrealistic stance. One of the key requirements is therefore for the various parties concerned to recognize their role and take ownership of it.

In fact, there is more to know at all levels of an organization, from the individuals who simply wish to use the technology, through to those that are tasked with providing the infrastructure and safeguards that enable them to do so securely. Indeed, a fundamental challenge is that we are not dealing with a one-size-fits-all situation. SETA needs exist at several levels, from users in personal settings, to users in a workplace context, and from technical specialists through to security professionals. As an illustration of how these levels may be split, and the requirements in each case, we can consider the following groupings:

- **Personal Users:** Need to understand how to protect their own data and use the associated technologies (devices and services) in a secure manner. They also need to be aware of why such protection is required.
- **Workplace Users:** Similar to the needs of personal users, other than the reason now relates to the need to protect workplace systems and data, in which they may not feel as directly invested.
- **Technical Specialists:** Refers to those responsible for designing, developing, implementing and running technology systems. There is a clear need for them to understand where security is required and how to deliver it.
- **Security Professionals:** Need a specific security skillset, which may be characterized and supported by specialist academic study and professional certifications.

These parties will develop and acquire their cybersecurity knowledge and skills in different ways and to different levels. Figure 1 presents a broad contrast between the paths that may be taken by general users versus those that become security professionals (noting that, for the cybersecurity professionals in particular, this is an illustration of a route rather than a prescription). For the former, one would hope that a general familiarity with cybersecurity issues would be developed during schooling, and then supported and supplemented by ongoing awareness-raising during any subsequent study and during their workplace life. This is intended to reflect that while they will not become in any way specialized in cybersecurity or technology more generally, they nonetheless need to have a credible understanding of the cybersecurity issues relating to them as individuals (and therefore require academia and employers to be playing their part in supporting this). Meanwhile, the path for security professionals is rather more focused. They would inherit the literacy and awareness aspects as lay users but would additionally be expected to have more specialized activities at each stage. For example, during schooling they may show a preference towards STEM (Science, Technology, Engineering and Mathematics) subjects, and then supplement this during higher education by opting for qualifications in subjects such as computer science or cybersecurity directly. Their workplace activity could then be supported by further specialized industry or professional certifications.