Journal of Learning for Development – JL4D
ISSN: 2311-1550
2020, Vol. 7, No. 2, pp. 261-263

# BOOK REVIEW

## An Introduction to Cyber Security for Busy People: How to be Safe and Secure in the Digital World

DR. DEREK W. KEATS

**Kenga Solutions, 2020, pp. 100**

The author of *An introduction to cyber security for busy people*, Dr Derek Keats, has worked in the information technology field for decades, and as he says, "since the days of punch cards". He has researched and published numerous academic papers on information technology and is a high profile technology and open source advocate. Dr Keates has for more than eight years been responsible for cybersecurity in two FinTech companies and is an active consultant in the cybersecurity field.

This book is short and purposefully presented as a quick read for those who need an overview on the topic of cyber security. Keats speaks about the threats users and organisations face, presents examples of typical threats and suggests ideas for preventing threats. His style is easy to read for the business and general reader and is not aimed at the IT specialist. It provides both a useful background and information to better position many people to know what questions to ask and how to understand the threats without being an IT expert.

Dr Keats provides an interesting yet brief history of the developments from early computers (of which he has personal experience) to modern global networks. His descriptions of examples of cybercrime do not stop at only those committed online but also show how crimes in the analogue world (the physical world we live in) can impact the online world.

Relating to the protection of critical personal and business data, Dr Keats uses the acronym "CIA", or Confidentiality, Integrity and Availability. Good cyber security needs to protect all three of these. He goes on to explain how vulnerabilities in computer software can be exploited by cyber criminals and become a threat. Readers learn how to apply the principle of minimising the "attack surface" so as to reduce the chances of being attacked.

Descriptions are included of a wide range of attacks that may crop up in conversations, especially when IT people are present. A basic knowledge of the terms and what they mean can be extremely helpful to the non-IT person when in conversation with IT specialists.

Even though one may add many software protections to a computer, users need to be especially aware of the physical security of devices. The number of computers, smartphones and other devices that are stolen each year must support an army of equipment sellers and re-sellers.

Dr Keats introduces readers to a conceptual framework for planning called "VPPTF" or Vision, Process, People, Technology and Finance. A focus on technology can lead one to ignore other aspects. Vision refers to the vision a person or organisation has for cybersecurity and how to prevent, contain and recover from breaches. Processes refer to what is in place to deal with cybersecurity threats. People are those who are assigned to cybersecurity roles. Technology tools refer to the kinds of hardware and software we are spending money on. Aare they the right tools? All this needs to be budgeted for (finance) and managed by adequately skilled personnel.

If skilled people are empowered to protect an organisation's digital assets, they will ensure that the most appropriate available administrative, physical and technical controls are in place. If your organisation does not yet have a person who has cyber security as a key focus area, you need to review the situation urgently. That person should be able to create a defence in depth approach and implement technologies to help reduce the risks to your organisation. The book provides an outline for a simple and basic attack prevention approach that can help the non-IT manager hold the much-needed discussion with IT specialists.

Some of the simplest checks individuals need to perform are to see what the administration login passwords are for devices around the house, such as WiFi routers. These are often set to "admin", "administration" or "password" which any mischievous person nearby can exploit and potentially make changes to your home IT system. One of the most common ways for your personal computer to become infected is via the clicking of links in emails or by plugging in other people's USB memory sticks ("thumb drives").

Dr Keats recommends implementing incident management, including these processes: (1) Prepare and plan; (2) Detect, alert and report; (3) Assess and decide; (4) Respond; (5) Learn and record. This would help to create constant learning opportunities and continue to build the organisation's cyber defences.

Dr Keats is a well-known supporter of open source and so readers can expect to hear about the use of the Linux operating system from time to time throughout the book. The book is well illustrated to help readers visualise the concepts. Dr Keats is a strong supporter of the Free and Open Source Software (FOSS) movement and user of Creative Commons copyright licenses.

Basic computer literacy is a minimum requirement these days and will become even more essential as the so-called Fourth Industrial Revolution settles in around us in the workplace. It is no longer enough to accept digital illiteracy for oneself while expecting others (such as students and subordinates) to be digitally literate and fluent. Saying "I just want it to work" to another person without having a working level of digital fluency is no longer acceptable. If you feel left behind, it is time to make the effort and become digitally fluent if you wish to remain in the current and future workforce. Personal cyber security is an important aspect of being digitally fluent.

One of the reasons for a lack of cyber security in organisations may be the inability of management to come to terms with the extent of the effort required to develop, run and keep safe the IT systems that everything depends on. Perhaps if senior managers equipped themselves with the necessary digital skills, they could reduce the risk to the organisation of IT system failures and attacks. The reviewer has heard there are two kinds of organisations — those that have been hacked and those that are still going to be hacked. Managers who have not gained a good understanding of their digital environment can look forward to a possible future of being hacked!

Dr Keats runs a website and consulting company that provides services in IT, Kenga Solutions:

https://kengasolutions.com

**Reviewed by:**

**Mr Paul West** is an Independent Consultant and Senior Advisor in Distance Education, Open Learning, Knowledge Management, OERs and Project Management. Email: pgwest@pgw.org

Cite this paper as: West, P. (2020). Book Review: An introduction to cyber security for busy people: How to be safe and secure in the digital world. Derek W. Keats. *Journal of Learning for Development, 7*(2), 261-263.