JESSICA BARKER

CONF!DENT CYBER SECURITY

HOW TO GET STARTED IN CYBER SECURITY AND FUTUREPROOF YOUR CAREER

First published in Great Britain and the United States in 2020 by Kogan Page Limited

2nd Floor, 45 Gee Street
London
EC1V 3RS
United Kingdom

122 W 27th St, 10th Floor
New York, NY 10001
USA

4737/23 Ansari Road
Daryaganj
New Delhi 110002
India

www.koganpage.com

ISBNs

Hardback	978-1789663426
Paperback	978-1789663402
Ebook	978-1789663419

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library.

Library of Congress Control Number

2020941948

Typeset by Integra
Print production managed by Jellyfish
Printed and bound by CPI Group (UK) Ltd, Croydon CR0 4YY

CONTENTS

ACKNOWLEDGEMENTS

Many people have helped and supported me whilst writing this book and I'm grateful to each and every one of them. First and foremost, to my husband FC, for his enormous help and support not just in writing this book, but in everything I do. He's my biggest champion and I'm grateful for that every day. I'm lucky to have a wonderful family – thanks to my Mum and Dad, Sue and Richard, and my brother, Danny, and his wife, Lucy. And, of course, Bubble the cat has been an unwavering cheerleader.

Thanks to the team at Cygenta – not just FC but also Madeline, Richard, Natalie and Dave – for being so helpful, and so patient, while I've been juggling this and the business. Thanks to all of my lovely friends, including those on Twitter, who have cheered me on from the sidelines. I've already mentioned Natalie, one of my oldest and dearest friends, so I must thank the others, or I'll be in trouble. Catriona, Aleyna, Laura and of course Kat, who started me down this path (I've just about forgiven you!).

This book features many amazing contributors and I really appreciate everyone who has shared their stories and their insights. Thanks to my fellow board members, and the whole membership, of ClubCISO for their moral support. In particular, I would like to thank Rob Bainbridge for sharing his time and expertise. I am grateful to Professor Peter Batey, whose red pen and counsel have continued to stand me in good stead ten years after finishing my PhD.

Special thanks to my editor at Kogan Page, Rebecca Bush, whose patience, professionalism and positivity throughout has been instrumental in completing this book. I'm grateful to the whole team at Kogan Page for making this book possible.

And, finally, to Yorkshire Tea. I could have done it without you, but it would have been much harder.

THIS PAGE IS INTENTIONALLY LEFT BLANK

An introduction to cyber security

'You can't work in cyber security unless you are very technical.'

'Users are the weakest link in cyber security.'

'Hackers are all criminals!'

'Cybercrime is targeted. It's only the concern of governments and big business.'

'No one would target me; my data is not worth anything!'

These myths, and many more, plague cyber security. In this book, we will see why all of the above statements are false. We will demystify cyber security, and show the breadth and depth of the field; how it encompasses not just computer science, but also psychology, sociology, physical security, behavioural economics, marketing, design, education and much, much more.

Cyber security is a topic that cuts across pretty much every area of life. Government, healthcare, politics, fashion, sports, the media, big business, small business, charities, education – you name it, it is affected by cyber security. It is a fascinating, challenging, fast-paced field that changes every day, but at the same time is concerned with issues that have been a part of human life for centuries. In the last few years, awareness has grown phenomenally. Cyber security issues make national news on a seemingly daily basis, and it has become a boardroom and household subject of conversation.

Having been working in this industry for nearly ten years, I've witnessed this rise in awareness alongside a growth in understanding

of the diversity of the topic. I have always worked on the human side of cyber security; I am passionate about raising awareness of cyber security, positively influencing people's behaviours online so they operate in a more secure way, measuring and advancing organizational cyber security culture, and translating technical messages for a non-technical audience. When I started in the field, this was very much a niche area of the industry and I would frequently have to explain to my peers in the community what it meant to work on the human side, and why people are an important dimension of this field. That is no longer the case: working on the human side of cyber security has become pretty mainstream within the industry. There has been an explosion in understanding that people are a fundamental part of cyber security, whether from the perspective of analysing the motivations and profiles of cybercriminals to designing security products to be more user-friendly, from recognizing what makes us so susceptible to social engineering to how we can better-communicate cyber security messages to be more mindful of pedagogy.

When I was a teenager in the early 1990s, first experiencing the internet, I would never have expected that I would go on to have a successful career in a technology field – let alone the field of cyber security itself. This was, understandably, not even remotely on the radar of my school's career guidance professional. I was interested in technology, a little, but I didn't think I was capable of a career there. I was more interested in people, and disciplines related to understanding themes of society: history, English literature and sociology.

Later, having finished my PhD and not knowing what to do, I was headhunted by a cyber security consultancy. I had no idea what cyber security was or how someone who saw themselves as non-technical could be relevant to the field, but I was keen to find out. The UK Government had not long since released their strategy on cyber security and it was obvious that it was becoming more of a priority for them. The role was to involve carrying out cyber security assessments of organizations, and interviewing people about how they work with technology and understand risk – so the skills

I had developed during my academic career were relevant. I was ready for a change, and excited to learn something new, so I took the job.

Entering the field of cyber security is a steep learning curve. However, what I immediately loved about the subject is how much there is to learn and how new challenges can emerge every day. This is one of the many things I still love about working in this industry: no two days are the same and being bored isn't much of an option. I quickly began to understand how my work before entering cyber security was relevant – people are easily as central to this discipline as technology.

The history of cyber security

The history of cyber security starts many years before the invention of the computer. Encryption – a system of encoding data to prevent prying eyes from reading it – is often assumed to be so entwined with computers that we can forget that this cornerstone of cyber security is thousands of years old. It is claimed that Histiaeus, a Greek ruler in the 6th century, tattooed a military message on the shaved head of a slave before waiting for the hair to grow back and sending the slave to his ally with a message to remove his hair and read the secret missive.

Julius Caesar is credited with inventing one of the first encoding systems, aptly called the Caesar cipher or Caesar shift. The Caesar cipher is very simple compared to the encryption mechanisms we have in place now, but at the time was revolutionary. It is a substitution cipher in which each plaintext letter of a message is replaced by a letter a fixed number of positions down the alphabet. So, if there is a rotation right 4, A would become E, B would become F and so on.

For example, if we are going to encode the words 'shift example' and shift four to the right, it would become 'wlmjx ibeqtpi'. This is illustrated in the wheel below.

Different rotations give different encodings. Try to decode this phrase, which has been encoded using a Caesar cipher (tip: you will need to work out the rotation number first): 'Guvf vf na rknzcyr bs n Pnrfne pvcure. Jryy qbar sbe qrpbqvat vg!'.

The answer is on page 230.

To cover the entire history of cyber security would take a whole book, or even several books – and we don't need to know *absolutely everything* in order to develop in-demand cyber security skills. Table 0.1 provides a quick timeline: this covers some of the key points in the evolution of information security.

0.1

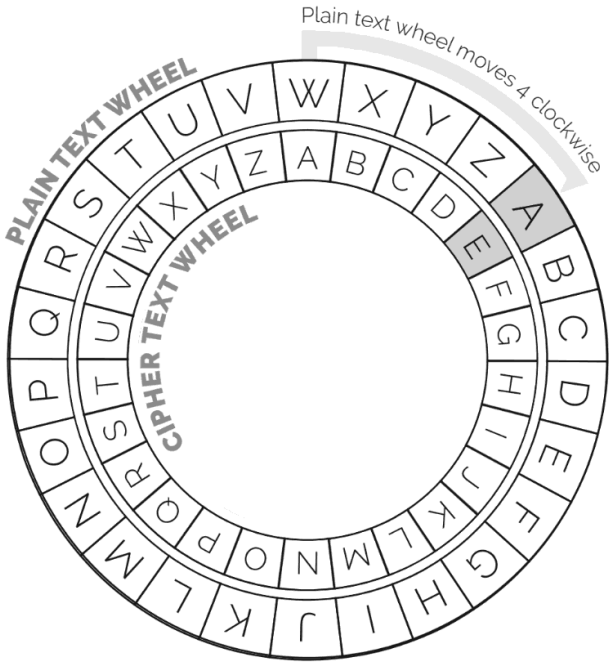

Table 0.1 Cyber security timeline

c.50 BC	Julius Caesar creates the Caesar cipher
1903	Nevil Maskelyne breaks into a demonstration of Marconi's wireless telegraphy, to highlight it is not secure and private
1916–18	Enigma cipher machine invented by German engineer Arthur Scherbius. The encryption device is used extensively by Nazi Germany in the Second World War
1932	Polish cryptologists Marian Rejewski, Henryk Zygalski and Jerzy Różycki break the Enigma machine code, enabling the Polish Cipher Bureau to read German Enigma messages from 1933
1939	Alan Turing creates the Bombe computer at Bletchley Park in the UK, developed from a device made by the Polish Cipher Bureau; the Bombe helps decipher German secret messages, encrypted using Enigma during World War II
1943–45	Tommy Flowers designs Colossus, widely regarded as the world's first programmable, electric, digital computer
1949	The paper 'Theory and organization of complicated automata' by John von Nuemann outlines self-replication of computer programs
1940s	The American mathematician Norbert Wiener uses the term 'cybernetics' to mean 'control or communication theory, whether in the machine or in the animal'[1]
1955	The word 'hack', to mean messing around with machines, is coined at the MIT Tech Model Railroad Club
1957	Josef Carl Engressia ('joybubbles'), a blind 7-year-old boy with perfect pitch, can whistle 2600 mhz, which is a tone that can control American telephone systems; alongside John Draper, he starts the Phreaking scene
1961	MIT's Compatible Time-Sharing System (CTSS) requires users to log in with a password; in the 1960s passwords start to be used on other computer systems

(*continued*)

Table 0.1 (Continued)

1970s	The Advanced Research Projects Agency Network (ARPANET) is invented, a precursor to the internet
1971	Ray Tomlinson is credited with inventing email, after implementing the first email program on ARPANET
1971	Creeper, the first computer virus in history, spreads the message 'I'm the creeper, catch me if you can' over ARPANET computers; the virus is harmless, created by Bob Thomas to test his theory that programs could be moved across computers
1971	Reaper is developed in response to Creeper (it is not known who created it; some claim it was Bob Thomas himself, whilst others credit Ray Tomlinson). Reaper detects Creeper on a computer and deletes it
1972	Rabbit, the first malicious virus, infects computers, reproduces itself and causes the system to crash
1981	*New York Times* reports on hackers and describes ethical hacking activities[2]
1982	The internet protocol suite (TCP/IP) is standardized, which enables worldwide proliferation of interconnected networks. Commercial internet service providers (ISPs) are set up in the late 1980s and early 1990s
1983	Six bills concerning cybercrime introduced in the USA after the activities of the 414s hacking group, the first widely recognized group of hackers
1984	*The Hacker Quarterly* is first published
1986	Clifford Stoll locates Marcus Hess using a honeypot; Hess had hacked into a network of US, European and East Asian military and industrial computers and sold the information to the KGB[3]
1986	US Congress passes the Computer Fraud and Abuse Act, making breaking into computers a crime

(*continued*)

Table 0.1 (Continued)

1985	Robert Schifreen and Stephen Gold arrested for hacking into a BT computer and accessing TeleCom Gold (an early email system) communications of Prince Philip; in 1986 they are convicted under the Forgery and Counterfeiting Act (the first people to be charged with forgery that deceived a non-human target) due to a lack of contemporary legislation in the UK against computer hacking
1988	The Morris Worm, written by Robert Morris, is one of the first worms distributed via the internet and spreads to over 6,000 of the approximately 60,000 computers connected to the internet at the time. Robert Morris is the first felony conviction under the US Computer Fraud and Abuse Act[4]
1988	Computer Emergency Response Team (CERT) formed at Carnegie Mellon University
1988	First CERT Advisory issued
1989	Sir Tim Berners-Lee invents the World Wide Web
1990	ARPANET decommissioned
1990	The UK introduces the Computer Misuse Act
Early 1990s	The first firewalls are used
1995	CVSSv1 is launched to rank computer system vulnerabilities (see Chapter 3 for more information)
1999	Mitre CVE list created to make it easier to share information on computer system vulnerabilities (see Chapter 3 for more information)
2003	OWASP top 10 first published, with the aim of highlighting information on the most critical computer vulnerabilities
2013	Edward Snowden leaks classified information from the US National Security Agency, revealing global surveillance programmes and techniques

(*continued*)

Table 0.1 (Continued)

2014	The UK launches its first CERT (CERT-UK)
2017	The UK National Cyber Security Centre is established, as the public-facing arm of GCHQ
2017	Wannacry ransomware spreads globally, with the cryptoworm targeting computers running Microsoft Windows operating system. A security researcher going by the handle MalwareTech stops the spread of the attack

The rise of cybercrime

During the 1980s, the growth of the internet meant that hacking became a worldwide subculture, but it was unclear how to deal with criminals that abused the systems already starting to appear.

In 1983, a group of six teenagers calling themselves the 414s (after their telephone code in Milwaukee) brought cybercrime to global attention. Neal Patrick, Timothy Winslow and four of their friends were young men who shared a passion for computers. When they discovered it was possible to remotely access a computer with a telephone modem, they would hack into the systems of organizations to access computer games on their systems. When they made it to the leader boards of the games, they would enter their '414' name. When they hacked into the medical company Sloan-Kettering, they noticed that all activity was being logged and so attempted to delete their tracks. They accidentally deleted more than they intended, including payment records of the company, which alerted an administrator at the company, who then contacted the FBI. The FBI lured the 414s back onto the Sloan-Kettering system with a honeytrap: a Star Trek game. When the 414s left their 'calling card', leaving their 414 tag on the game leader board, the FBI were able to trace the hack back to them. Without legislation

Part One
Why cyber security?

THIS PAGE IS INTENTIONALLY LEFT BLANK

01
What cyber security is

Cyber security has technically only been around for a few decades, yet it is now so mainstream that it's in the dictionary, defined as:

> Measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack.

Whilst the dictionary defines protection of *computers* as central to cyber security, I would argue that it is more precisely about protecting *information*. We're not protecting the computers, but what is on the computers (for example, confidential plans for a new product); what the computers provide access to (for example, your online banking); or what the computers are programmed to do (for example, operate power plants).

At first glance, then, cyber security might sound inherently and absolutely technical. This is certainly the popular image: a green screen of code, geeks in hoodies, blinking lights and neon streams of light. The reality is that, whilst technology is of course central to cyber security, the discipline is much wider than that. The types of jobs in the profession vary widely, from deeply technical to very much people-focused.

Here's why: technology does not exist in a vacuum. Technology is invented and developed by humans. Code is written by people – people who inadvertently create bugs that make technology vulnerable. People then interact with technology, and use it in ways it was not intended to be used. Then there's the physical aspect:

INDEX