

JESSICA BARKER

# CONFIDENT CYBER SECURITY

HOW TO GET STARTED  
IN CYBER SECURITY  
AND FUTUREPROOF  
YOUR CAREER



KoganPage

**Publisher's note**

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and authors cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the editor, the publisher or the author.

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

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licences issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned addresses:

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](http://www.koganpage.com)

© Jessica Barker 2020

The right of Jessica Barker to be identified as the author of this work has been asserted by her in accordance with the Copyright, Designs and Patents Act 1988.

**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* xiii

## **An introduction to cyber security** 1

The history of cyber security 3

The rise of cybercrime 8

Cyber security, you and your career 9

Notes 10

## **PART ONE** Why cyber security? 11

---

### **01** What cyber security is 13

The cyber security rainbow: Red, blue and purple 14

The cyber security spectrum: Who are the hackers? 18

Hacking and the law 20

Good hackers gone bad? Professional ethics in cyber security 21

Cybercrime 22

Case study: TalkTalk 23

Case study: SamSam 26

Malicious and non-malicious insiders 27

Case study: Andrew Skelton 28

Case study: Dow Jones and Facebook apps 30

Exercise 1.1: Assessing the risks 31

Notes 32

### **02** Why cyber security is important 34

Risks, threats and vulnerabilities 35

Risk assessment and management 36

Risk, threat, vulnerability and mitigations 38

Cyber security and the law 38  
Cyber security and personal lives 42  
Notes 43

## **PART TWO** The technical side of cyber security 45

---

- 03** **Technical vulnerabilities** 47  
Common Vulnerabilities and Exposures list 47  
Common Vulnerability Scoring System 48  
Open Web Application Security Project top ten 49  
Case study: TalkTalk 50  
Case study: WannaCry 54  
Case study: Life at Parliament View Ltd 56  
Exercise 3.1: Identifying vulnerabilities 57  
What technology is vulnerable? 57  
Notes 59

## **PART THREE** The human side of cyber security 61

---

- 04** **Why people are so important in cyber security** 63  
Design 64  
Creation 65  
Case study: The Big Hack 65  
Testing 66  
Use 67  
Case study: Amazon S3 68  
Abuse 77  
Destruction 80  
Notes 81

- 05 Social engineering** 84  
Social engineering red flags 84  
Social engineering through history 85  
Non-criminal social engineering 90  
Why social engineering works 91  
Case study: Alice and Bob 92  
Exercise 5.1: Hot state triggers 99  
Notes 99
- 06 Attacks that utilize social engineering** 101  
Phishing 101  
Case study: Bill 103  
Case study: FireEye 105  
Case study: WhatsApp 106  
Case study: Business email compromise 108  
Money trails and cryptocurrency 109  
Ransomware 109  
Offline social engineering attacks 111  
Notes 112

## **PART FOUR** The physical side of cyber security 113

---

- 07 Why physical space matters in cyber security** 115  
Access control systems 116  
CCTV 119  
Exercise 7.1: Spot the security flaw 121  
Physical vulnerabilities in the Internet of Things 122  
The physical infrastructure of the internet 125  
Notes 126

- 08 How organizations can better protect themselves** 127
  - Firewalls 128
  - Anti-virus software 128
  - Network segmentation 129
  - Airgapped networks 129
  - Policies and procedures 130
  - Logging 130
  - Monitoring 131
  - Auditing 131
  - Intrusion detection systems and intrusion protection systems 131
  - Block list and allow list 132
  - Cyber threat intelligence and threat hunting 133
  - Vulnerability scanning 133
  - Penetration testing 134
  - Awareness-raising training 134
  - Security culture 135
  - Champion programmes 136
  - Digital footprint assessments 136
  - Physical security controls 137
  - Social engineering assessments and red team engagements 137
  - A layered approach 138
  - Notes 139
  
- 09 How individuals can better protect themselves** 140
  - Protect your accounts 141
  - Biometric security 145
  - Loyalty points theft 146
  - Protect your devices 147
  - Protect your data 148
  - Be social media savvy 151
  - Be social engineering savvy 151
  - Notes 153

**10 Nation-state cyber security: Geopolitics 154**

Policing the internet 154

Nation-state level cyber attacks 156

NSA insiders 162

Companies and nation-state level attacks 163

Misinformation and disinformation 165

Notes 167

**PART FIVE The future of cyber security  
and what it means for your  
career 169**

---

**11 Cyber security in different industries 171**

Celebrity, entertainment and pop culture 171

Journalism and the media 174

Sport 175

Social media and influencers 176

Small and medium enterprises 177

Education 178

Conveyancing fraud 180

Notes 181

**12 Cyber security at the board level 183**

Cyber security frameworks 184

Cyber security governance 184

Risk appetite and risk tolerance 186

The board perspective on cyber security 187

Board members as challengers 188

Cyber security as a business risk 191

Notes 193

**13 Pursuing a cyber security career 195**

Qualifications and certifications 196

What do employers want? 199

What can you do to get a job in the industry? 202

Jack Daniel, BSides co-founder 204  
Sophia McCall, Captain of Team UK at the European  
Cyber Security Challenge 206  
Note 208

**14 The variety of cyber security careers 209**

The start-up CEO 209  
The infosec pundit 212  
The professor 214  
The journalist 216  
Alternative paths into cyber security 216  
The ethical hacker 218  
The lawyer 219  
The analyst 219  
The national cyber security advisor 220  
The security awareness leader 223  
Specialists and generalists 224  
The security contractor 225  
A final word: Keep a learning mindset 226  
Notes 229

*Appendix: Answers 230*

*Index 233*



# ACKNOWLEDGEMENTS

**M**any 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!'*

**T**hese 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.

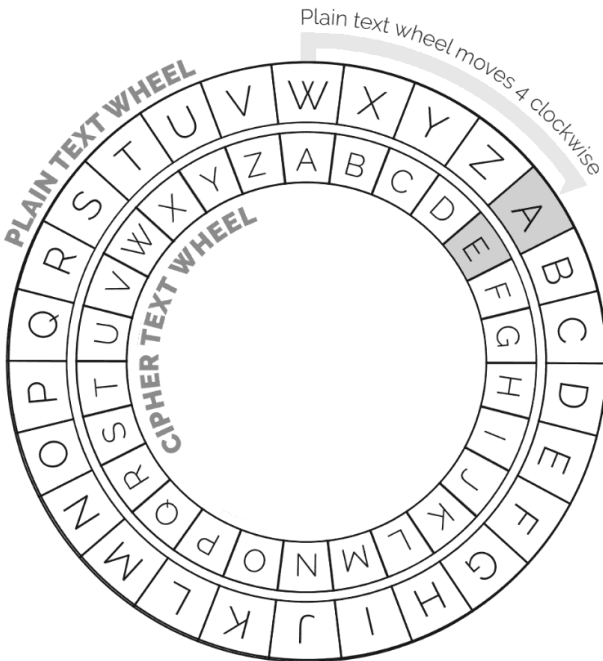
For example, if we are going to encode the words ‘shift example’ and shift four to the right, it would become ‘wlmjx ibeqtpi’. This is illustrated in the wheel below.

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 rknz-cyr bs n Pnrfne pvcure. Jryy qbar sbe qrpqvat 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' <sup>1</sup>
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	<i>New York Times</i> reports on hackers and describes ethical hacking activities <sup>2</sup>
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	<i>The Hacker Quarterly</i> 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 <sup>3</sup>
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 <sup>4</sup>
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

- Abagnale, F 88–89
- advanced persistent threat (APT) 24
- Allsopp, C – jailed for TalkTalk breach 51
- Amazon 66
  - Simple Storage Service (S3) 68
- appendix: exercise answers 230–31
  - exercise [1.1](#): assessing the risks 230–31
    - local estate agent 230–31
    - multinational bank 230
    - political party 230
  - exercise [3.1](#): identifying vulnerabilities 231
  - exercise [5.1](#): hot state triggers 231
- Apple 34, 66, 68, 148
- Armstrong, J 219, 228
- Ashley Madison – hacked by cyber criminals 42–43
- attacks that utilize social engineering 101–12 *see also* case studies
  - money trails and cryptocurrency 109
  - offline social engineering attacks 111–12
  - phishing 101–09
    - spear-phishing 102–03
    - voice-phishing or vishing 103
  - ransomware 109–11
    - and No More Ransom initiative 110–11
- Avid Life Media (ALM) 42–43
  - and breach of Ashley Madison 42
  - rebranded to Ruby Corp 43
- Beckham, D 123
  - and his £100,000 BMW 123
- Caesar, J [3](#)
- Caesar cipher/shift 3–4, [4](#)
- Carroll, J (security contractor) 225–27
- case studies (for)
  - attacks that utilize social engineering
    - business email compromise 108
    - FireEye 105–06
    - voice-phishing: Bill 103–04
    - voice-phishing: FireEye 105–06
    - WhatsApp 106–07
  - social engineering
    - why social engineering works: Alice and Bob 92–93, 93
  - technical vulnerabilities
    - Life at Parliament View Ltd 86
    - TalkTalk 50–51
    - WannaCry 54–55 *see also* WannaCry
  - what cyber security is
    - cybercrime: ransomware – SamSam 26–27
    - cybercrime: script kiddies – TalkTalk 23
    - malicious insiders: Andrew Skelton 28–29
    - non-malicious insiders: Dow Jones and Facebook apps 30–31
  - why people are so important in cyber security
    - creation: The Big Hack (Bloomberg Businessweek) 65–66
    - use: Amazon Simple Storage Service (S3) 68
- chapter notes (for)
  - attacks that utilize social engineering 112
  - cyber security at the board level 193–94
  - cyber security in different industries 181–82
  - how individuals can better protect themselves 153
  - how organizations can better protect themselves 139

- chapter notes (for) *Continued*
  - introduction to cyber security 10
  - nation-state cyber security:
    - geopolitics 167–68
  - pursuing a cyber security career 208
  - social engineering 99–100
  - technical vulnerabilities 59–60
  - the variety of cyber security careers 229
  - what cyber security is 32–33
  - why cyber security is important 43–44
  - why people are so important in cyber security 81–83
  - why physical space matters in cyber security 126
- Clinton, H 165, 166
- Computer Emergency Response Team (CERT) 80
- cyber security: introduction 1–10
  - see also* why cyber security is important
  - cyber security, you and your career 9–10
  - history of cyber security 3–4, 4, 5–8
  - the rise of cybercrime 8–9 *see also* legislation (UK) and legislation (US) and the 414s 8–9
- cyber security at the board level 183–94
  - board members as challengers (and) 188–91
  - NCSC (UK): key questions for board to ask 189–90
  - need to receive on-going communication on threats 191
  - questions for members to ask 190–91
- the board perspective on cyber security 187–88
  - key findings of UK Government report (2019) 187–88
  - see also* reports
- cyber security as a business risk (and) 191–93
- cloud computing 193
- questions – knowing which, when and how to ask 192
- cyber security frameworks 184
  - see also* subject entry
- cyber security governance 184–85
- risk appetite and risk tolerance 186–87 *see also* studies
- cyber security in different industries 171–82
  - celebrity, entertainment and pop culture 171–74
    - Caitlyn Jenner 173–74
    - Kim Kardashian 173
    - Taylor Swift 171–73
  - conveyancing fraud 180
  - education 178–79
    - of 430 UK schools 83% had experienced a cyber security incident 179
    - cyber attack/phishing emails at Lancaster University 179
  - journalism and the media 174–75
  - small and medium enterprises 177–78
  - social media and influencers 176–77
    - ‘Joshua Brooks’ influencer scam 176–77
  - sport 175–76
- cyber security frameworks
  - Cyber Essentials 184
  - ISO 27001 184
  - National Institute of Standards and Technology (NIST) 127, 184
- cyber weapon: Stuxnet 125
- Diachenko, B 30–31
- Disney ‘hack’ (2019) 70
- Dunning, D 25
- Estonia, the Bronze Soldier statue and cyber attacks 157–59
- exercises (for)
  - social engineering: hot state triggers 99
  - technical vulnerabilities: identifying vulnerabilities 57
  - what cyber security is: assessing the risks 31
  - why physical space matters in cyber security: spot the security flaw 121

- Facebook 73, 84, 101, 166 *see also*  
 case studies  
 Messenger 34
- figures  
 Alice and Bob's email 93  
 Caesar cipher/shift 4  
 cybercrime bell curve 25  
 plain text wheel 4
- Financial Conduct Authority  
 handbook: *Handbook of  
 Rules and Guidance* 39
- Freakyclown 227
- Gates, B 145
- Geers, K (cyber intelligence  
 analyst) 219–20, 227
- Gold, S 9
- Greenberg, A 123
- hackers (and)  
 Advanced Persistent Threat 28  
 (APT28) 165  
 Fancy Bear 165  
 Guccifer 2.0 165  
 hacking of US Democrat  
 emails 165  
 hacks and 'hacks' 70  
 Jmaxxz 123  
 Miller, C 123, 124  
 Sofacy Group 165  
 Valasek, C 123, 124  
*Handbook of Rules and Guidance*  
 (Financial Conduct  
 Authority) 39
- Hanley, M: jailed for TalkTalk  
 breach 51
- Histiacus 3
- how individuals can better protect  
 themselves (by) 140–53  
 being social engineering  
 savvy 151–53  
 seven steps for protection  
 against cybercrime 152  
 being social media savvy 151  
 biometric security 145  
 from loyalty points theft 146–47  
 protecting their accounts (by/  
 with) 141–47  
 biometric security 145  
 password managers 142–43  
 two-factor authentication  
 145–46  
 writing passwords down  
 143–44  
 protecting data 148–50  
 by backing up 150  
 on websites 149–50  
 on Wi-Fi 148–49  
 protecting devices 147–48  
 how organizations can better protect  
 themselves (with) 127–39  
 anti-virus software 128  
 auditing 131  
 awareness-raising training 134–35  
 block list and allow list 132  
 champion programmes 136  
 cyber threat intelligence and threat  
 hunting 133  
 digital footprint assessments  
 136–37  
 firewalls 128  
 intrusion detection systems (IDS),  
 intrusion protection systems  
 (IPS) 131–32  
 a layered approach 138–39  
 logging 130  
 monitoring 131  
 network segmentation 129  
 and airgapped networks 129  
 penetration testing 134  
 using Kali Linux and Burp Suite,  
 Metasploit, OpenVAS 134  
 physical security controls 137  
 policies and procedures 130 *see  
 also* research  
 security culture 135–36 *see also*  
 definitions *and* Schien, E  
 social engineering assessments and  
 red team engagements  
 137–38  
 vulnerability scanning 133
- Instagram 34, 74, 176–77
- introduction *see* cyber security:  
 introduction
- ISO 27001 standard 127, 131
- Jenner, C 173–74
- Kahnemann, D 94 *see also* *Thinking  
 Fast and Slow*
- Kardashian, K 173
- Kelley, D: jailed for TalkTalk  
 breach 51



- Kotomah, B (UK fashion designer) 176  
 Kruger, J 25
- legislation (UK)  
 Communications Act (2003) 39  
 Computer Fraud and Abuse Act (1986) [6](#)  
 Computer Misuse Act (1990) 9, 39  
 Data Protection Act (DPA, 2018) 39, 56  
 Forgery and Counterfeiting Act (1981) 9  
 General Data Protection Regulation (GDPR, 2018) 39–41, 56  
 Network and Information Systems Regulations (NIS Regulations, 2018) 39  
 Privacy and Electronic Communications Regulations (PECR, 2003) 39
- legislation (US): International Traffic in Arms Regulations (ITAR) 156
- Li, Professor S *and* advice on cyber security 214–16
- Lustig, V 87–88
- McArthur Wheeler case 25
- Malwarebytes *see* research
- Mollett, A 180  
 defrauded of life savings (2017) 180
- Moussouris, K 155
- Mulholland, [I](#) 155
- nation-state cyber security:  
 Geopolitics 154–68  
 companies and nation-state level attacks 163–64  
 NotPetya *and* Maersk shipping 163–64  
 Saudi Aramco 163  
 Ukraine and NoetPetya malwrae 164  
 misinformation and disinformation 165–66  
 accusations of interference with US election (2016) 165  
 publication of the Mueller report (2019) 165–66  
 report on Russian campaign to influence US 2016 election 165  
 nation-state level cyber attacks (and/the) 156–62  
 Bronze Statue 157–59 *see also* Estonia  
 Great Seal 157  
 Stuxnet 159–60  
 WannaCry 160–62 *see also subject entry*  
 NSA insiders (box) 162  
 policing the internet (and the) 154–56  
 International Traffic in Arms Regulation (ITAR) 156  
 Tallinn Manual [2.0](#) 154–55  
 Wassenaar Arrangement 155–56
- Noun, M (security awareness manager) 217
- Nudge* 94 *see also* Sunstein, C *and* Thaler, R  
 and the Homer Simpson and Spock ways of thinking 94–95
- Obama, B 174
- O’Flaherty, K 216, 224
- Open Web Application Security Project (OWASP) 80
- organizational culture, definition of 135 *see also* Schien, E H
- Patrick, N [8](#), [9](#)
- physical space: why it matters in cyber security 115–26  
 access control systems 116–19  
 badges and lanyards 117–18  
 biometrics 118  
 magnetic locks 118–19  
 CCTV 119–21  
 lack of monitoring 120  
 poor placement and lack of coverage 120–21  
 poor quality 119–20  
 physical vulnerabilities in the Internet of Things 122–26  
 and the physical infrastructure of the internet 125

- Privacy Commissioners: Australia *and* Canada 42
- pursuing a cyber security career (and) 195–208
- Jack Daniel, BSides  
co-founder 204–05
- qualifications and  
certifications 196–99
- Certified Ethical Hacker (CEH) 197
- Certified Information Systems Security Professional (CISSP) 197–98
- Offensive Security Certified Professional (OSCP) 198
- ‘real world’ experience 199
- Security+ 196
- university study 198
- what do employers want? – your personal attributes *and* skills 199–202
- acceptance that you don’t know everything 200–201
- communication skills 202
- curiosity 200
- a desire to learn 200
- empathy 201
- ethical and moral code 199–200
- situational awareness 201
- spotting patterns 201–02
- what can you do to get a job in the industry? 202–08
- BSides 203–05  
and co-founder: Jack Daniel 204–05
- bug bounties 207
- ‘capture the flags’ (CTFs)  
competitions 205–07
- Sophia McCall (Captain, Team UK, European Cyber Security Challenge) 206–07
- DEFCON groups 203
- develop your network 207–08
- Putin, V 165
- report: FTSE 350 companies and cyber risk governance (UK Government 2019) 187
- research  
on information security policies (Club CISO, 2019) 130
- into spear-phishing email campaign (Malwarebytes) 96–97
- risk, threat and vulnerability – and their meaning 35
- Room, C (Director, Pulse Conferences) 218
- Sawers, S and J 73
- Schien, E [H](#) 135
- Schifreen, R 9
- Sheeran, E 172  
and definition of organizational culture 135
- Shipley, D 209 (CEO, Beauceron) 209–11, 212
- Skelton, A 28–29
- social engineering 84–100  
through history 85–90
- Francis Cabot Lowell 86
- Frank Abagnale 88–90  
and did you know? 89–90
- the Trojan Horse 85–86
- Victor Lustig 87–88
- non-criminal 90–91
- red flags 84–85  
and why social engineering works 91–99 *see also* case studies
- exercise [5.1](#): hot state triggers 99
- hot state emails:  
Shame 95–97
- hot states 94–95
- sextortion 97–99
- Sorenson, A (CEO, Marriott Group) 41
- Spitzner, L (Director, SANS Security Awareness) 216, 223, 224
- studies (of/on)  
850 ICS and SCADA networks 57–58
- determination of risk appetite levels (UK Government) 186
- Sunstein, C 94–95 *see also* *Nudge and* Thaler, R
- Supermicro 65–66
- Swift, T 171–73