



Contents

<i>Foreword</i>	5
<i>Acknowledgment</i>	9
CHAPTER 1: We're all a dot com	15
The Gotcha	21
CHAPTER 2: Some scenarios	25
Scenario 1: APT and Destructive Payload	26
Scenario 2: Supply Chain Risk	28
Scenario 3: Medical Centres	30
Scenario 4: The Horse has Bolted	31
CHAPTER 3: How Things Work (and do not Work)	35
The Internet	36
Servers and the Cloud	38
Corporate Networks	40
Firewalls	42
Antivirus	45
VPNs	46
Encryption	47
Passwords	48
CHAPTER 4: Additional Prevention Measures	51
Protecting the 'Endpoint'	52
Monitoring	54
Well-tested Incident Response Plans	56
Knowing our Vulnerabilities	56



Backups.....	57
Strategic Cyber-security Governance	58
APT and Government Contact	59
CHAPTER 5: Some Terms We May Have Heard.....	63
Big Data.....	64
Botnet.....	64
BYOD.....	65
Cookies	65
Distributed Denial of Service Attack	66
Drive-by.....	67
Waterholing.....	67
External Media.....	68
Insiders.....	68
Phishing.....	69
Spearphishing	71
Ransomware.....	71
Remote Access Tool.....	72
Social Media Leakage	72
Spyware.....	73
Viruses, Worms and Trojans.....	74
Blended Threats	75
CHAPTER 6: What to Do Next	77
For everyone.....	78
For Small to Medium Businesses.....	81
For Larger Government or Corporations.....	85
CHAPTER 7: CyberBasics Checklists	91
Checklist for Everyone.....	92
Checklist for Small and Medium Business.....	95
Checklist for Larger Government or Corporations.....	98



End Notes	103
The Card Game	110
About the Consulting Editor	111
About the Author	112
About Gotcha!	113