Book

Title: Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection, Prevention and Response

Example citation: Hills, M., (ed.) (2016) *Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection, Prevention and Response.* New York: Nova Science Publishers. 9781536100907.

Version: Accepted version

Note: Preface

PREFACE

WHY ANOTHER BOOK ABOUT CYBER SECURITY?

This is an important question. The world does not need more books that opine on the threat caused to the invisible cyber infrastructures that we all depend on by hackers and viruses and how we need new software and hardware to spot and engage with it. Equally, there should be no market demand for the thoughts of academics disconnected from the exigencies of the real world about how we should conceptualise threats and systems. We have also read enough from consultants using thinly-disguised articles to sell mundane and derivative training activities.

But challenging the very meaning of 'cyber' itself and seeking out positive, practical and pragmatic ways in which any organization could enhance its security against cyber (and cyber-enabled) threats: this is a path of enquiry that is much less well-travelled. The contributors to this volume, all with extensive pedigrees in the 'real world', are passionate about persuading whoever will listen that any engagement with 'cyber' must recognize it as a socio-technical challenge.

This book is a provocative manifesto of disruptive thinking about cyber security. It presents cutting-edge thinking and professional reflection and is designed to be a source of ideas and approaches that can be adopted and adapted for application in the real world by those who recognise that conventional ways of defining and considering cyber attack are insufficient.

All of the authors believe that 'cyber' must be urgently wrestled back from the technologists, cyber security professionals, consultancies and corporate silos that have hijacked it (seemingly without any resistance) and rendered the term essentially meaningless. The authors write from applied and often unique experience in a range of commercial, consulting, state and defence environments.

In planning for, managing against and rehearsing responses to cyber attack – businesses and governments alike prepare for an artificially limited version of reality. In preparing for conventional understandings of cyber attack – organisations are compromised from the outset. Scenarios envisaged are predictable, often incomprehensible to the C-suite and non-technical personnel and focus on the failure or compromise of critical systems.

There are, of course, some purely technical cyber-threats (e.g. viruses or a hacking campaign directed at specific content). But even in regard to these eventualities, organisations neglect the strategic and other consequences of non-trivial disruption to business processes and novel challenges of a less than benign operating environment. In preparing for cyber-technical scenarios, organisations neglect to consider how the rest of it functions in conditions where response capability maybe overwhelmed, recovery may be impossible or take an indefinite and unpredictable amount of time. The organisational response to cyber threats - which might turn a businesses' servers into an inaccessible digital crime scene, eviscerate market value, generate massive reputational cost and unpredictable consequences - presents a very high bar for success. Business continuity, emergency planning, disaster recover, crisis management and other functions – carefully prepared in isolation from one another – thrash around searching for issues that they can apply traction to.

Many of the authors of this volume have direct experience of inflicting, reporting on and protecting organisations from such effects and also have knowledge of taking the challenge to additional levels. Most consultancies, academics and 'experts' don't live in the real world, are content with operating in the commoditised world of cyber-technical security and don't have the intellectual capacity to understand, engage with or monetize this more challenging reality. This book is intended to help organisations improve preparedness for both the established world of cyber and the real one.

Improving the resilience of organisations to cyber-technical attack is, of course, critical and is difficult. But it would not be enough. Growing dynamic immunity to a far broader spectrum of cyber is vital and a source of competitive advantage to those that can manage it. Few will. This book is for those that recognise the compelling need to see cyber security as always more than a technical issue.

CYBER IS IRREDEEMABLY SOCIO-TECHNICAL

The collective understanding of the contributors to this volume is that we should always and only see cyber as a socio-technical threat. The combination of humans and computers (in whatever form) blended to produce shock and surprise to corporate and government systems. Consequently, preventative counter-measures and response structures must leverage socio-technical genius to out-think, out-prepare and out-manoeuvre adversaries. We think that in considering cyber attacks, we have no choice but to think of them as extending across the electro-magnetic spectrum; involving either simple or more complex use of computing power; drawing on creativity and innovation; perpetrated by smart criminals, terrorists, competitors, employees (or accident) and underpinned by emerging and novel technology. Computers will be involved – but these could be used in unexpected ways, such as:

- capture of an executive or manager, via cyber-enabled blackmail, in criminal behaviour (e.g. the use of a digital ‘honeypot’)
- insertion of errors in software that a system or platform depends on (e.g. an illegal ‘defeat device’ planted in a competitor auto-maker)
- the crafted email which triggers the organisation into responses which undermine value
- the targeted and subtle hacking of critical Intellectual Property (IP) – removing or compromising it
- the distracting mini-technical event which distracts attention from the real exploit

- the use of novel attacks that generate cyber from kinetic effects (e.g. directed energy weapons)
- loss of trust and reputation via the targeting of up-stream or down-stream partners in a supply-chain

Against these and other threats - organisations need agile, adaptive, decisive decision-making, enabled by reliable and rehearsed flows of actionable information from sensors that provide early warning and rich insight. Systems and structures must act on reflex, hit strategic objectives hard, sustain a response, make competitive and sustainable decisions that can be amended on the fly and draw on a suite of timely and usable insight from technical, legal and other experts.

THE CHAPTERS

This book opens with two chapters which explore the philosophical dimensions of cyber security – in a genuinely pragmatic manner. **Dr Keith Scott** starts by setting out, in characteristically challenging and wide-ranging fashion, why it is that complete cyber security will always be unachievable. Rather than rely on technological or policy solutions (which won't work), Keith suggests that we must come to terms with the cyber domain as an ever-growing threat landscape, consider that its inherent anarchy may present defensive and offensive benefits and develop strategies for threat mitigation which are cognizant of the real character and challenges of the cyber space.

Dr John Ardis extends on these thoughts by bringing an Information Operations (IO) perspective to bear on the characteristics of cyber systems and their socio-technical components. By intellectually exceeding what typical thinkers on cyber-security consider are the properties of the systems they pretend to understand, John sets out a view of systems as difficult to understand but where socio-technical understanding is competitively advantageous.

The next four chapters are the distillation of the experience over many decades of practitioners attempting to secure the legal and hardware/software industries as well as a complementary public sector view that protests that cleaving to technical security has completely overlooked the critical role of human error to cyber security. The final contribution in the section reports on how a major IT re-seller helps educate and empower its small and medium-sized customers about risk.

David Wood describes why the global legal industry can be characterized as 'low hanging fruit' to cyber attackers, especially in the small to medium-sized business space. The implementation of technical solutions has been compromised, its people, behaviours and cultures are easy targets and, despite the assumptions that reasonable people might make, the legal industry is the weakest link in the chains upon which its clients are dependent. Fortunately, David has some ideas about how to improve matters cheaply and effectively.

That ethos is continued by **Graham Palmer**, who presents seven practical maxims for our information security age. Whilst cyber (and cyber-related) security is incredibly important, achieving interest, buy-in and compliance is very difficult. Graham's maxims, culminating in the recognition that cyber is about 'brains not boxes' have enabled him to positively communicate holistic socio-technical information security ideas with board members, senior executives, IT staff and fellow security professionals. They could be used in any organization, anywhere.

Clint Barker turns his attention to the fact that senior management teams already hold the means for effective security in the cyber age. After demonstrating the mis-use of the term 'cyber security', Clint criticizes the alleged cyber security professionals for neglecting human error and socio-technical means – whilst also showing how solutions can be speedily produced from existing human resources.

Finally in this section, **Dr Mils Hills** and **Louise Atkinson** report on some good news from the world of the IT re-seller. The company that they analyse specializes in working with small and medium sized businesses, where an ethical and sustainable culture means that pre-sales and other functions educate clients on their actual risk exposure from hardware and software implementation and advise on cost-effective mitigations. They fill an information gap left by government and other complicated sources and provide a trusted, trustable and tailored solution.

The next two chapters detail the properties of socio-technical cyber threats that conventional analysts and commentators have yet to explore. **Dr Mils Hills** dives into the ways in which cyber-enabled adversaries could use smart techniques to influence or direct the decision-making of individuals and bureaucracies. Protection from an enhanced corporate immune system subject to frequent, cheap exercises, and with active sensors, needs to be in place to detect and destroy the potential for any organization to be prevented from self-determination.

Stefanie Hills, Thomas Jackson and **Martin Sykora** continue the theme of the unexpected cyber risk by reporting on emerging findings about the use of terse text in social media to achieve potential persuasive effect in target populations. Organisations and individuals within them both need to be sensitized to the fact that cyber security means being aware that they may be the targets of attempts to persuade them to think or do something. Well-crafted terse text can help change opinions or make it more likely that links to malicious websites, for example, are clicked on.

Many of the prior contributors mention in passing the need to exercise relevant corporate plans for responding to a cyber risk coming to pass – whether that is in terms of detecting it before crisis strikes, or when the crisis does strike with little or no warning. The next three chapters detail practical and proven ways of testing plans at all levels of an organization but including the senior management; developing serious games to explore how best to act - for use at the middle and senior hierarchical levels and, finally, how teams and individuals should be selected to enable the best possible sustainable and strategically-aligned performance under possibly overwhelming levels of stress.

Nick Simms opens this section by reviewing the reasons why organizations *should* rehearse their cyber resilience plans, although notes that in his experience many will not have such plans in any case. Practical and pragmatic advice is given for those commissioning or designing such exercises, covering phases such as the triggering and usability of plans and considerations as to how exercises are conducted, and why.

Dr Paul Theron presents the results of a great deal of reflection on how best to conduct serious games about cyber threat, which can be a highly effective way of getting beyond the technology-focus of traditional cyber discussions and raise awareness about the wider implications of cyber attack. Paul reviews the various approaches which are available, compares their efficiency and concludes by describing a way in which serious games can be part of a framework to helpfully raise management awareness about cyber threat.

Finally in this section, **Guy Batchelor** draws on his experience in preparing for and (successfully) swimming the English Channel. His chapter explores how a combination of the ethos of his military background combined with a well-chosen support team enabled him to deliver strategic main effort. In choosing individuals to lead and teams to support cyber and other crisis management mechanisms, the events and maintaining delivery of set strategic objectives should be thought of as being physically, mentally and emotionally arduous.

The final two chapters reflect on how socio-technical appreciation can be implemented into cyber security functions in order to deliver enhanced risk management and insight. **Stewart K Betram** opens this section, by reclassifying system intrusions as ‘threat systems’ such as Stuxnet. An enhanced, fine-grained understanding of the operational sophistication of such threat systems - missed by a purely technical assessment - is proposed, where the use of approaches which consider the human dimension could have a critical role in future cyber security processes.

The final chapter of the book continues this theme. **Arun Warikoo** reviews the development of technical cyber attack detection technologies, but notes that, despite the implementation of these, breaches continue to occur. Arun proposes improvements to current techniques for detecting, preventing and responding to cyber attack through the use of a qualitative, risk-centred approach. This additional layer adds value to the enterprise by providing actionable intelligence, categorizes cyber-attacks, prioritizes risks in real-time and automates responses to cyber-attacks (wherever possible).

Dr Mils Hills

Berlin 29 July 2016