BEYOND SIMPLE HUMAN THREATS TO CYBER-SECURITY:

THE NEED FOR STRONG PROACTIVE MEASURES AND RESILIENT RESPONSES TO CYBER RISK

By Dr Mils Hills, Associate Professor in Risk,
Resilience and Corporate Security, Northampton Business School

THE UNIVERSITY OF NORTHAMPTON
Northampton Business School

This paper sets out an argument that cyber-security needs to be thought of as an inherently socio-technical challenge where people are the source both of the strongest threat and countermeasure. I draw on experience researching cyber- and information warfare and consult onboard and operational tests of responses to such attacks. I am also fortunate to be part of an energetic and unconventional cluster of theorists (the CORTEX group) looking at cyber and related risks from the viewpoint of being both practitioners and academics. Our belief is that many thinking about and working in cybersecurity suffer as a result of minimising the consideration of the human factor. Organisations which embrace a broader view of what cyber-security is could enjoy a competitive advantage in terms of situational awareness, risk mitigation and crisis response denied to those who cleave to a technologically-weighted definition. This chapter sets out some ideas to stimulate debate – how can organisations evolve efficient and effective counter-measures to the human dimension of cyber-security?

Fundamentally, cyber-security is about protecting the ability of an organisation to make decisions and continue the delivery of strategic objectives. If vital databases are inaccessible, core Intellectual Property (IP) stolen, trust and confidence lost, private conversations made public, asset registers corrupted, prospects missed, an organisation will be unable to continue with its normal course of business, generate options and make choices on its own terms, against its own priorities and determine its normal time horizons.

The usual decision-making cycle is impossible as a crisis of potentially existential proportions has erupted. Otherwise rational decision-makers lose their heads, find themselves obsessed with tactical detail rather than the strategic picture and become driven by media coverage rather than business requirements. Freedom of manoeuvre is reduced to almost nothing, with the tempo and pace of activity set by the ensuring crisis. There are few upside opportunities and an awful lot of downside risks and costs.

Even if nothing has happened, the perception that something has is corrosive to upstream trust: great reassurance is needed for many stakeholders, where, sometimes, reassurance will be impossible. McKinsey and Co. evidence this in reporting one of their client's unfortunate direct costs in dealing with a cyber-incident, some $100m. However, "those costs were small compared with the subsequent multibillion-dollar loss in market capitalisation, which was largely attributed to investors' loss of confidence in the company's ability to respond" (McKinsey & Co, 2013).

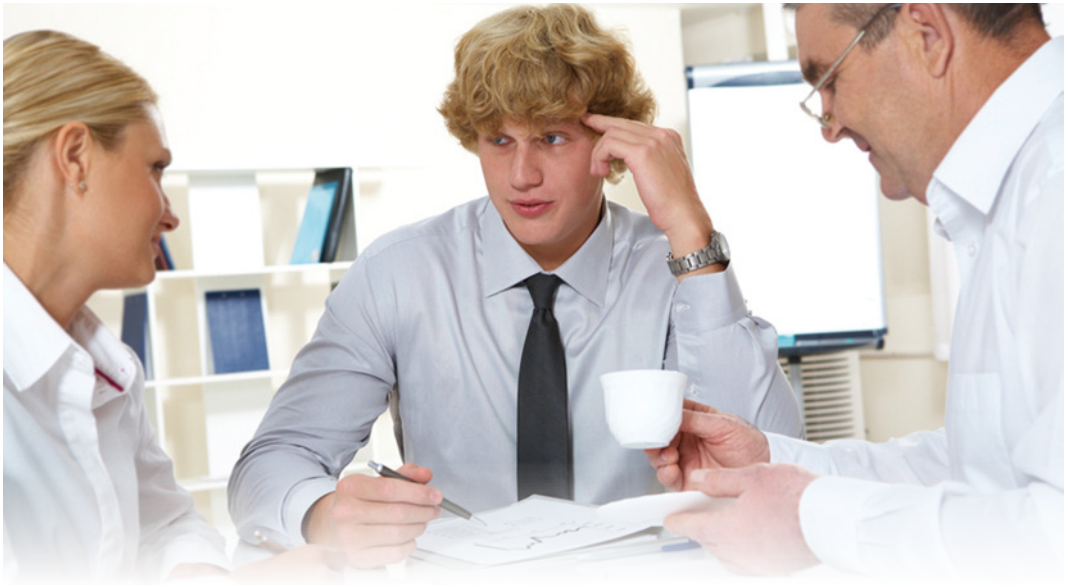
Although some cyber-security exploits are deeply subtle and clever – many are not – when expensive and smart measures are put in place they can often be made irrelevant by simple behavioural realities. A specialist law enforcement officer told me of a simple experiment outside a bank data centre: 100 individuals passed and spotted a 'mislaid' USB data-stick in the car park; all 100 picked it up with the intention of satisfying their basic human curiosity as to its contents.

However, caution needs to be adopted in thinking that examples such as these are the limit of the extent of socio-technical risk. Such problematic reactions and underpinning assessments of risk are not far along a continuum which (we must anticipate) will conclude with extremely sophisticated attack vectors and techniques. Therefore, there is a pressing need to develop immunity to pretty basic attempts to subvert technical security measures and conventional user monitoring. It would be unwise for companies and governments to assume that what they are aware of or experience at the moment is the worst 'cyber-threat weather' that can be encountered. Of course, it is worth noting that surveys indicate that the existing entry-level threats consistently penetrate existing protective measures, for example. The 2014 Information Breaches Survey found that 81% of large and 60% of small businesses detected security breaches (Business Innovation & Skills, 2014), and yet these could be thought of as the 'GCSEs of cyber-attack' as the then Cabinet Secretary Gus O'Donnell once described my exercise of the crisis machinery facility COBR against an analogous scenario!

In running extensive exercises of boards and operational responses to cyber-challenges, my experience has been that organisations struggle to reach an understanding of (a) the potential of cyber-security risks in general (b) the implications for the delivery of business and (c) of the ways in which an unfolding situation could have, or be early signs of, a cyber-dimension. Because cyber-risks are so poorly understood and have largely become thought of as owned by jargonised, technologically-based experts, boards and others barely grasp their significance in the abstract, non-crisis context and certainly cannot reach a swift understanding under the stress of an incident.

THERE IS A PRESSING NEED TO DEVELOP IMMUNITY TO PRETTY BASIC ATTEMPTS TO SUBVERT TECHNICAL SECURITY MEASURES AND CONVENTIONAL USER MONITORING

Here is a brief insight into just how poorly organisations conceptualise cyber-security: employees are being suspended, subject to disciplinary investigation and (likely) dismissed on the basis of physical copies of alleged digital evidence. For example, in human resources and other functions of organisations, there is no awareness that it is possible to completely fake WhatsApp and other messaging exchanges. Faking at the digital level is one thing: but this is merely the generation of what appear to be exchanges – but printed out. In receipt of such paper



'evidence', organisations should, of course, request copies of, be able to handle or commission professional digital forensic analysis. Instead, the paper 'evidence' is accepted as *prima facie* proof that something needs investigation at the level of the employee(s) implicated – rather than actually shielding the employee and the organisation from stress, cost and distraction by requiring the supply of authenticated materials. It is so simple to download emulators of the WhatsApp user interface and edit every detail that without digital evidence (or by requiring that alleged criminality is reported to the law enforcement community rather than the employer) such print-outs of alleged screenshots should be viewed as works of art and nothing more.

It is becoming clear that organisations accept such emulated product and launch immediate and heavy-handed disciplinary proceedings – safe in the knowledge that they can likely dismiss an employee on the grounds of this 'evidence' because they have a reasonable belief that it is genuine. Whilst this may be legally safe, it is not helpful for the business or institution, which stands to lose talent, as well as the intangibles such as trust, confidence and goodwill amongst remaining employees, due to entirely faked and easily refuted artefacts.

In short, at board level and elsewhere in organisations, cyber-security is restrictively thought of as being about electronic attack conducted through the medium of malicious software and hacking – directed against firewalls and other security infrastructure. When cyber-scenarios are considered, they are usually addressed in terms of how the company would restore availability and assure integrity of systems *separate to managing the wider business consequences.* So, for example, managing a disastrous failure of a key server and its dependant applications would be explored in isolation from the multitude of direct business effects and additional work (e.g., client liaison, investor reassurance, press and PR activities) generated.

This underscores an easy mental separation that has become accepted as normal. The scope of cyber-, the likely shape and characteristics of a cyber-threat and the business impacts. This has produced a dangerous and skewed perception, which is both limited and limiting.

Counter-measures to cyber-risks are generally neatly compartmentalised as being about having the best (value) firewalls and other systems, with personnel mandated to change passwords and adhere to basic information security protocols. These topics are

of little interest to boards where technical knowledge is limited and, even where there is a Chief Information Officer (CIO) or Chief Information Security Officer (CISO) in the C-suite, they struggle to win resources or attention arising from even a narrowly defined version of cyber-security.

Just as the saying goes 'good information warfare is indistinguishable from bad administration', so the potential of clever socio-technical attack is that the pre-placement or recruitment of employees, etc., would be indistinguishable from the normal 'noise' and chaos that characterises the modern workplace. Indeed, even as individuals move *organically* (e.g., if motivated by their own personal beefs or malevolence) or *strategically* (e.g., guided by an activist group, industrial competitor or hostile intelligence service) towards causing or enabling the causation of cyber-compromise, the likelihood of detection by existing sensors is vanishingly small.

To further complicate matters, we in the CORTEX group believe that cyber-security (as a socio-technical phenomenon) should also encompass even less technical events – but events which nonetheless depend on cyber-infrastructure. In a forthcoming conference presentation, my colleague Guy Batchelor and I will reflect on the lessons that ought to be learned by any public or private sector organisation by the fall from grace of Brooks Newmark MP (and former Junior Minister) as well as that of Sir Malcolm Rifkind MP (former Chair of the Intelligence and Security Committee). To focus on the former, the very simplest form of digital tradecraft was used to effectively shape the situational awareness of the Minister of State for Civil Society.

A journalist developed a Twitter profile purporting to be that of a young, blonde, female Conservative Party public relations staffer. Comprised with the bare minimum of content – but clearly just enough to convince at least one target of its authenticity – unproblematic Twitter messaging was effectively used to enable the migration of the online conversation to alternative platforms. Exchanges of photos then occurred, which, when ultimately released into the public domain, terminated Mr Newmark's career.

This is hardly the most sophisticated, nor novel, type of way of causing embarrassment to politicians or other middle-aged men. What is, perhaps, slightly more surprising is that this was so easily achieved in an ever more security conscious world, replete with warnings about the easy exploitation of social media.

And things could have been even worse. Indeed, maybe there are for others yet to hit the headlines. If it was *so* easy to detect and exploit a very conventional vulnerability in a figure in public life, we can reasonably assume that senior individuals in other walks of life may be just as (if not more) vulnerable. The effect sought in the Newmark case was clearly to generate business for a freelance journalist – but what if the effect sought were different?

There is no reason why Newmark, a director of procurement, head of security of any other senior or middle-ranking individual might not be targeted on behalf of commercial rivals or others. If, rather than being motivated solely by generating embarrassment and media coverage in the very short term, Newmark's behaviour (or that of a procurement, contract, facilities or other director or manager) had led to their being retained as an asset, what might they be pressured to do? For example, the threat of exposure could be leveraged by a criminal enterprise or others to award a

contract to an uncompetitive bidder, re-open or close a regulatory investigation, endorse a product or service by attending functions or, simply, allow access to a site or a system by an unknown person.

Here are some concluding thoughts. How should organisations react to these challenges? What should they do at a conceptual level to ensure that they become ever more resilient at the human as well as the technological level? Analogies are very useful – one of my favourites is that of an immune system. Organisations should feel the need to expose themselves to attenuated or synthetic pathogens (as with vaccinations) and thereby grow resistance as well as having a generally 'fit' system that is capable of avoiding obvious potential harms. This should include reacting as well as possible when a compromise does occur (the equivalent of infection by an unknown parasite, virus or bacteria). From a combination of enhanced sensors (to avoid), cognition (to anticipate) and rapid response (the reflexes) the building of immunity is acquired. Just as immune systems in bodies are protected by a perimeter (such as the skin and devices to prevent the ingestion of bacteria and virus-laden objects, such as the *Vibrissae* hairs of the nasal passages) – so the technological perimeter of cyber is just one of which must be an integrated, agile and adaptive suite of approaches to socio-technical security.

Conceptualising the immune system idea in practice is no doubt challenging. However, it is a way of achieving higher levels of protection required in an ever more turbulent world where the privately owned critical national infrastructure may be a target for adversaries, and where outages are not tolerated by either consumers or investors. The planning for and response to cyber incidents must be underpinned by a broad definition of just what cyber can involve (i.e., any computer-mediated communication) in shaping, restricting or determining the decision-making of the targeted organisation and individuals. As Ernst and Young have recently stated: "being in a proactive position to anticipate and mitigate cyber threat is one of today's most important business objectives" (Ernst and Young, 2015: 1). ■

REFERENCES

Business, Innovation and Skills, Department for, 2014 *Information Security Breaches Survey:* Technical Report, available at www.pwc.co.uk/assettts/pdf/cyber-security-2014-twchnical-report.pdf

Ernst and Young, *Cybersecurity and the Internet of Things,* in Insights on Governance, Risk and Compliance, March 2015.

McKinsey and Company, How good is your cyberincident-response plan? (2013), available at: http://www.mckinsey.com/insights/business_technology/how_good_is_your_cyberincident_response_plan

ABOUT THE AUTHOR

Dr Mils Hills, is the first security anthropologist employed by the UK government, and has unique experience and expertise in cyber-, human factors and other forms of risk. His intellectual work is of the highest calibre, disruptive to conventional approaches and guided by a commitment to deliver findings that make a difference.

He began his career with the Ministry of Defence, and later headed a national SME team targeting, protecting and defending decision-making. He was then seconded into the Cabinet Office's nascent Civil Contingencies Secretariat (CCS). Working on national strategic capability across departments, he developed a unique suite of exercise, research and analysis tools that rapidly tested and reinforced resilience to a wide range of challenges.

Between 2005-10, he ran Analytic Red LLP - providing the same services to public and private sector organisations. In 2012, he joined Northampton Business School and has been appointed as Associate Professor in Risk, Crisis and Corporate Security Management in 2013.