Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Is the responsibilization of the cyber security risk reasonable and judicious?

Karen Renaud[a,*], *Stephen Flowerday*[b], *Merrill Warkentin*[c], *Paul Cockshott*[d], *Craig Orgeron*[e]

[a] *Abertay University, Dundee, Scotland, United Kingdom*
[b] *Rhodes University, Grahamstown, South Africa*
[c] *Mississippi State University, Mississippi State, Mississippi, USA*
[d] *University of Glasgow, Glasgow, Scotland, United Kingdom*
[e] *MS Department of Information Technology Services, Jackson, Mississippi, USA*

ARTICLE INFO

Article history:
Received 6 April 2018
Revised 6 June 2018
Accepted 30 June 2018

Keywords:
Cyber security
Responsibilization
Neoliberalism
Risk regulation
Hierarchism
Risk management

ABSTRACT

Cyber criminals appear to be plying their trade without much hindrance. Home computer users are particularly vulnerable to attack by an increasingly sophisticated and globally-dispersed hacker group. The smartphone era has exacerbated the situation, offering hackers even more attack surfaces to exploit. It might not be entirely coincidental that cyber crime has mushroomed in parallel with governments pursuing a neoliberalist agenda. This agenda has a strong drive towards individualizing risk i.e. advising citizens how to take care of themselves, and then leaving them to face the consequences if they choose not to follow the advice. In effect, citizens are "*responsibilized*." Whereas responsibilization is effective for some risks, the responsibilization of cyber security is, we believe, contributing to the global success of cyber attacks. There is, consequently, a case to be made for governments taking a more active role than the mere provision of advice, which is the case in many countries. We conclude with a concrete proposal for a risk regulation regime that would more effectively mitigate and ameliorate cyber risk.

1. Introduction

Cyber crime and other cyber risks show no signs of abating, making the securing of devices and computers more challenging with each passing year (Kröger, 2008; Pfleeger and Caputo, 2012). Yet it is a relatively recent phenomenon. Cohen (1987) traces the first computer virus back to 1983, whereas physical crime is probably as old as humanity itself. We, as a species, have had centuries to learn how to secure our physical property and belongings (Roth, 2014). The cyber crime threat, however, is mere decades old.

Cyber security risk, especially the malicious actions of cyber criminals and their tools (e.g. malware), is fundamentally different from other crime risks, and far more challenging for a number of reasons. In the *first* place, the cyber crime field is fluid and adapts very quickly (Choo, 2011; Andreano, 1999). *Secondly*, much of the software pre-installed on personal devices is vulnerable to attack (Bishop, 2002; Subashini and Kavitha, 2011). *Finally*, the non-expert device owner sometimes inadvertently compromises security for a variety of reasons (Granger, 2001; Riley, 2006). These factors combine to ensure that cyber criminals easily find vulnerabilities to exploit. The average citizen who owns any kind of smart device seems

* Corresponding author.
E-mail address: k.renaud@abertay.ac.uk (K. Renaud).

https://doi.org/10.1016/j.cose.2018.06.006
0167-4048/

to be particularly vulnerable to attack (Nthala and Flechais, 2017; Imgraben et al., 2014). Small businesses also struggle to defend themselves[1] (Renaud, 2016).

If we consider the fact that 21st century citizens increasingly own multiple computers, often carrying one in their pockets as they go about their day-to-day lives, and that our homes and cars are also hyper-connected in this emerging age of "Internet of Things" (IoT), we have a 'perfect storm'. The current situation is one within which millions of device owners are vulnerable to being exploited by increasing numbers of technically competent and innovative hackers across the globe.

Yet most governments do not actively support citizens in terms of mitigating the cyber risk the way they act to regulate other, older and more well-known risks. They have well-established structures and institutions to manage a variety of health, safety and physical crime risks. The way these risks have been managed has been refined over many centuries (Lentz and Chaires, 2007; Hooker, 1849). For example, to mitigate physical crime risk, policemen patrol the streets and actively monitor public behavior. They have finely honed techniques for crime prevention. Crime investigations and prosecutions are mature fields informed by well-established academic disciplines. The fire safety risk, too, is scrupulously regulated, with educational drives reaching most members of society. Safety science, too, is a mature field, requiring organizations to ensure that workplaces are safe and fire hydrants are available. Specialist firefighting teams respond to reported fires.

In sharp contrast, the computer owner of 2018 is largely held responsible for managing his/her own cyber security (Horgan and Collier, 2017). In the *lingua franca* of the millennium, the computer owner has been *responsibilized* when it comes to managing the cybercrime risk. We believe this to be an accurate characterization because there is very little support from the government or governmental bodies in terms of actively helping people to manage their cyber defences, nor is an official safety net put in place to support those who do fall victim to cyber attacks. As things stand, the most pervasive official strategy is the provision of advice. There is very little sign of the supportive infrastructure that one sees in areas such as physical crime, health and safety.

In this paper, we will consider the advisability of this approach to cyber security risk i.e. the responsibilization agenda. We will examine and critique the responsibilization approach, and compare it to older, more effective and well-established risk management regimes. We will detail the different cyber crime risk descriptors, and the factors contributing towards the risks all device owners are subject to.

There are two questions we wish to answer in this paper, given the complexity of computer networks and systems, the newness of the cyber crime risk, the sophistication of the cyber criminals, and the ubiquity of personal computers:

(1) Is it *reasonable* to assign responsibility for cyber security to device owners and users? *In other words*, can device owners be expected to possess the knowledge and skills required to manage the risk effectively?
(2) Is the cyber security responsibilization agenda *judicious*, given the widespread impact of cyber attacks? *In particular*, is the risk of such a nature that the failure of a small number of device owners to manage their personal risk will lead to harm for large numbers of other account and device owners?

We will commence by making an argument for the fact that device owners are indeed being responsibilized for their cyber security risk (Section 2). In Section 3, we introduce the concept of risk regulation regimes and cultures and provide some examples of how this is achieved. We then consider the cyber security risk, contemplating its nature, as compared to other risks. Section 5 proposes a more appropriate cyber security risk regulation regime before Section 6 concludes.

2. The responsibilized individual

In the context of risk and threats, it is widely presumed (and accepted) that individuals should and will make responsible life choices to improve their own well-being, though we also often engage in some degree of risky behavior. This phenomenon of expecting individuals to shoulder the responsibility for avoiding risk is referred to as 'responsibilization.' Hannah-Moffat (2001) explains that responsibilization is a technique used by neoliberal governments that requires individuals to take deliberate action to reduce their vulnerability to a number of risks, i.e. not expecting the state to assume full responsibility for taking action. The subtext seems to be that they should then expect to shoulder responsibility for negative outcomes that might occur if they fail to take advised precautions.

The term 'responsibilization' suggests a shift in responsibility from government to individual, under the assumption that this gives citizens the autonomy and agency that they are entitled to (Wakefield and Fleming, 2008). Wakefield and Fleming explain that this trend is driven by the assumption that the agent being made responsible has, thus far, avoided their duty or that the responsibility was previously, erroneously, assigned to a government body, but that it is now being restored because this is the right thing to do. Over recent decades, there has been a shift from governments focusing on social and collective values to a notion of individual responsibility (Comack and Peter, 2005).

Biebricher (2011) explains that responsibilization governs people by means of their freedom. In essence, the regime ascribes to the principle that the individual citizen should be given choice, freedom, and responsibility. Citizens are given advice on what actions to take, made responsible for the actions they choose to take, and then have to accept the outcome, good or bad.

This concept appears to have been internalized by many 21st century citizens. When a major security incident occurs and reaches the news media, the first reaction is often to find

[1] http://www.scotsman.com/news/nearly-70-of-uk-firms-have-no-staff-training-for-cyber-attacks-figures-show-1-4537695.

someone who is at fault; someone to shoulder the blame. It is often the victim him or herself who is blamed for what has happened to them. Consider, as an example, the ransomware attack of May 2017. Journalists soon assigned the moniker "WannaCry" to evoke the understandable response to falling victim. Some of the first news reports blamed the event on a user falling for a phishing message.[2] When that was refuted, subsequent reports blamed Microsoft for not patching Windows XP machines.[3] Then it emerged that Microsoft had indeed released a patch. The media then started pointing fingers at the UK's National Health Service (NHS) for not applying the patches[4] and the UK government for underfunding the NHS.[5] The blame then shifted to the intelligence agencies such as the USA's National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ) for not playing their part in preventing these kinds of occurrences.[6] The latest 'guilty party,' as we write this paper, is the North Korean government, who is being blamed for launching the WannaCry attack.[7] It does not seem to occur to journalists that this kind of event results from systemic failures: a number of factors coming together to allow such a wide-scale ransomware event to propagate and flourish.

2.1. *Examples of responsibilization*

Garland (2001), cited by Lynch (2002), explains that those who commit crime have to take responsibility for it, despite any social aspects that may have influenced them to commit such crimes. Victims of crime are also somehow implicated in the crime, owing to not having taken deliberate action to make themselves less vulnerable (Hollway and Jefferson, 1997; Kennedy and Sacco, 1998). A common example of this is blaming rape victims for dressing provocatively and thereby bearing some responsibility for their rape (Grubb and Turner, 2012).

Unemployment, which used to be considered related to economic causes, and a matter for governmental concern (Kenyon, 1997; Lindvall, 2010), is now considered a personal responsibility failure (Biebricher, 2011). Health, too, is often presented as a personal responsibility, with the powers-that-be ignoring the fact that disease processes are stochastic, being the outcome of a multiplicity of causes, only some of which, in some pathologies, are in any way influenced by personal decisions (Rossiter, 2012).

Even the most marginalized members of society are held responsible for their situation. Scoular and O'Neill (2007) describe how the UK government changed its approach to encouraging people to exit prostitution. They argue that while the government sells its new approach as being one of social inclusion, it actually epitomizes the responsibilization agenda. Scoular and O'Neill (2007) cite Melrose, 2006, Sanders, 2007 to make the argument that this approach frames involvement in prostitution as an issue of personal responsibility. A model of reform emerges which is centred on individual interventions designed to assist women to exit from sex work and resume 'normal' lifestyles. Increasing emphasis is placed on counselling, support and retraining to overcome victimhood and re-enter normal society. One could contrast this with the Swedish Social Democratic model in which the state intervenes actively to prevent sexual exploitation by prosecuting those who pay for sex (Ekberg, 2004).

The responsibilization trend is even happening in areas that have traditionally been the responsibility of organizations and government. In Canada, there is a move towards responsibilizing employees for health and safety violations in the workplace (Gray, 2009). Skinns (2003) explains how the UK government has made communities and non-state actors shoulder some responsibility for crime control. Even the problem of pirates, which would traditionally have been dealt with by nation states, is being responsibilized, with shipping companies being expected to repel pirates without necessarily expecting assistance from armed forces (Spearin, 2010). In Texas, the government is encouraging citizens to assist border control authorities by watching live streams from surveillance cameras and alerting the authorities should they spot someone trying to enter the USA illegally (Koskela, 2011).

The neoliberal message, and agenda, is that "*Whether it is the labor market, retirement, health care or crime, individuals are activated and encouraged to take care of themselves*" Biebricher (2011) [p.472].

2.2. *Unintended consequences*

Biebricher (2011) argues that there are some people who are simply unable to be fully responsible for all aspects of their lives, for a variety of reasons. In addition, Ehrenberg et al. (2010) talks about people developing a weariness, which could result in drug or alcohol abuse, simply because they do not have the wherewithal to deal with all the decisions they have to make and the choices that lie before them. Rossiter (2012) emphasizes that the responsibilization of health, as one example, could lead to people becoming anxious, guilt-ridden and hyper-vigilant. The same argument is made by Stol et al. (2016) who talk about omnipresent and frequent health checks leading to people erroneously holding themselves responsible for particular health issues. They refer to this as *over-responsibilization*. Phoenix and Kelly (2013) report that responsibilization can lead to people, in their case young offenders, feeling that no one can help them to change their lives and improve their outcomes.

On the other hand, Soneryd and Uggla (2015) point out that responsibilization can also lead to resistance, instead of compliance. Skinns (2003) investigated an attempt to make the local community responsible for crime and disorder. He reports a rather disappointing outcome, with community partners not being treated as equal stakeholders, and this leading to delays and obfuscation rather than a combined and concerted effort that effectively curtails crime.

[2] http://www.techguylabs.com/episodes/1389/wannacry-latest-phishing-ransomware-attack.
[3] https://www.engadget.com/2017/05/13/Microsoft-WindowsXP-WannaCrypt-NHS-patch/.
[4] https://www.scmagazineuk.com/wannacry-update–who-is-to-blame-and-are-we-facing-round-two/article/661486/.
[5] https://www.scmagazineuk.com/wannacry-in-the-nhs-who-takes-responsibility/article/661492/.
[6] https://www.theguardian.com/technology/2017/may/15/who-is-to-blame-for-exposing-the-nhs-to-cyber-attacks.
[7] https://www.theguardian.com/technology/2017/jun/16/wannacry-ransomware-attack-linked-north-korea-lazarus-group.

Garland (2001) argues that responsibilization occurs more at the level of rhetoric than reality and, certainly, Skinns (2003) report seems to confirm that the concept is not as effective as the politicians would have us believe.

2.3. *Cyber crime risk*

Responsibilization is defined as a technique of neoliberal governance and crime control that expects and requires individuals to take reasonable precautions thereby minimizing their risk of becoming victims. If they fail to take all the right precautions and fall victim, a certain degree of responsibility for the consequences rests with them (Yan, 2015). If we pick this definition apart it seems to have two critical elements characterizing a responsibilized risk:

(1) the requirement for Jo Citizen to take precautions to reduce the probability that they will fall victim, and
(2) the fact that they have to accept some or all of the blame, and all the consequences, if they do fall victim.

Let us now make the case that cyber security has been responsibilized. *Firstly*, governments, such as the UK and the USA, issue a great deal of advice about what actions people ought to take to protect their devices and home computers (Renaud, 2016). Hence the "responsibility" rests on their shoulders. This satisfies the first element of the definition. *Secondly*, if they *do* fall victim, they are often blamed for not taking precautions, with evidence of this attitude in the public media[8]. They are given no help in dealing with the consequences of their victimhood. It could be argued that this looks very much like victim blaming, but it also does satisfy the second element of the definition.

In essence, the current situation is one in which a great deal of advice, much of it conflicting (Renaud, 2016; Renaud and Weir, 2016), is provided by a range of institutions and government departments. Most governments do not act to offer services to help computer owners in the way they offer health care and fire-fighting assistance. If Jo Citizen falls victim to a cyber attack they have to cope with the harm that ensues, with little to no help from anyone in authority in terms of recovering from the attack.

We thus conclude that many governments are responsibilizing the cyber security risk.

However, it could be argued that responsibilization only works when those who are responsibilized are indeed able to accept and manage that responsibility. If they lack the skills or requisite emotional stability they will not be able to take responsibility for managing a particular risk. Cyber security does not meet these requirements.

Rycroft and Kash (2002) argue that the complexity of technology punishes individualism and rewards collaboration. They wrote this in 2002, long before cyber security had become the huge issue it is today. Their arguments appear to apply equally to the cyber security field as to innovation, the field they wrote about.

We examine more mature risk regulation regimes in the following Section before returning to the cyber crime theme.

[8] https://edscoop.com/human-error-majority-k-12-education-data-breaches.

3. Risk regulation

It is instructive to consider how we currently defend ourselves against various kinds of other risks. Consider burglary, as a different kind of crime. Individual citizens are expected to act sensibly and take precautions, such as locking their homes and not leaving their belongings lying around. In some parts of the world, homeowners are encouraged to own firearms to act as a deterrent to criminals (e.g. Kennesaw, USA[9]). Many people own dogs and put bars over their windows. If crimes occur, police forces and courts will pursue and prosecute miscreants; hence, responsibility for managing the risk is shared by individuals and the state. Individuals act to minimize their vulnerability, and the state then acts to remediate by catching, prosecuting, incarcerating and, in some cases, assisting in rehabilitating the criminals who exploit such vulnerabilities. As criminals formulate new kinds of crimes, police forces update their advice, ensuring that deterrence efforts are current and up to date. They also issue advice to individuals in terms of how to protect themselves, i.e. what precautions to take, and how to deter criminals.

This description refers to what Hood et al. (2001) call a "risk regulation regime". Risk regulation regimes, Hood et al. argue, are essentially cybernetic systems, with multiple interacting parts. Fuenfschilling and Truffer (2014) explain that such systems naturally evolve into stable configurations whereby societal functions are best served. Accordingly, such regimes can be characterized by a number of different interacting features i.e. "descriptors," denote the way societal risks are managed within societies and countries.

3.1. *Risk regulation descriptors*

Hood et al. (2001) explain that risk regulation has two important crosscutting descriptors (Fig. 1). The first is related to how the regime carries out its core *activities*, and the second describes the *features* of the specific regime. Both of these are specific to the regime and serve to distinguish and characterize it.

The first activity-related descriptors comprise three basic *Activities* that characterize any control system: (1a) *information gathering*, (1b) *standard setting*, and (1c) *behavior modification mechanisms*.

The second feature-related descriptor pertains to the (2a) context and (2b) content of the regime. *Context* has three components: (a) type of risk, (b) public preferences and attitudes, and (c) organized interests. *Content* includes (a) size, (b) structure, and (c) style.

The contextual components are self-explanatory, but we will briefly detail the content elements here. The first, *size*, reflects the amount of regulation applied to a given risk. We also measure size in terms of how aggressively the regulations are applied and in terms of the monetary investment made by the regime.

[9] https://www.aol.com/article/2016/07/28/5-american-cities-that-require-you-to-own-a-gun/21439364/; https://edition.cnn.com/2018/03/06/us/kennesaw-georgia-gun-ownership/index.html.

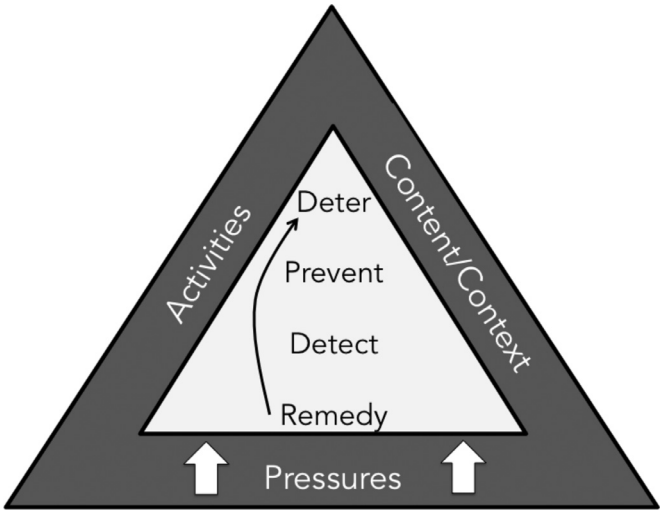

Fig. 1 – Cyber crime risk regime regulation pressures & activities (Derived from (Hood et al., 2001) and (Straub and Welke, 1998)).

The second is *structure* and refers to the way the regulation is organized: to what extent public and private actors are involved, and the extent to which compliance activities are distributed between actors.

The final component is *style*, which denotes the conventions and attitudes of those who apply the regime. Different risks have regulations that are enforced with varying levels of zeal, which are reflected in this component.

Regimes are also influenced by a number of *Pressures* that inform the nature of the risk regulation regime.Hood et al. (2001) suggest that at least three pressures shape risk regulation regimes: (3a) market failure, (3b) public opinion and (3c) interest groups. They also mention (3d) the impact of path dependencies and historical points of origin in influencing the activities and characteristics of risk regulation regimes (Baumgartner and Jones, 1991; Thelen et al., 1992). Fig. 1 is derived from the concepts proposed by Hood et al. (2001) and Straub and Welke (1998).

3.2. *Cyber security management*

In the context of information security, Straub and Welke (1998) propose a Security Action Cycle, comprising four successive activities: (1) deterrence, (2) prevention, (3) detection, and (4) remedies. In order to carry this out, employers and governments formulate a tailored risk management or regulation stance, reflecting their approach to the particular risk, i.e. who is responsible for each activity.

In terms of Straub and Welke's Security Action Cycle (Straub and Welke, 1998), the state's standard-setting activities act to deter. The state engages in a number of actions to prevent risks: it gathers information to detect people engaging in risks, and it remediates once people's misbehaviors are detected (behavior modification). Fig. 1 depicts these activities as being core to Cyber Crime Risk Management.

3.3. *Government risk management culture*

The final characterization proposed by Hood et al. (2001) is that of governmental culture, as follows:

1 *Fatalist*: this approach is essentially that little is done to avert the risk, but a response is formulated by government, as and when the event occurs. Example: responses to natural disasters.
2 *Hierarchist*: whole-society solutions are developed, informed by expert forecasting and management. Examples: Automobiles and UK management of dangerous dogs.
3 *Individualist*: supports markets and underpins informed choice but responsibility is essentially the individual citizen's. Examples: Smoking and Cyber Crime.
4 *Egalitarian*: the government supports communities in managing the risk and encourages local participation. Government will step in once an event occurs. Example: Pollution reduction by providing public transport alternatives.

3.4. *Risk culture examples*

Individualist cultures place full responsibility on people themselves to manage risks. They can choose to avoid or take a risk, and face the consequences of their actions. Citizens, in these cases, are responsibilized. Smoking, for example, is considered to be an individual choice. The state issues advice about the dangers of smoking [behavioral modification], and some countries mandate warnings to appear on packaging and prohibit sales to minors [standard setting]. However, if a smoker gets lung cancer or emphysema, no one is prosecuted and the smoker, alone, bears the consequences of his or her actions. The notable key distinguishing feature here is that smoking damage is not contagious, but smoking in public spaces, where others could be affected by "second-hand smoke," is indeed the subject of numerous laws.

The smoking risk has two important characteristics. The first is that smoking hurts only the smoker herself. When second-hand smoke can affect others, legislation is often used to prevent this. As long as the smoker only harms herself, she is left to manage the risk. So, the risk is to the *individual*, not to the community, and the government does not intervene. The second characteristic is that people usually need assistance from those with *specialist* knowledge to reduce their risk when it comes to smoking. Governments and health professionals with this knowledge provide a great deal of advice to support people in dealing with these kinds of risks.

Personal household security is another individualist culture example. Much advice is issued by police services, and in some US states police services loan scribing devices to people so that they can ensure that their property is identifiable if stolen. Some people, however, may still choose not to lock their doors, or to leave their belongings unsecured. If these are stolen, even though the criminal may be apprehended and punished, the owner is not recompensed by the state. They have to accept the loss, whether it was caused by their own carelessness or was purely bad luck. Yet the police will come if summoned and will attempt to find and arrest the miscreant.

Egalitarian cultures tend to come into play when structures are provided which the government then expects *communities* to make use of. They might provide public transport, for example, to reduce road congestion. The community benefits if they make use of it, but it does not require any *specialist* expertise to use.

Hierarchist cultures are fundamentally different. To make this point, we will discuss (1) fire, (2) infectious diseases, and (3) automobiles, risks that are managed hierarchically. We will show that these risks share two particular characteristics: *firstly* they require special skills to manage and *secondly* that a failure to adequately deal with the risk affects the community at large.

(1) *Fire* is indispensable, but it also kills and maims. Accidental fires are *calamitous*. The need for fire vigilance and firefighting is as old as humanity itself. The Roman emperor Augustus instituted a corps of firefighting vigils ('watchmen') back in 24 BC (Tacitus, 1942). Yet fire still remains untamed centuries later, as evidenced by a number of terrible fires (Associated Press, 2016; Reddaway, 1951; Sammarco, 1997; Sawislak, 1995). It is a sad reality that it is not a simple matter to prevent, fight or contain the fire risk (Associated Press 2016).

How have the powers-that-be attempted to address the risk of fire through the ages? Initially individuals in a community were responsibilized (ushistory.org 1995). Later, public bodies started to pass laws to compel people to take measures to prevent fires, most notably cleaning chimneys regularly (Mohun, 2013). However, people were too busy trying to make a living and had no energy to expend on fire prevention. Thus, responsibilization failed and government intervention was required.

The next step in the fight against fire was to establish a society of firefighters who were specialists and could fight fire effectively, far better than the public could. The state paid for these, and the shift in responsibility from individuals to responsible authorities took place.

Fire management today is a healthy mix of prevention and firefighting. Legislation exists to compel certain preventative measures, and fire crews are available at short notice to deal with the fires that do occur. Many organizations regularly train their employees in firefighting, and children are taught basic 'common sense' with respect to fire.

In essence, the state enacts legislation to ensure that preventative measures are taken, that building codes are followed (prevention in the form of standards setting). They also ensure that advice is provided to the population to ensure that they know which preventative measures to implement (deterrence). Individuals implement measures to reduce their vulnerability (behavioral modification). If the worst happens, the state provides agents to manage fires that do occur (remediation, including information gathering). Finally, the state will investigate fires and prosecute those who have been criminally negligent or when they consider that fires have been started deliberately (remediation: behavioral modification and possible standard setting).

Fires demonstrate the two characteristics we mentioned at the outset. The first is that the fact that fires require *specialist* knowledge to prevent, manage and fight. The second is that they are potentially *calamitous* i.e. they often spread and affect many people and communities.

(2) *Infectious diseases* such as smallpox were initially managed by the women in a household. They nursed those who were ill. However, when smallpox reached epidemic proportions, the authorities realized that they would have to take action (Blake, 1959). Their initial action was to isolate those with the disease to try to halt its spread: mayors enacted quarantines, forced people to clean streets and burn the possessions of those who had died. Then came the discovery that inoculations could prevent people from catching smallpox. The Boston board of health, among others, established entities to inoculate the population and mandated vaccination (Albert et al., 2001). Those who refused vaccination (Mather, 1708) were subject to a $5 fine or a 15-day jail sentence (Anon 1902).

Consider where we are today, with respect to infectious diseases. When a serious infectious disease breaks out, governments or the World Health Organization intervene to quarantine and treat those who catch the disease so that it does not spread any further.[10] Moreover, vaccinations might be mandated to protect the uninfected population.

Infectious diseases also demonstrate the two key characteristics. The first is the fact that diseases require *specialist* knowledge to prevent, manage and treat. The second characteristic is that there are, by their very nature, *contagious* i.e. they often spread and many people fall ill.

(3) *The automobile risk* management culture is also hierarchist. The need for this kind of culture has become clear over many years as the number of cars on the roads increased and the associated risks thereof became evident.

[10] https://learningenglish.voanews.com/a/4398370.html.

Table 1 – Automobile risk regulation regime.

	Components	Characteristics
Context	Type	High risk of harm
	Public preferences	Low levels of public dread
	Organized interests	Mothers against drunk driving (MADD) in the USA; car manufacturers use safety as a selling point; local councils gain revenue from traffic fines [**behavior modification**]
Content	Size	High levels of statistics collection [**information gathering**]; high investment in regulation [**standard setting**]; high standards for highways [**standard setting**]
	Structure	Low levels of involvement from private organizations; low fragmentation; high levels of behavioral modification to improve safety [**behavior modification**]
	Style	High levels of regulation [**standard setting**] promoted zealously [**behavior modification**]

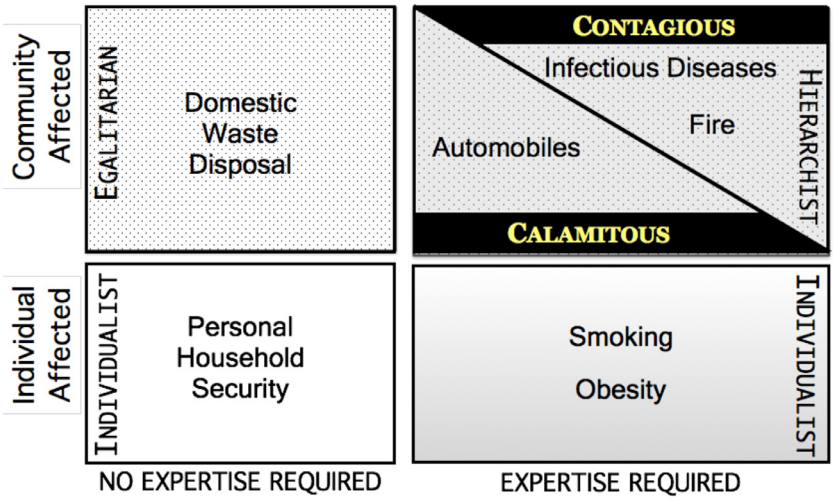

Fig. 2 – Risk Dimensions & regulation cultures.

Drivers are required to pass a competency test. Law enforcement officers enforce the road traffic regulations, all to ensure our safety.

Table 1 delineates the automobile risk regulation regime using the Hood et al. (2001) model.

The automobile risk again *demonstrates the two crucial characteristics:* the first is that one needs special *expertise* to drive an automobile, and the second is that other people on the roads (the wider *community*) are affected when someone drives badly: this is evidence of potential calamity.

In Summary: In the past, as society became more aware of the risks introduced by 'new' technologies, it has formalized measures and controls in order to manage these risks. Taking note that the Internet was designed with resilience, and not security, in mind, one can expect measures and controls to be introduced by society to manage the risk introduced by this new technology. The risk management culture will emerge as have the ones we have discussed in this section. We believe that the culture emerges from the characteristics of the risk itself, and in the following section we present two dimensions that we believe are key to the way the culture will develop.

3.5. *Risk dimensions*

We have identified two *dimensions* of the kinds of risks that seem naturally to indicate that a hierarchist culture ought to be instituted to manage them. These are:

1 *The expertise that is required to manage the risk*: The kind of knowledge required to regulate and manage the risk: either specialist knowledge not necessarily possessed by the wider community, or knowledge that the average citizen can be expected to possess.
2 *Who is impacted:* (a) *Individual* or (b) *Community*: Adverse events resulting from the risk impacts either the individual or the wider community.

Fig. 2 shows how different kinds of risks fit into a two-dimensional grid, depending on which of these characteristics they demonstrate. We also map these to Hood's risk regulation cultures.

When a risk is characterized by *both* of these dimensions, an individual's failure or inability to take responsibility, and act to mitigate the risk, affects the community at large. An uncontained fire quickly affects others, becomes *calamitous*, and mandates urgent action. A *contagious* disease spreads through the community. For risks demonstrating potential for either contagion or calamity, and a need for specialist knowledge, it is necessary for the state to formulate a hierarchist risk regulation regime and to provide a supportive infrastructure.

If the community is affected, but no special expertise is required, an *egalitarian* approach might be appropriate. The state can provide advice that people can apply, and put supporting structures in place. An example is domestic waste disposal,

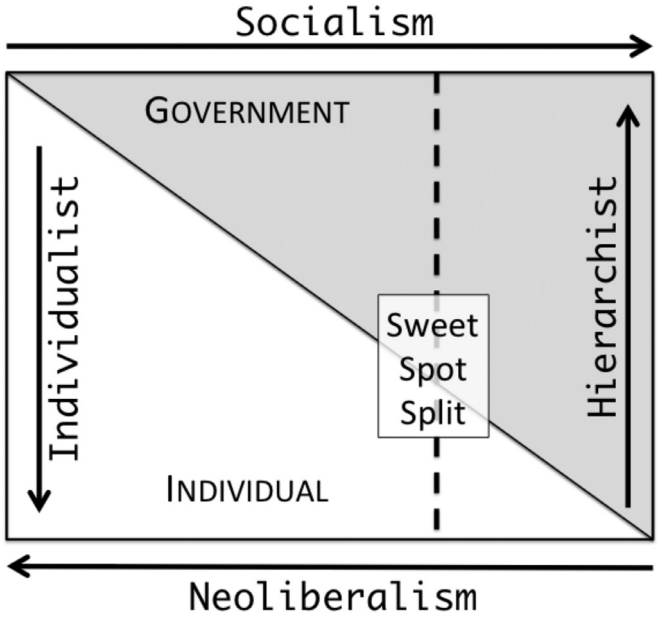

Fig. 3 – The dashed line is the "Responsibility Line" depicting differing participation levels of responsibilization.

which requires no special expertise, but does require the authorities to run a waste collection programme and provide secure bins for domestic waste.

If only the individual is affected, there is less reason for the state to become involved. This is especially the case when no special expertise is required. An example is personal household security. Houses are fitted with locks and people routinely keep their homes locked. If they fail, only they are affected and have to accept the consequences.

In each of the risk areas discussed above, cultures have shifted, over time. For many, such as fire, the responsibility shifted from being primarily an individual responsibility, to being egalitarian with communities doing their reasonable share, and finally ending up with a hierarchist risk regulation regime. Fig. 3 demonstrates the continuum upon which the responsibility split can lie. There is, of course, a balancing act to be found between the cost of 'big government' and the infringement of 'individual rights.' Thus, each culture or society, will determine what they are comfortable with for each particular risk.

Smoking lies at the far left of the continuum in Fig. 3. Contrast this to the current fire fighting management strategy, which is situated much further to the right, as discussed above.

The vertical "Responsibility Line" that runs through the rectangle in Fig. 3 can shift left or right, depending on how much or how little the government should be involved in risk management. This vertical line represents the *level of responsibility*. This shift will reflect differing national cultural values. In some countries, the line would be further towards the left and in others, it would shift right. Moreover, the responsibility line will shift within a country depending on the nature of the risk itself.

Cyber defence, we argue, is currently situated at the far left of Fig. 3 (as depicted in Fig 4), together with smoking in many Western countries, and this seems a poor match for the type of contagious and community-impacting risk that cyber crime constitutes. Thus, we advocate a shift to a hierarchist risk regulation regime (as depicted in Fig 5). We will argue this in the following section.

4. The cyber security risk

Digital information technology (IT) has been in existence for about 140 years and is still rapidly changing and evolving. If we take the 1870 invention of the Baudot teleprinter code as the starting point of digital IT, it was not until the Second World War that the first cyber security techniques were applied, with the Lorenz enciphering machines. The Lorenz device allowed a pseudo random bit stream to be Xored with the data stream, supposedly rendering it immune to eavesdropping. This cyber security measure, in turn, stimulated the invention of the first practical digital computer, Colossus, as a means of cracking the enciphered data transmissions (Cragon, 2003; Gannon, 2014). The 'hacking,' in this case, was carried out by a government research laboratory. Colossus set a pattern in which apparently secure digital systems have subsequently proven to be penetrable, if sufficient effort, intelligence, and processing power are applied.

Only in the last 25 years or so has a cyber security threat emerged that affects the public at large rather than governments alone. The emergence of this threat was made possible by the widespread use of standardized computers. The existence of a monoculture ecosystem (majority of computers using Windows) and the interconnectivity facilitated by the Internet made the spread of computer viruses elementary. The subsequent worldwide interconnection of all computers then offered new vectors of transmission, and the possibility of remote theft of data. Computing is not the first technology to bring, in its train, new hazards.

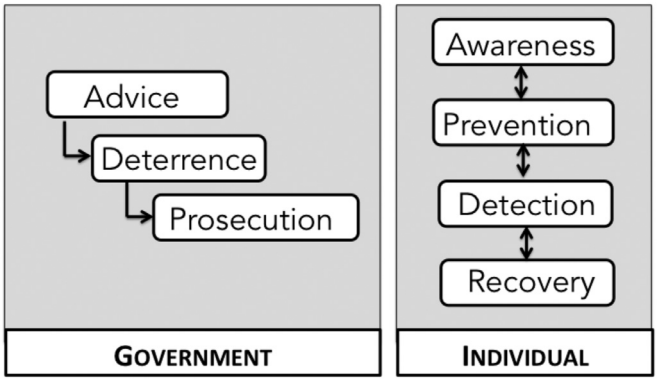

Fig. 4 – Current cyber security risk management regime.

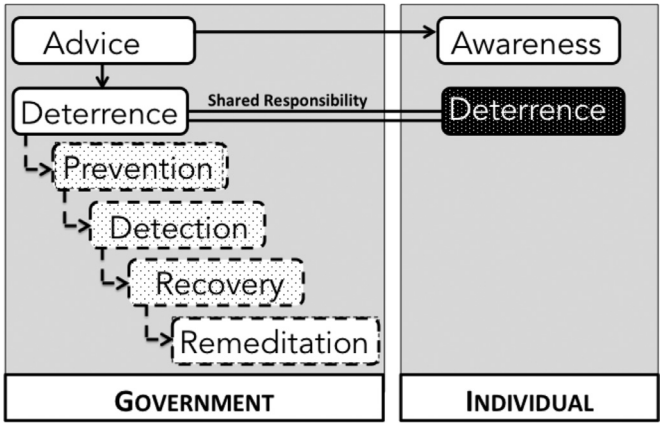

Fig. 5 – Cyber security risk management regime (Dashed lines depict shifted responsibility).

Table 2 – Current cyber security risk regulation regime.

	Components	Characteristics
Context	Type	High risk of attack
	Public preferences	Newspaper reporting of widespread attacks but general apathy amongst general public
	Organized interests	Many security companies offer support to organizations, many standards bodies publish advice and standards (e.g. NIST) but little or no standard setting by governments
Content	Size	Very few reliable statistics related to the size of the risk; very little investment in regulation
	Structure	No investment from private sources; multiple advice given by different bodies
	Style	Low levels of regulation; difficulties in prosecution

4.1. *Current cyber security risk management & regulation regimes*

Society has embraced the Internet and most governments have adopted a neoliberalist approach to cyber security. We consider that device owners and users have essentially been responsibilized (Biebricher, 2011), a case we made earlier. Moreover, the cyber security risk demonstrates both characteristics that situate it within the top right quadrant of Fig. 2: cyber attacks are ***contagious***, and managing the risk requires *specialist* expertise.

As outlined in Fig. 1, the current cyber security risk regulation regime descriptors are as shown in Table 2. There is little evidence of standard setting or information gathering, and the only behavioral modification activity tends to be the provision of advice.

The current approach in many countries, with respect to a cyber risk management governmental culture, is individualist: the so-called responsibilization of the individual. Back in 1988, when computers started to diffuse into organizations, Dray (1988) wrote of the need for government to establish clear guidelines for the security measures that ought to be taken. He argued that this would help organizations to deal with the complexity of the issue. This action seems even more crucial now that society at large is grappling with IT security issues. Yet at the moment, of Straub and Welke (1998) activities, the

government engages primarily in deterrence in the form of advice and awareness campaigns. Prevention is left to device owners. Detection is challenging owing to the relative invisibility of the crimes, yet there is little support from the powers-that-be in this respect. The global distribution of cyber criminals makes remediation even more challenging.

4.2. *Need for a new approach?*

Responsibilization has, at its core, the assumption that the government's only responsibility is the provision of good advice, the provision of services that the person may choose to benefit from, and perhaps the execution of post-event detection and prosecution. There are, however, a number of problems with this approach:

- The fact that this advice comes from the government, and thus has authoritarian undertones, might mean that it is not universally embraced and accepted, especially when trust in governments is at a record low (Muro and Vidal, 2017).
- Soneryd and Uggla (2015) suggest that such a hegemonic approach is not guaranteed to responsibilize people. If the responsibilization does not work, the risk is essentially unregulated and the consequences will be harm.
- A purely information-based delivery approach, in bringing about behavioral change, has proven to be less than efficacious in other areas (Gardner and Berry, 1995; Geller, 1981; Midden et al., 1983; Jordan et al., 1986; Geller et al., 1983; Bada and Sasse, 2014).

We have to ask whether, despite all the officially issued advice, individuals are sufficiently aware of cyber security risks and are capable of prevention and recovery mechanisms. It would seem from the daily reports of successful cyber crimes that the current responsibilization of device owners is not effectively deterring attackers.

Certainly, there are actions that the individual can take. Making backups is one of these but doing this correctly is not necessarily understandable to the non-expert. For example, keeping the backup disk connected 24/7 is a mistake because ransomware will simply encrypt the backup as well as the main hard drive. It is hard to measure the knowledge of the general population in this respect, but the devastation experienced by WannaCry victims suggests a lack of knowledge.

The task of securing personal systems and devices is undeniably challenging, and might be impossible for untrained individuals. That being so, it is *unreasonable* to responsibilize individuals when it comes to cyber security.

Moreover, there is a strong similarity between the spread of computer and biological viruses. In fact, ransomware often spreads when a cyber-criminal gains access to someone's email account and subsequently distributes the malware to all the person's contacts 'under false colors.' The kind of risk regulation regime that eventually proved effective against the biological viruses may be required to regulate cyber viruses. Other kinds of computer-related risks, such as hard drive failures, are *calamitous* rather than *contagious* and could benefit from the application of techniques used to deal with such risks in other sectors. Allowing one insecure computer to compromise many others without hindrance, because its owner lacks expertise and is unsupported, is clearly *injudicious*.

In summary, the cyber security situation shares the key characteristics of the other areas we studied with hierarchist regimes. Firstly, cyber security requires a level of technical *expertise* that is relatively rare in the general population. Expecting them to manage their own cyber security is likely to be *unreasonable*. Secondly, if an individual fails to secure his device, it very quickly becomes a *community* issue, and is *injudicious*.

5. Cyber security regime proposal

Geels (2010) explains that socio-technical systems occupy three kinds of configurations. The first of these is the niche, followed by a more stable socio-technical regime, followed finally by an exogenous socio-technical landscape. He explains that changes in regimes do not happen easily, because systems favor incremental changes rather than extreme shifts to a new way of doing things. Yet, as discussed above, mechanisms for regulating fire, contagious diseases and automobile risks have indeed made these transitions. The stable socio-technical systems we see today serve us well because our ancestors saw the need to make transitions from an individualist to more community-based hierarchist approaches.

If we consider the historical shift to a more hierarchist approach, as demonstrated by the progression in other established fields that display contagion and require expertise, cyber security risk management is in its infancy and it is perhaps time for us to consider a step change.

It seems more appropriate for the responsibility to be shared between the individual and the state, with the individual being required to take certain simple preventative measures and the state taking care of the rest. It does seem that we can prevent a great deal of cyber crime by accelerating the de-responsibilization process to arrive at a more hierarchist approach. The sedate historical pace of responsibility shift characterizing the other risk areas is infeasible in the cyber domain.

Combating the cyber security risk seems to mandate a hierarchist approach. Efforts are required from all stakeholders: the individual, institutions, and the state. Many governments favor responsibilization with a neoliberal approach. However, based on the current relatively unhampered success of cyber criminals, this approach demands reconsideration.

Neoliberalism and responsibilization will probably not be abandoned any time soon. There are many examples of cases where responsibilization has indeed proved efficacious. Yet, based on our discussion, it does seem that what might be best, for cyber security, is more of a partnership between state and individual citizen.

5.1. *Cyber crime*

O'Driscoll (2018), reporting on cyber crime trends, says that cyber crime was the 2nd most reported crime in 2016, 41% of people, globally, are not able to identify phishing emails, and 35% of consumers in 21 countries do not protect their personal

devices from viruses and malware.[11] This gives some indication of the size of the risk.

This state of affairs, as a global issue, has buttressed the argument for the protection of corporations, but also individuals, from the untoward use of the Internet by illicit actors. Authors and academics have, in the last handful of years, called for multi-stakeholder Internet governance (Kuehn, 2014), given the rising concern of national security as a key consideration in the formulation of public policy. Yet, evolving and advancing cyber security challenges persist and plague nations as well as individual citizens, as the governance of cyber security is highlighted as a crucial element to the security of a nation (Christensen and Petersen, 2017; Hathaway and Stewart, 2014; Kello, 2013).

For international cooperation in the development of shared policy and governance associated with the Internet and the mitigation of cyber security risks, Cowhey and Aronson (2017) argue for development of a common international policy framework. This realization sparked the establishment of the Global Commission on Internet Governance (GCIG) in January 2014. The Commission, and the subsequent report, *Toward a Social Compact for Digital Privacy and Security* (Global Commission on Internet Governance (GCIG) 2015), advocates for the creation of a new social contract between citizens, government, civil society and the Internet technical community, with the "*goal of restoring trust and enhancing confidence in the Internet*" (p.1).

While individual nations have developed and circulated a unique national cyber security strategy, which vary in domestic focal points and methods (Luiijf et al., 2013), numerous countries and international bodies pursued common ground forging mutual obligations on cyber security via the Draft International Code of Conduct for Information Security (Lkhagvasuren, 2017).

These developments provide confirmation of a growing global awareness of the need to formulate a cyber crime risk management regime.

5.2. *Cyber risk management*

Although a pattern has emerged in terms of how society has addressed risk in the areas we describe (e.g. fire, infectious diseases, and automobile), a clear pattern has not yet emerged in terms of how we ought to deal with cyber risk, in particular. We attribute this primarily to the complexity and relative recency of the risk, the continuously-changing nature of the field, and the fact that it requires a significant amount of expertise to manage. What is clear is that we cannot take as long to work out how to manage the risk effectively as we, as a species, took to manage fire and contagious disease.

A major contributing factor to both the complexity and urgency of this is the fact that cyber risk knows no geographical boundaries. This situation has been exacerbated by the emergence of the Internet of Things. Without stifling innovation and limiting the Internet, it is quite reasonable to assume that the individual is unable to defend him or herself against cyber-attacks. Attempts are made but are quickly overcome by the evolving nature of the risk and the sophistication of modern hackers (Voiskounsky and Smyslova, 2003).

The argument for responsibilization, in this case, could be seen as the government abdicating its responsibility. Maybe they, too, are overwhelmed. Within the sphere of cyber risk, the individual citizen has been introduced, within the short space of 25 years, to the Internet, email, online banking, social media, gaming, smartphones, and storing their content in the cloud. Each of these has multiple vulnerabilities. Furthermore, governments and larger organizations have been familiarized with a 24/7 operating schedule, concerns of critical infrastructure failures or attacks, privacy concerns, online espionage and terrorism, and remote access breaches. All of these risks require reconsideration and re-evaluation of the way we live and work. Although empowering the individual is certainly laudable, the complexity of cyber risk demands that governments act proactively to address this risk. This ought to take place to support and protect the individual citizen, organizations and their own information and systems.

5.3. *Hierarchist cyber security regime proposal*

If an individual citizen is unable to take sufficient action to protect themselves then they need to be able to rely on the state to step in. Begg et al. (2017) argue, "*personal mitigation measures should not be seen as a substitute for state support.*" [p. 605].

In accordance with the hierarchist regime, the state ought to act on three fronts: (1) standard setting to prevent and ease management, (2) information gathering by encouraging reporting of cyber crime and establishing skilled cyber crime units to provide advice and help citizens to manage such risks; and (3) behavioral modification by applying sanctions to those who do not follow preventative advice or adhere to standards. Dray (1988) argues that these kinds of activities will serve to demonstrate top-level commitment to cyber security and will encourage organizations and individual citizens to take it more seriously.

Individual Responsibility:

- *Prevention & Deterrence* (behavioral modification): Individuals are given a list of preventative measures to take. Instructions should be easy to follow and help centers should be available to give advice on implementing these.

Government Responsibility:

- *Deterrence* (behavioral modification): Ensure that advice is provided to citizens to make sure that they know which preventative measures ought to be implemented (e.g. Hatmaker, 2018). Additionally, there should be a 'measure' in place to evaluate whether the individual understands the advice.
- *Prevention* (standard setting): Provide clear guidelines for prevention measures. Legislate to ensure that organizations implement these measures. This would involve setting legally enforced technical standards for the cyber security of hardware, operating systems, email systems and financial transaction systems. Such standards would be analogous to the technical standards that are enforced for aircraft, trains or nuclear power plants.

[11] https://www.symantec.com/security-center/threat-report.

- *Detection* (information gathering, standard setting, and behavioral modification): The government needs to ensure that people do indeed take the required prevention measures and there should be very real consequences for not doing so. This is modeled along the lines of foreign travel assistance.[12]
- *Incident management* (information gathering and behavioral modification): Assistance during attack and to support recovery. This should not be in the form of advice, but rather practical assistance. This should be modeled on the care provided by health professionals: available on call when needed.
- *Remediation* (behavioral modification and standard setting): Governments should actively prosecute cyber criminals. More importantly though, there is a clear need for legal structures to be put in place that can accommodate the speed at which cyber crime changes and evolves.

Such an approach relies on governments' understanding of the urgency of the situation, and there is little evidence that they do indeed have this understanding at present. In the UK, as one example, it is particularly telling that the Government Digital Service's[13] home page does not even mention cyber security. Politicians often make statements that betray a poor understanding of the risk.[14] The current president of the USA talks about "shutting down the Internet" as if this were even a possibility.[15] The Australian prime minister was recently widely derided for his ignorance of the need for encryption.[16]

One does not expect regular politicians to understand this field, but one does expect them to listen to the experts. There is no evidence that they are doing this, however, which perhaps goes a long way towards explaining their responsibilization of cyber security.

It is time for ordinary citizens to insist that governments formulate effective cyber security risk regulation regimes. As Fig. 1 shows, public opinion and interest group pressures can bring about changes in risk regulation regimes.

It is every citizen's duty to hold his or her government to account in this matter. If we do not pressure them to take action, the cyber criminals will continue to wreak havoc. Allowing governments to continue with their responsibilization agenda, when it comes to cyber security, is no longer an option.

[12] https://www.gov.uk/guidance/foreign-travel-insurance.
[13] https://www.gov.uk/government/organisations/government-digital-service (Accessed 20 September 2017)
[14] https://www.theinquirer.net/inquirer/news/3014855/amber-rudd-the-little-people-dont-need-encryption; https://www.techdirt.com/articles/20170611/11545237565/theresa-may-tries-to-push-forward-with-plans-to-kill-encryption-while-her-party-plots-via-encrypted-whatsapp.shtml.
[15] https://www.theverge.com/2015/12/7/9869308/donald-trump-close-up-the-internet-bill-gates.
[16] http://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-of-mathematics-do-not-apply-australia-encryption-l-a7842946.html.

6. Conclusion

In the introduction, we asked whether the responsiblization of the cyber crime risk was (1) reasonable, and (2) judicious. We have argued that it is *unreasonable*, because it requires expertise to manage the risk that relatively few members of the public possess. We have also argued that it is *injudicious* because when one particular person does not manage their personal cyber risk, the resulting attack can demonstrate a measure of contagion, affecting the community at large. For all other risks demonstrating these two characteristics, a hierarchist approach has become widely accepted and implemented.

We suggest that a hierarchist approach, based on the history of risk management in other areas, is more appropriate for managing the cyber security risk. Such an approach relies on governments taking a more active role, committing more resources, and upskilling their crime fighting police forces and prevention units as a matter of urgency.

Acknowledgments

This research commenced while the first author was a Fulbright Cyber Security Scholar at Mississippi State University.

REFERENCES

Albert MR, Ostheimer KG, Breman JG. The last smallpox epidemic in Boston and the vaccination controversy, 1901–1903. N Engl J Med 2001;344(5):375–9.
Andreano FP. Evolution of federal computer crime policy: the ad hoc approach to an ever-changing problem. Am J Crim Law 1999;27:81.
Anon. About 10,000 vaccinated in South Boston. Boston Globe 1902.
Associated Press. Raging Oakland warehouse fire trapped victims in smoke .
Bada M, Sasse A. Cyber security awareness campaigns: why do they fail to change behavior?. Oxon: Global Cyber Security Capacity Centre, University of Oxford; 2014.
Baumgartner FR, Jones BD. Agenda dynamics and policy sub-systems. J Politics 1991;53(4):1044–74.
Begg C, Ueberham M, Masson T, Kuhlicke C. Interactions between citizen responsibilization, flood experience and household resilience: insights from the 2013 flood in Germany. Int J Water Resour Dev 2017;33(4):591–608.
Biebricher T. (Ir-)Responsibilization, genetics and neuroscience. Eur J Soc Theory 2011;14(4):469–88.
Bishop MA. The art and science of computer security. Boston, MA: Addison-Wesley Longman; 2002.
Blake JB. Public Health in the Town of Boston, 1630–1822. Boston, MA: Harvard University Press; 1959 No. 72.
Christensen K, Petersen K. Public–private partnerships on cyber security: a practice of loyalty. Int Affairs 2017;93(6):1435–52.
Choo K-KR. The cyber threat landscape: challenges and future research directions. Comput Secur 2011;30(8):719–31.
Cohen F. Computer viruses: theory and experiments. Comput Secur 1987;6(1):22–35.
Comack E, Peter T. How the criminal justice system responds to sexual assault survivors: the slippage between "responsibilization" and "blaming the victim". Can J Women Law 2005;17(2):283–309.

Cowhey PF, Aronson JD. Digital DNA: disruption and the challenges for global governance. New York: Oxford University Press; 2017.
Cragon HG. From fish to colossus: how the German Lorenz Cipher was broken at Bletchley park. USA: Cragon Books; 2003.
Dray J. Computer security and crime: implications for policy and action. Office Technol People 1988;4(3):297–313.
Ehrenberg A, et al. The weariness of the self: diagnosing the history of depression in the contemporary age. In: Homel David, et al, editors. Montreal and London: McGill-Queen's University Press; 2010.
Ekberg G. The Swedish law that prohibits the purchase of sexual services: best practices for prevention of prostitution and trafficking in human beings. Violence Women 2004;10(10):1187–218.
Fuenfschilling L, Truffer B. The structuration of socio-technical regimes: conceptual foundations from institutional theory. Res Policy 2014;43(4):772–91.
Gannon P. Colossus: Bletchley Park's last secret. Atlantic Books; 2014.
Gardner PH, Berry DC. The effect of different forms of advice on the control of a simulated complex system. Appl Cogn Psychol 1995;9(7):S55–79.
Garland D. The culture of control. Vol. 367. Oxford: Oxford University Press; 2001.
Geels FW. Ontologies, socio-technical transitions (to sustainability), and the multi-level perspective. Res Policy 2010;39(4):495–510.
Geller ES. Evaluating energy conservation programs: is verbal report enough. J Consum Res 1981;8(3):331–5.
Geller ES, Erickson JB, Buttram BA. Attempts to promote residential water conservation with educational, behavioral and engineering strategies. Popul Environ 1983;6(2):96–112.
Global Commission on Internet Governance (GCIG). Toward a social compact for digital privacy and security [accessed December 1, 2017] https://www.intgovforum.org/cms/igf2016/uploads/proposal_background_paper/GCIG_Social_Compact.pdf .
Granger S. Social engineering fundamentals, part I: hacker tactics. Security Focus 2001 December, 18, http://www.academia.edu/download/33172114/04SocialEngineeringWebQuest.pdf.
Gray GC. The responsibilization strategy of health and safety neo-liberalism and the reconfiguration of individual responsibility for risk. Br J Criminol 2009;49(3):326–342.
Grubb A, Turner E. Attribution of blame in rape cases: a review of the impact of rape myth acceptance, gender role conformity and substance use on victim blaming. Aggress Violent Behav 2012;17(5):443–52.
Hannah-Moffat K. Punishment in disguise: penal governance and federal imprisonment of women in Canada. Toronto: University of Toronto Press; 2001.
Hathaway M, Stewart J. Taking control of our cyber future. Georgetown J Int Affairs: Int Engag Cyber 2014;4:55–68.
Hatmaker, T. New York City is launching public cybersecurity tools to keep residents from getting hacked. 29 March 2018. https://techcrunch.com/2018/03/29/nyc-secure-new-york-cybersecurity-app-de-blasio/.
Hollway W, Jefferson T. The risk society in an age of anxiety: situating fear of crime. Br J Sociol 1997;48(2):255–66.
Hood C, Rothstein H, Baldwin R. The government of risk: understanding risk regulation regimes. Oxford: OUP; 2001.
Hooker Worthington. Physician and patient; or, a practical view of the mutual duties, relations and interests of the medical profession and the community. Baker and Scribner; 1849.
Horgan S, Collier B. Barriers to "Cyberaware" Scotland. Scott Justice Matters 2017;4(3):19–20 November.
Imgraben J, Engelbrecht A, Choo K-KR. Always connected, but are smart mobile users getting more security savvy? a survey of smart mobile device users. Behav Inf Technol 2014;33(12):1347–60.
Jordan JR, Hungerford HR, Tomera AN. Effects of two residential environmental workshops on high school students. J Environ Educ 1986;18(1):15–22.
Kello L. The meaning of the cyber revolution: perils to theory and statecraft. Int Secur 2013;38(2):7–40.
Kennedy LW, Sacco V. Crime victims in context. Los Angeles, CA: Roxbury; 1998.
Kenyon P. Infrastructure spending and unemployment: government responsibility for growth and jobs. Aust Econ Rev 1997;30(4):421–32.
Koskela H. 'Don't mess with Texas!' Texas virtual border watch program and the (botched) politics of responsibilization. Crime, Media, Cult 2011;7(1):49–65.
Kröger W. Critical infrastructures at risk: a need for a new conceptual approach and extended analytical tools. Reliab Eng Syst Saf 2008;93(12):1781–7.
Kuehn A. Extending cybersecurity, securing private internet infrastructure: the US Einstein program and its implications for internet governance. In: Radu R, Chenou JM, Weber R, editors. The evolution of global internet governance. Berlin: Springer; 2014. p. 157–67.
Lentz SA, Chaires RH. The invention of peel's principles: a study of policing 'textbook' history. J Crim Justice 2007;35(1):69–79.
Lindvall J. Mass unemployment and the state. Oxford: Oxford University Press; 2010.
Lkhagvasuren G. Cybersecurity cooperation of countries: impact of draft international code of conduct for information security. Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance. ACM; 2017. p. 564–5.
Luiijf E, Besseling K, De Graaf P. Nineteen national cyber security strategies. Int J Crit Infrastruct 2013;9(1-2):3–31.
Lynch M. The culture of control: crime and social order in contemporary society. PoLAR: Polit Legal Anthropol Rev 2002;25(2):109–12.
Mather C. Diary of Cotton Mather: 1681–1708. Massachusetts Historical Society; 1708.
Melrose M. Trying to make a silk purse from a sow's ear? A comment on the government's prostitution strategy. Saf Commun 2006;5(2):4–13.
Midden CJ, Meter JF, Weenig MH, Zieverink HJ. Using feedback, reinforcement and information to reduce energy consumption in households: a field-experiment. J Econ Psychol 1983;3(1):65–86.
Mohun AP. Risk. Baltimore: Johns Hopkins University Press; 2013.
Muro D, Vidal G. Political mistrust in Southern Europe since the great recession. Mediterr Polit 2017;22(2):197–217.
Nthala N, Flechais I. 'If it's urgent or it is stopping me from doing something, then I might just go straight at it": a study into home data security decisions. International conference on human aspects of information security, privacy, and trust. Springer; 2017. p. 123–42.
O'Driscoll A. 100+ terrifying cybercrime and cybersecurity statistics & trends [2018 EDITION] May 25 Accessed 4 June 2018 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/ .
Pfleeger SL, Caputo DD. Leveraging behavioral science to mitigate cyber security risk. Comput Secur 2012;31(4):597–611.
Phoenix J, Kelly L. 'You have to do it for yourself' responsibilization in youth justice and young people's situated knowledge of youth justice practice. Br J Criminol 2013;53(3):419–37.
Reddaway TF. The rebuilding of London after the great fire. London: Edward Arnold; 1951.

Renaud K. How smaller businesses struggle with security advice. Comput Fraud Secur 2016(8):10–18.
Renaud K, Weir GR. Cybersecurity and the unbearability of uncertainty. *Cybersecurity and cyberforensics conference (CCC)*. IEEE; 2016. p. 137–43.
Riley S. Password security: what users know and what they actually do. Usability News 2006;8(1):2833–6.
Rossiter K. Talking turkey: anxiety, public health stories, and the responsibilization of health. J Can Stud/Revue d'etudes Can 2012;46(2):178–95.
Roth MP. An eye for an eye: *a global history of crime and punishment*. London: Reaktion Books; 2014.
Rycroft R, Kash DE. Emerging patterns of complex technological innovation. Technol Forecast Soc Change 2002;69(6):581–606.
Sammarco AM. The great Boston fire of 1872. Mount Pleasant, SC: Arcadia Publishing; 1997.
Sanders T. Illicit and illegal: sex regulation and social control – By Joanna Phoenix and Sarah Oerton. Gender, Work Org 2007;14(4):388–90.
Sawislak K. Smoldering city: Chicagoans and the great fire, 1871–1874. Chicago, IL: University of Chicago Press; 1995.
Scoular J, O'Neill M. Regulating prostitution social inclusion, responsibilization and the politics of prostitution reform. Br J Criminol 2007;47(5):764–78.
Skinns L. Responsibility, rhetoric and reality: practitioners' views on their responsibility for crime and disorder in the community safety partnerships. Br Soc Criminol 2003;6:1–18.
Soneryd L, Uggla Y. Green governmentality and responsibilization: new forms of governance and responses to 'consumer responsibility'. Environ Polit 2015;24(6):913–31.
Spearin C. Against the current? Somali pirates, private security, and American responsibilization. Contemp Secur Policy 2010;31(3):553–68.
Stol YH, Schermer MH, Asscher EC. Omnipresent health checks may result in over-responsibilization. Public Health Ethics 2016;10(1):35–48.
Straub DW, Welke RJ. Coping with systems risk: security planning models for management decision making. MIS Q 1998:441–69.
Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 2011;34(1):1–11.
translated by Tacitus PC. The complete works of tacitus. In: Church Alfred John, Brodribb William Jackson, editors Digireads.com Publishing; 1942. translated by.
Thelen KA, Longstreth F, Steinmo S. Structuring politics: historical institutionalism in comparative analysis. New York: Cambridge University Press; 1992.
ushistory.org. The electric Benjamin Franklin. Independence Hall Association; 1995 http://www.ushistory.org/franklin/philadelphia/fire.htm On the Internet since July 4.
Voiskounsky AE, Smyslova OV. Flow-based model of computer hackers' motivation. CyberPsychol Behav 2003;6(2):171–80.
Wakefield A, Fleming J. The SAGE dictionary of policing. London: SAGE Publications; 2008.
Yan Zheng. Encyclopedia of mobile phone behavior. IGI Global; 2015.

Karen Renaud is a Scottish computing Scientist working on all aspects of Human-Centred Security and Privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. Her research approach is multidisciplinary, essentially learning from other, more established, fields and harnessing methods and techniques from other disciplines to understand and influence cyber security behaviours.

Karen was one of five UK Cyber Security Fulbright Awardees for 2016/17 at Mississippi State University in Starkville, Mississippi in the USA. She joined the University of Abertay as Professor of Cybersecurity in October 2017. She is associate editor for the *International Journal of Human Computer Studies, Transactions on Computer Forensics and Security, The Journal of Security and Applications* and *Information Technology & People*.

Stephen Flowerday holds a BSc and an MBA, as well as a doctoral degree (IT). He is an NRF-rated researcher in South Africa, and has supervised 37 postgraduate students to completion (10 doctoral and 27 master's). He is currently supervising a number of master's and doctoral students in the field of cybersecurity, behavioural information security, and information security management. Over the last thirteen years, he has authored and co-authored in excess of 80 refereed publications and has presented papers in various countries. Furthermore, he is a reviewer for conference publications, an editor and reviewer for a number of academic journals, and serves on various panels of the National Research Foundation (NRF).

Merrill Warkentin is the James J. Rouse Professor of Information Systems in the College of Business at Mississippi State University. His primary research focus is in behavioral IS security and privacy issues, and has appeared in *MIS Quarterly, Journal of MIS, Journal of the AIS, European Journal of Information Systems, Information Systems Journal, Decision Sciences, Information & Management*, and others. He was the 2016 AMCIS Program Co-Chair. He holds or has held editorial positions at *MIS Quarterly, Information Systems Research, European Journal of Information Systems, Decision Sciences, Information & Management*, and the *AIS Transactions on Replication Research*.

Paul Cockshott trained in Economics and Computer Science. He worked as a hardware designer for ICL and Memex Ltd, later becoming an academic at the Universities of Strathclyde and Glasgow. His research work in computing has included data persistence, data compression, video coding, special purpose hardware processors, 3D television, parallelising compilers and the physical foundations of computability. His published work in economics has covered value theory, models of profitability and economic planning. He retired in 2017 and is now an honorary researcher at the University of Glasgow.

Craig Orgeron has over 28 years of information technology experience in both the private sector and the federal and state level of the public sector. Dr. Orgeron began his career as a communicationscomputer systems officer in the United States Air Force. Currently, he serves as the Executive Director of the Mississippi Department of Information Technology Services (ITS) and Chief Information Officer for the State of Mississippi. In this role, Dr. Orgeron provides statewide leadership in the provision of services that facilitate cost-effective information processing and telecommunication solutions for agencies and institutions. He has served as President of the National Association of State Chief Information Officers (NASCIO), currently serves on the Executive Committee of the Multi-State Information Sharing & Analysis Center (MS-ISAC), and has participated in numerous government information technology task forces and committees.