Identity Theft and the Gullible Computer User:
What Sun Tzu in *The Art of War* Might Teach [*]

Joseph Savirimuthu
Lecturer in Law
Liverpool Law School
University of Liverpool
jsaviri@liverpool.ac.uk

Abstract. Securing trust is now a priority. Identity theft, phishing and pharming have exposed shortcomings in the criminal law. The online environment is now seen as the playground of criminals. Online criminal activities pose significant social and economic costs. Apparently, the Fraud Act 2006 is the instrument that will now neutralise the threats posed by phishers and identity thieves. This concept paper is an attempt to chart a less tenuous path of claim and counterclaim that often rears its head when the subject turns to personal Internet security. Accordingly, the paper aims to initiate a debate on how we can begin to think about information security and the role of law against the growing threats posed by identity thieves and phishing. I draw on the insights of Sun Tzu in *The Art of War* as way of understanding how best we can manage and reduce complexity. The debates have all too often focussed on liability rules and legal reform. The resulting impasse can be overcome if the problem is first of all properly characterised. A balanced policy debate requires an understanding of two key matters - 'trivergence' and the gullible computer user. The hypothesis is that before we can think about regulatory tools to curb practices like phishing an identity theft we need a better understanding of the interactions between data, devices and networks.

1. Introduction

There is a meme – law is an optimal instrument for steering through policies in respect of responsible computer use. As broadband penetration increases, personal internet security has become a live political issue. The reasons are not difficult to fathom. Increased Internet connectivity has led to an explosion of economic and social activity. The exponential growth of the Internet has brought with it a dark side. Criminals have harnessed new information and communication technologies for their own ends. Such is the concern about the threats posed by the new wave of criminal activity that the Internet is even being seen as a playground for criminals (House of Lords Select Committee on Science and Technology, 2007)[1]. This view is underscored by the Internet Security Threat Report, issued on 17 September this year, and which describes an increase in the use of new communication technologies in the commission of identity theft and activities relating to breaching network security systems (Symantec, 2007). Phishing is now assuming viral characteristics. 23917 unique phishing reports were received during July 2007 and the attacks continue to increase both in volume and intensity (Anti-Phishing Working Group, 2007). Securing trust is not an option – it is a necessity. Identity theft, phishing and its variants have also raised issues in respect of the role, if not the continued relevance of law in curbing this social problem. These concerns are reasonable - criminal activities transfer onto society significant social and economic costs. As many phishing attacks and security breaches go unreported, true estimates of the costs being internalised by society is difficult to ascertain (Dutton and Helsper, 2007). This poses an important question about the emphasis placed by legislators on the immunizing properties of the Fraud Act 2006 – identifying standards of behaviour and norms are useful. Legal commentators are cautiously optimistic that recent legislative incursions into the realm of information security will pay dividends. That said, we are still left with the issue of what avenues need to be pursued if securing compliance continues to be a problem (Privacy Rights Clearinghouse, 2007). To be sure, the testimonies before the Select Committee rehearse longstanding problems relating to enforcement and raise questions about whether content filtering mechanisms should be used, intermediary and vendor liability and the need to set up a centralised and coordinated task force. The Government's response to the Select Committee's report lacks a proper understanding of the complexities of governance in the online environment (UK Government, 2007). It is also unhelpful. All these are noteworthy matters but the focus on the issues, which continue to be raised, obstructs efforts in undertaking a balanced assessment of how best the threat landscape ought to be managed. The high level policy deliberations and examinations of personal internet security appear not to frame the problem accurately (Team Cymru, 2006). Internet service providers and software manufacturers may have sound commercial reasons for resisting the general thrust of the observations made by the Select Committee. We are consequently left with a

[*] This paper was first published in Kierkegaard, S.(2007) Cyberlaw, Security and Privacy , pp. 183- 200.

mischaracterisation of the problem that can only serve to produce policy initiatives that are incoherent, lead to a dialogue of claims and counterclaims or result in the status quo being maintained. In the light of the Government's response to the Select Committees, the last observation would appear to be true. Accordingly, the paper aims to begin a debate on how we could begin to think about information security and the role of law against the growing threats posed by identity thieves and phishers. There has been very little by way of discussion on the relationship between the converging multimedia platforms and the management of complexity on the one hand and the significance of convergence of data, devices and networks for the continued role of the criminal law. To overcome some of the hurdles that often accompany attempts to look beyond the steering role of law, I draw on the insights of Sun Tzu in *The Art of War*. A balanced policy debate requires at the very least an understanding of two key matters - 'trivergence' and the 'gullible' computer user [2]. The hypothesis is that before we can think about regulatory tools to curb practices like phishing and identity theft we need a better understanding of the interactions between data, devices and networks. I frame the governance challenges posed by identity theft and phishing in terms of warfare and suggest a framework that may help us refocus our efforts in developing creative and sustainable solutions. That process can only be initiated if we first make clear what managing complexity entails – an issue that is obscured by the repeated emphasis on the juridicalization of online criminal acts including phishing and identity theft. The paper applies ideas from *The Art of War* to a phishing scenario, to illustrate the limits of law as an instrument for managing and reducing complexity and suggests practical solutions which may help us overcome the current impasse regarding personal Internet security. This analysis has three implications for current approaches to personal Internet security. First, law should not be viewed as the sole or critical instrument for managing risks. Second, pervasive insecurity is the price we pay for increased connectivity. Third, when thinking about information security we need creative solutions that reflect emerging realities. As 1.3 billion people become increasingly networked, the convergence of data, devices and networks now provides the 'tipping point' for the centralised institutions for control. Sun Tzu's *The Art of War* contains some timely reminders about managing 'trivergence' and the gullible computer user.

2. The Fraud Act 2006: The Tipping Point?

The idea that the criminal law be used to maintain order and security is not a particularly novel one. Neither, should it be said is the view that the coercive machinery of the law be used to compel individuals to internalise acceptable social norms and values. What follows is a brief description of the role of law in curbing activities like identity theft and phishing.

The term 'identity is often used in an arbitrary and imprecise manner in popular media and literature (Chawki and Wahab, 2006). Identity theft can be viewed as a term of art used to describe activities like the dishonest acquisition of personal information in order to perpetrate fraud, typically by obtaining credit, loans, etc., in someone else's name. It is arguable that the appropriation of an identity of itself will not give rise to a criminal offence [3]. Phishing, vishing and pharming on the other hand are more specific in nature. These may arise as a result of identity theft, but can also be self-contained acts [4] Phishing, for example, is an online activity that uses social engineering strategies and technical ploys to gain access to an individuals' personal identity, data and other information. 'Vishing' involves criminals sending a spoof emails to unsuspecting businesses and individual. Rather than require the individual to click on the fraudulent link, the email provides a fraudulent customer services telephone number. Spear phishing on the other hand looks very much like an authentic email one expects to receive from an employer, business or organisation. In this type of phishing attack, the recipient may submit relevant information like passwords and login information as they assume that the request has come from a trusted person within that organisation or business.

Policymakers view the criminal law as an important instrument for ordering society. There is undoubtedly some justification for the importance placed on the criminal law as an instrument for promoting order and the requirement that individuals internalize a set of social norms and values. Enacting precise and clear legislation is critical if individuals in society are to adjust their behaviour in accordance with the legal rules and standards. Coercion and penal sanctions are seen as necessary since order and security have a public interest dimension.

2.1 Key Provisions

Section 1 of the Fraud Act 2006 creates a new general offence of 'fraud', which can be committed in three ways: by false representation (s2); by failing to disclose information (s3); and by abuse of position (s4). Section 2, with which we are primarily concerned here, provides as follows:

> ' (1) A person is in breach of this section if he—
> (a) dishonestly makes a false representation, and
> (b) intends, by making the representation—

> (i) to make a gain for himself or another, or
> (ii) to cause loss to another or to expose another to a risk of loss.
> (2) A representation is false if—
> (a) it is untrue or misleading, and
> (b) the person making it knows that it is, or might be, untrue or misleading.'

Liability for the *actus reus* of the section 2 offence will be established without more where the phisher makes a false representation. For example, an email purporting to come from a trusted source like an online bank, organisation or employer will be regarded false as it is untrue or misleading (s2(2)(a)). Section 2(3)(4) respectively state that a representation will include:

> '(3) any representation as to fact or law, including a representation as to the state of mind of—
> (a) the person making the representation, or
> (b) any other person.
> (4) A representation may be express or implied.
> (5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).'

In short, the elements of the *actus reus* in a phishing act will be found to be present when the initial email requesting the recipient to access a given website is received. The email constitutes an implied representation that it is from a legitimate source and which is false. With respect to *mens rea* requirements for section 2, the first element that must be proved by the prosecution is that the phisher made the representation dishonestly. This is not defined by the 2006 Act, and consequently remains a question of fact for the jury to determine.(See R v Ghosh [1982] QB 1053) The second element to be proved is that the phisher must know that his representation is or might be untrue or misleading (s2(2)(b)). Third, the phisher must intend, by the false representation to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss. It is important to be clear that section 5 provides that both these elements extend only to gain or loss in money or other property; and include any such gain or loss whether temporary or permanent. Property here can now be said to cover any property whether real or personal (including things in action and other intangible property). "Gain" includes a gain by keeping what one has, as well as a gain by getting what one does not have. "Loss" includes a loss by not getting what one might get, as well as a loss by parting with what one has. The impression one gleans from an examination of the broad definition of the section 2 offence is that it is technologically neutral. Given that phishers have sophisticated technological skills and use innovative technological instruments for social engineering, it is important that the legal rules anticipate new forms of subterfuge. The 2006 Act does not only cover phishers and those engaged in the criminal acts of social engineering or identity theft. Persons who have in their possession or under their control any article for use in the course of or in connection with any fraud can now be prosecuted under the 2006 Act (s6(1)). Furthermore, any person who makes, adapts, supplies or offers to supply any article for use with the activities covered by section 1(2) will be regarded as having committed an offence. The 2006 Act would also appear to make prosecution of phishers and suppliers of rootkits or related technology much easier. Prosecution needs to show that the person knew that the article was designed or adapted for use in the course of or in connection with fraud, or intended it to be used to commit, or assist in the commission of fraud.

2.2 Pervasive Insecurity

The Home Office minister, Gerry Sutcliffe regards the 2006 Act as making an important contribution to the fight against fraud (Out-law.com, 2006). His observation corresponds with the general thrust of the 2006 Act - the removal of the deficiencies in the previous regime on fraud and the incorporation of principles which conform with the concept of technological neutrality. This is undoubtedly a step in the right direction. If the criminal law is to be utilised effectively, procedural or technical obstacles must not be permitted to obstruct the prosecution of online fraudster. For example, it should not be open to a phisher prosecuted under this legislation to claim that he was deceiving the computer or that the intended victim did not read the spoof email. The 2006 Act makes clear the types of conduct, which will now be prohibited. Bainbridge (2007) observes that the legislation "extends the offence of fraudulent trading to sole traders and others not previously caught by the Companies Act. Although of wider application, the Fraud Act 2006 has significantly improved the ability of the criminal law to deal with computer fraud, including tackling 'phishing', that is, obtaining information such as a person's bank account details by sending an e-mail purporting to be from that person's bank" (p. 276).

We can conclude that the criminal law has an important standard setting role in this context. Unequivocal rules and norms provide a benchmark, which can in turn be used to determine the boundaries of permissible behaviour and penalise those who do not comply. That said there is very little consensus on whether legal reform and more generally the criminal law actually deter prospective phishers or identity thieves. It may be the case that an ineffective law is better than no law. We should not however underestimate the significance of the deep-seated concerns regarding the ability of the State to deter online criminal activity. How can a centralised model of control and coercion secure compliance in an environment free of traditional barriers to criminal activity? Effective policing of the online environment is heavily reliant on access to scarce resources. The police and specialised agencies dealing with serious organised crime are also hindered by the fact that they lack technological skills and hardware. Phishing and related online fraudulent scams thrive on the fact that computers view packets of information are viewed as authentic signals. Digitalisation of information in a highly networked environment compounds the problem of policing and enforcement. To this we can add the problems of information asymmetry and market failure in providing the necessary correctives to the criminal law. Shortcomings in "human systems" and vulnerabilities in protocols provide attackers with another exploit venue. Recently hackers, exploited server vulnerabilities in Monster.com, and acquired personal and financial information of approximately 1.3 million job seekers [5]. KPMG Forensic's Fraud Barometer has also reported that fraud levels in the UK are increasing dramatically [6]. Fraud levels rose to their highest level in 10 years in 2005, to £900m that year. As society, businesses and organisations become increasingly networked, it is apparent that the criminal law cannot by itself anticipate the evolving threat landscape or compensate for failures in soft systems. Anderson regards the problem of information security as one of misplaced incentives (Anderson and Moore, 2007). He suggests that intermediaries like software vendors and Internet service providers should be held liable for buffer overflows, and other software vulnerabilities that could have been detected. Legal instruments like contract and tort could be used to overcome the problems of market failure (Cert Advisory, 2003). There is very little information in the public domain to assist us in forming a view on why we have seen little or no litigation activity involving software vendors and Internet service providers. The other rationale for holding these entities, apart from the fact that the have access to key resources is that computer user to deal with emerging security threats (Bruce Schneier, 2007). Others have suggested that the sanctions imposed by the criminal law on online fraudsters should be increased to provide effective deterrence. There is some mileage in each of these proposals and it remains to be seen whether the Judiciary or Parliament will be the driving force for implementing these ideas or whether the current status quo will be tolerated. What is particularly interesting when thinking about the Government's response to the Select Committee's report is that policymakers appear not to focussed on the specific concerns raised (Select Committee, 2007). To be sure, commentators like Schneier and Anderson touch upon an issue that is often obscured by legal commentators and policymakers (Schneier, 2007): how can we manage and reduce complexity when data is transmitted across networks, applications and devices? Implicit in this question is the assumption that the computer and by extension the network is as a trusted system. Anderson seems to have picked on this point. He (2001) observes that

> "[a] typical security system consists of a number of principals such as people, companies, computers, and magnetic card readers, which communicate using a variety of channels including phones, email, radio, infrared, and by carrying data on physical devices such as bank cards and transport tickets. The security protocols are the rules that govern these communications. They are typically designed so that the system will survive malicious acts such as people telling lies on the phone, hostile governments jamming radio, or forgers altering the data on train tickets. Protection against all possible attacks is often too expensive, so protocols are typically designed under certain assumptions about the threats " (p.13).

The assumption of trusted systems needs to be re-examined (Gordon and Loeb, 2002). The idea of misplaced incentives is a sophisticated attempt to understand rational decision-making processes of "attackers" and "victims". This point is underscored by the recognition that many software manufacturers and businesses do not attach sufficient importance to information security. Clayton and Moore (2007) view "`take-down' as a reactive strategy, an increasingly prevalent trend in the way that security issues are being handled. Software vendors wait for vulnerabilities to be discovered and then issue patches. Anti-virus tools update their databases with new signatures as new viruses are identified. In these reactive approaches, the defenders aim to identify the bad guys as quickly as possible to minimise exposure, while the bad guys scramble to open new holes at a sufficiently fast rate to continue their activities."

There is a clear issue here as to whether the continued bias of the law towards software vendors and intermediaries can be defended [7]. It is not the aim of the paper to explore the normative issues raised. Consequently, the remainder of the article provides a framework for addressing the following question: If the computer and networks cease to be trusted systems, what strategies can we adopt which is both efficient and sustainable? This is a fundamental issue that goes to the core of the Select Committee's recommendations and which the Government's response does not adequately address. The layered network system makes identification and monitoring by the law problematic – this is a critical aspect in managing the threat landscape. Whilst traditional email exchanges provide information of the sender and recipient, in many phishing attacks, the websites used for the attack are frequently changed or located on servers outside the jurisdiction of law enforcement authorities. The key point here is that if we are to better understand how complexity can be both managed and reduced we need to have a clearer idea of the significance of the interaction between data, devices and networks in a decentralised and distributed computing environment. To conclude, we cannot focus merely on the Fraud Act 2006 but need to think about managing complexity when users interact with data, devices and networks. Identity theft or phishing is not a problem that "technology" or "law" can solve – it is a problem about finding a strategy to better manage complex network systems where trust is frequently breached. More crucially, given that many computer users are not computer scientists how should policymakers code rules that anticipate the gullible computer user?

3. Sun Tzu and *The Art of War*

How do ideas regarding the successful prosecution of armed conflicts lend themselves to the challenges posed by identity theft and phishing? Strategic thinking and planning in armed conflicts can be seen as a tool for managing complexity, risks and uncertainty. Phishers and identity thieves introduce complexity into trusted systems and architecture. Risk and uncertainty are the corollary of complexity. Business goodwill and enterprise is conditional on trust being maintained. Consumer's use of the online services is dependent on their trust in the integrity of network systems. Security breaches and online fraud serve to erode trust. The converse here is that costs have to be incurred by legitimate online users. Military generals have long been aware of the dire consequences that follow if an enemy is able to externalise the costs of its activities onto its opponent. The terrain, climatic conditions and free flow of information can often pose unexpected problems and challenges. In *The Art of War*, Sun Tzu configures data, technology and control into the complex battlespace. What follows is a general exposition of his noteworthy observations [8] .

3.1 The Art of War: A Primer

One school of thought in military warfare is that an enemy can be overcome by the sheer might and superiority of an army's firepower. Clausewitz's strategy of rapid dominance is sometimes seen as a proponent of this approach (Clausewitz, 1976). The strategy of overwhelming force may be useful if armed conflict takes place, for example, in an open battlefield but less so where the terrain or climatic conditions are varied. According to Sun Tzu, the prosecution of war should be underpinned by sound understanding of three main aspects: the threat landscape, the motivations of the enemy and an assessment of the strengths and weaknesses of both armies (Griffiths, 1963). Decision-making must be informed by 'five fundamental factors'. These can be summed up as requiring a moral and coherent framework of planning that is rooted in the prevailing geographical and climatic conditions. Strategic planning, according to Sun Tzu is not a science. Accordingly, a General must integrate the 'seven elements' into the decision making process. These involve an evaluation of time, space and distance and a proper assessment of the risks of success or failure. Sun Tzu's characterization of war as art is a reminder of the need for continuous assessment of the conditions in the theatre of warfare and to adapt the strategies accordingly. *The Art of War* cannot be separated from its historical context. Around 500 BC, feudal conflicts involved the expenditure of vast numbers of manpower and total annihilation of the enemy was seen as key. Sun Tzu was adept in recognizing the need for deploying strategies that were efficient and sustainable. This can be seen in his belief that the "Elements of the new armies, capable of co-ordinated movement in accordance with detailed plans, were responsive to systematic signals. The science (or art) of tactics was born. The enemy, engaged by the *cheng* (orthodox) force, was defeated by the *ch'i* (unorthodox, unique, rare, wonderful) force, or forces; the normal pattern was a holding or fixing effort by the cheng while *ch'i* groups attacked the deep flanks and rear (Griffiths, 1963 pp. 34-35)".

When organizing the logistics Sun Tzu urges the General to master the art of deception and exploit the weaknesses of the enemy. He also suggests that it is best to remove the opportunities for attack by creating sound defences – the idea that an enemy cannot attack if there are defences may seem counterintuitive and even reactive. Sun Tzu's point here is a deeper one – remove the incentives for attack by creating effective defenses.

3.2 From *The Art of War* to Coding for Complexity

Let us summarise the parallels between the threat landscape in online and offline environments before exploring the practical reach of Sun Tzu's claim that the removal of incentives can lead to a reduction of attacks. The theme of warfare is also appropriate to changing dynamics of control that previously defined the relations between the State and individuals. Arquilla and Ronfeldt (1997) point out that "[I]nformation, in all its dimensions, will enhance both the destructive and the disruptive capabilities of small units for all the services; in an information-age 'battlespace', massed forces will simply form juicy targets for small, smart attackers. In the new epoch, decisive duels for the control of information flows will take the place of drawn-out battles of attrition or annihilation; the requirement of destroy will recede as the ability to disrupt is enhanced" (p.2).

Free flow of information can assist both the army and its enemy. The challenge for the protagonists in both online and offline contexts is the same – managing the convergence of data, network infrastructures and devices. The threat landscape can be likened to a digital panopticon where the attacker has the advantage of identifying the time, frequency and place of attack. Accordingly, legitimate computer users and organisations have to assume the burdens resulting from a criminal's ability to leverage interconnectivity, mobility, inexpensive communication technologies. Indeed, social engineering techniques like phishing correspond very much with the tenets in *The Art of War*. As the Anti-Phishing Working Group indicates, "[s]ocial-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes" (2007).

Sun Tzu insights can help us in going beyond the constraints that juridicalization of social problems appear to pose. Indeed, the problems identified by Sun Tzu have contemporary equivalents: misplaced incentives, information asymmetry and market failures. Or in Cyberlaw, the four modalities: law, technology, market and norms. It is Sun Tzu's understanding of the nuances of warfare, goal definition and the need to undertake fresh consideration of the strengths and weaknesses of the respective armies that provides us with a pungent example of how we can begin to think seriously personal Internet security. In short, governance is a problem rooted in managing complexity.

3.3 Coding For Security

I focus on one key challenge – to reduce the avenues for exploitation by phishers through design solutions which replicate prudent decision making processes. This is not a task that is ahead of its time. Benkler (2006) reminds us that we "live in a technological context in which a tremendous amount of excess capacity of the basic building blocks of our information and communication infrastructure is widely deployed…Harnessing this excess capacity to create such a survivable infrastructure will likely be done most effectively, not through improving the ability to price these resources, but through improving the conditions for social sharing and exchange of the excess capacity users own. If we invest our policy efforts in hardening our systems to attack instead of rendering them survivable, if we ignore in our institutional design choices the effects on price-based markets and enterprise organization, we will lose a significant opportunity to improve the survivability of our information systems at relatively low cost and with minimal bureaucratic intervention" (p.75).

Benkler's point, echoes of Sun Tzu's emphasis on making the enemy externalise the costs of his activities through creative use of all available resources. To put it differently, as convergence creates a digital panopticon, ongoing reinforcement expenditure in the form of "digital locks" is unlikely to be a viable and sustainable enterprise. It is now becoming apparent that most phishing attacks are launched by organised criminal gangs and highly sophisticated computer users. From the perspective of the attacker, the benefits to be derived and the scale of the attacks is in inverse ratio to the likelihood of detection and capture. Networks and computer systems have been shown to be vulnerable to system exploits in the form of buffer overflows. System flaws can be detected by attackers remotely and escape detection. Phishers now send spoof emails from zombie networks of home computers or use anoymising systems like the Onion routing system. Keyloggers allow identity thieves to eavesdrop into communications conducted over networks. Spoof emails exploit the vulnerability inherent human trusted systems. The result of such techniques is that monitoring, detection and capture become difficult.

Let us test the value of the *The Art of War* and in particular, assess whether it generates additional insights in respect of personal Internet security? Consider as an example a phishing attack on a bank in Liverpool. A victim receives a phishing email purporting to come from a trusted party – Tsing Chao Banking Corporation. This email has a link to a fraudulent website. The attacker leverages the resources of the trusted system into tricking the unsuspecting individual into thinking that the Bank initiated the communication. Assume that the victim responds to the spoof email. The phisher now gains access to a range of information, which includes personal data, usernames and passwords and financial information. Coding for security is about managing convergence. Andrew Zimmerman has suggested that the new dynamics of engagement revolve around the convergence of networks, data and devices. Zimmerman's observation corresponds very much with Sun Tzu's view that planning and deployment efforts cannot be dissociated from the architectural landscape. Sun Tzu's insights are instructive as they draw attention to three features that characterize the management of complexity in the age of 'trivergence'. First, we need to better understand the reasons victims falls prey to social engineering techniques. Second, the decentralised communications infrastructure will prescribe the trade-offs and options that need to be brought to bear in respect of managing complexity. Third, technology, economic and social processes must be viewed as part of a broader governance strategy that includes, information gathering, standard setting and behaviour modification

(Hood, Rothstein and Baldwin, 2001). These three features remind us that law is a crude instrument through which "end-to-end" relationships of trust can be sustained. Coding responsive security protocols may however provide us a strategy for creating disincentives for phishers and identity thieves. The benefits in adopting this measure is not to be underestimated. Failures in 'human systems' lay at the root of the security breaches in Monster.com. Attackers used the Infostealer, Monstres Trojan to exploit Monster.com's database. The attackers gained access to the resume database using legitimate usernames and passwords of employers and human resource personnel's accounts. Spoof emails sent to Monster.com's clients were designed to look like an authentic email from the company. According to Dun and Bradstreet, identity theft fraudsters are turning their attention to social networking sites (Dun & Bradstreet, 2007). Sophos, the IT and Security corporation recently conducted a Facebook ID probe and discovered the ease with which information and identity theft takes place on social networking sites. It will be apparent here that an attacker needs to access only a few portals of information to recoup the dividends of his actions globally.

The ubiquitous computing environment, as reflected in the convergence of data, devices and networks, opens up possible design solutions. Sun Tzu reminds us that trust is socially constructed and managing complexity is an important part of the construction process. To date, we have assumed that the computer is a trusted system and that the 'end-to-end' architecture is somehow outside the boundaries of law. The focus on functionality of software creates a tradeoff between convenience and security. The values and priorities implicit in the balancing process needs to be reassessed. If principles of coding are to be reassessed what shape might they take? I suggest that the answer revolves around the axis of four key norms: (i) coding for trust through increased authentication; (ii) coding for "human failure"; (iii) coding as reaction to "bad code"; and (iv) coding as scientific communications. We need to 'couple' law with other regulatory tools. Rather than introduce legal reforms or regulations we could perhaps incentivise organisations to develop and sustain scientific and educational developments in this area. Technological solutions may be a positive response to overcoming the deficits in trusted computing systems and human failures. There is some evidence that the market is already aware of the need to bridge the trust deficit. VeriSign, for example, provides intrusion detection, threat scanning and patch implementation functions. Google, currently use web-crawlers to identify infected web pages. Exploit Labs, for example provide a LinkScanner functionality. Website owners can install a malicious content scanner on their site. Visitors to the site can type or paste a URL into the LinkScanner text box and will know whether the web page is safe. If the link has potential malware binaries, the visitor will be informed of this. Organisations in the public and private sector are using education as a means to promote responsible risk behaviour. ISPs are beginning to educate subscribers and users on the importance of safe browsing. This initiative is an important response to malware writers increasingly targeting instant messaging and peer-to-peer networks as potential vectors for distribution of viruses and worms. Equally, commercial and non-commercial organisations now make available "safety packages" as part of their subscription, with regular information about security issues and updates for browsers, plugins, applications and operating systems. For example, the Mozilla Foundation now makes phishing protection available on a non-commercial basis. Visitors to the site are provided with a test site to see if the phishing protection facility on their system has been enabled. Microsoft also provides a range of information seeking to educate users on the type of phishing hoaxes. These initiatives aim to provide a counterpoint to the methods employed by phishers and identity thieves in abusing trust. Recall how phishers use social engineering techniques to breach traditional perimeter and end point controls in anti-virus or anti-spyware products. Technology that mirror 'prudent behavioral norms' help minimise the threat consequences posed by the "gullible" human. The design solution here is the overriding of decision-making processes that lead to risk exposure. Real time protection and monitoring of application-level traffic will operate independently of the human computer user. Coding for security can be extended to developing software products that enable the identity of websites to be authenticated. Such software will enable end users to determine whether the website they are visiting or accessed via an email link is a trusted site. The process of authentication is fairly straightforward. The user needs only to place the mouse over a logo or image and the verification software will highlight the trust credentials of the site. BankSafe have a commercial product that encodes "risk management" norms into its anti-phishing software. This software runs on Windows applications and provides real time protection. It scans web pages visited by the end user. For example, when the user visits a malware vector that steal passwords and usernames, the browser is instantly shut down. The software also provides an early warning detection facility when phishing emails arrive into the inbox or fake DNS entries detected.

4. Conclusion

The Government's response to the report issued by the Select Committee underscores the premise of this paper – 'trivergence' conceals a paradox that law and politicians may be incapable of resolving. Indeed, the threat landscape is far more complex than the Government's response implies. This paper has proposed a way of thinking about managing complexity and what that entails in tangible terms. Limitations of space mean that some of the emerging information security problems in social networking sites or from increased convergence have not been examined in great detail. Cyberlawyers steeped in the idea that law has the 'right answers' may be disappointed in the thrust of the arguments offered. Policymakers who start from the premise that absolute security is attainable may react in a similar fashion. The distinguished members of the Select Committee should be congratulated for placing personal information security on the public platform and the testimonies of Schneier and Anderson deserve greater examination. In keeping with the general thrust of providing a balanced policy analysis I focused on the benefits of coding security norms. This is an avenue for delivering efficient, accessible and sustainable design solutions. Effective governance is not merely a matter of deterrence, it also requires an understanding of complexity and an examination of how best issues of functionality, convenience and security are to be negotiated. Functionality and convenience are not necessarily compatible with security considerations. As design solutions are increasingly embedded into networks and devices, security norms can be engineered into default protocols. The proposals offered by Anderson and Schneier in shifting the cultural mindset of software vendors and manufactures merit serious consideration. Re-thinking design principles may be a way forward – there is emerging evidence in the market that this is not a Panglossian exercise. It may be that as consumers of security, we may like Sun Tzu, have to make choices. The difficult choice here, and which is one of the enduring insights from *The Art of War* is this: what is the price to be paid for continuing to enjoy the benefits provided by the Internet whilst mindful that deviants have always sought to destroy value and create chaos? Information security is more than science – design solutions should not be underestimated. But neither should we forget, managing complexity is an *art*.

Reference (Selected)

1. Anti-Phishing Working Group Report (2007) Retrieved 8 November 2007, http://www.antiphishing.org/reports/apwg_report_july_2007.pdf
2. Anderson, R. (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. London: John Wiley.
3. Anderson, R. & Moore, T. (2006). Information Security Economics and Beyond. Retrieved November 5, 2007, from http://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf
4. Arquilla, J. & Ronfeldt, D. (1997). A New Epoch – And Spectrum – of Conflict. In J Arquilla & D Rondfeldt, (Eds.), In Athena's Camp: Preparing for Conflict in the Information Age. US: Rand.
5. Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. Computer Law & Security Report. Volume 23, 276-281.
6. Benkler, Y. Peer Production of Survivable Critical Infrastructures. In M. Grady and F. Parisi (Eds.), The Law and Economics of Cybersecurity. US: Cambridge.
7. Cert Advisory (2003). CA-2003-16, Buffer Overflow in Microsoft RPC. Retrieved from http://www.cert.org/advisories/CA-2003-16.html
8. Chawki, M. & Wahab, M. (2006). Identity Theft in Cyberspace: Issues and Solutions. Lex Electronica Volume 11, (Issue 1), 1-41. Retrieved July 10, 2007, from http://www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.htm.
9. Clausewitz, C.V. (1976). *On War*. In M Howard and P Paret (Ed. and Transl). Oxford: Princeton UP.
10. Dun & Bradstreet. (2007). Social Networkers at Risk of Identity Theft. Press Release August 8.
11. Retrieved on November 6, 2007, from http://www.scoop.co.nz/stories/print.html?path=BU0708/S00580.htm
12. Dutton, W. and Helsper, E. (2007). The Internet In Britain 2007. Oxford: Oxford Internet Survey.
13. Gordon, L. & Loeb, M. (2002).The economics of information security investment". ACM Transactions on Information and System Security Volume 5 (Issue 4), 438-457.
14. Hood, C. Rothstein, H. & Baldwin, R. (2001). The Government of Risk. Oxford:OUP (pp.4-35).
15. House of Lords Select Committee on Science and Technology. (2007). Personal Internet Security (HL Paper 165 – I). (London: Stationary Office).
16. Moore, T & Clayton, R. (2007). An Empirical Analysis of the Current State of Phishing Attack and Defence. Workshop on the Economics of Information Security. Retrieved November 1, 2007, from http://weis2007.econinfosec.org/papers/51.pdf.
17. Out-law.com. (2006). Prison term for phishing fraudsters. The Register, 14 November, 2006. Retrieved November 8, 2007, from http://www.theregister.co.uk/2006/11/14/fraud_act_outlaws_phishing/
18. Privacy Rights Clearing House, (2007). A Chronology of Data Breaches. Retrieved November 7, 2007, from http://www.privacyrights.org/ar/ChronDataBreaches.htm.
19. Science and Technology Committee Session 2006-07 HL Paper 165, *Personal Internet Security*.
20. Schneier, B. (2007). Minutes of Evidence before the Select Committee on Science and Technology, February 21, 2007. Retrieved November 7, 2007, from http://www.publications.parliament.uk/pa/ld/lduncorr/s&tii210207a.pdf.

21. Sophos Plc.(2007). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. Retrieved November 7, 2007, from http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html
22. Symantec Plc.(2007). Internet Security Threat Report, Volume XII
23. Team Cymru (2006). The underground economy:priceless. Retrieved November 8, 2007, from http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf
24. UK Government. (2007). The Government's Reply To The Fifth Report From the House of Lords

NOTES

[1] Hereinafter Select Committee.

[2] See generally the idea of trivergence in Andrew Zimmerman's blog. Retrieved November 5, 2007, from http://www.accenture.com/Global/Accenture_Blogs/Trivergence_Blog/default.htm. Also reference can be made to http://www.accenture.com/NR/rdonlyres/2F69B741-A4DA-4ADE-A71E-32043B007B75/0/edge.pdf. Retrieved November 5, 2007.

[3] See Memorandum from the Society for Computers and Law—Internet Interest Group and Privacy and Data Protection Interest Group paragraph 5. Retrieved November 5, 2007, from http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/7012406.htm.

[4] See generally information at http://www.microsoft.com/protect/yourself/phishing/.

[5] See http://help.monster.com/besafe/.

[6] See http://www.kpmg.co.uk/news/detail.cfm?pr=2913. Retrieved on November 5, 2007.

[7] https://www.kb.cert.org/vuls/id/635463. Retrieved on November 5, 2007. Also the US ruling L Pisciotta and D Mills v Old National Bancorp US Court of Appeals for the Seventh Circuit No 06-3187 http://blog.wired.com/27bstroke6/files/5W1FFXPR.pdf. Retrieved on November 5, 2007.

[8] The account on Sun Tzu synthesizes the information from Griffith, S.B. (1963). *Sun Tzu: The Art of War*. Oxford: Clarendon Press. Bartley, C (2005). The Art of Terrorism: What Sun Tzu Can Teach Us About International Terrorism. *Comparative Strategy* Volume 24, 235–51.