An empirical analysis of cyber risk data and development of cyber risk scenarios

Cybersecurity, Hacking and Technology – an illustration of a Cyber Risk Model

John Houston [1] and Madhu Acharyya [2]

Abstract

In this paper we propose a game-theoretic cybercrime model and test the management of cybercrime risk by organisations. We apply the concept of expected utility theory to explain the behaviour of hackers and defensive decision-making by the managers in the presence of risk and uncertainty. It is evident that in many occasions the hackers are bound to be at least partially successful and the risk mitigation through technological solutions alone cannot eliminate cyber risk completely. This is because the hackers hold superior knowledge and skill on modern technology and sophisticated skill than the organisations' managers. The hackers are always able to develop alternative ways to hack the online systems whatever sophisticated technology is used to mitigate cyber risk. Moreover, the organisations often operate under practical constraints (either economic, e.g., budget or governance) to manage their cyber-risk exposures. Furthermore, the technological solutions are temporary as hackers change their positions, strategy and techniques very frequently making management of cyber risk even harder for the organisations. Consequently, it is important to analysis the hacker motivations and operational strategy of the hackers from the perspective of behavioural economics.

Key words: cybercrime, risk analysis, risk model, game theory

[1] Senior Lecturer in Economics, Glasgow Caledonian University, Glasgow. Email: J.Houston@gcu.ac.uk

[2] Senior Lecturer in Risk Management, Glasgow Caledonian University, Glasgow. Email: Madhu.Acharyya@gcu.ac.uk

Section 1: Introduction

Cyber-risk is a growing threat for large corporations. This has emerged increasingly as a profitable industry for many 'hackers'. As the organisation grows, its operational activities extend and side-by-side, the size of its database increases. In order to reduce time and costs, the greater use of information technology displaces the manual and repetitive jobs. This is also to meet ever-increasing stakeholders' demand for faster services, in order to survive in the tough and competitive global market environment. In line with this increasing demand, the supply of new tools and techniques are innovated by suppliers and manufacturers. It is now evident in the aftermath of 2008 global economic crisis, that the financial industry has moved to digitalisation of operational services (McKinsey, 2015). However, no technological innovation is risk free. History suggests that several leading organisations encountered severe economic and reputational losses due to their failure in balancing the risk and reward relationship, particularly when digitalising their operational activities.

Cyber attacks takes several forms. Research suggests that the historical losses happened due to destructive attacks, cyberwarfare, government espionage, corporate espionage, stolen e-mail addresses and login credentials, stolen credit card and financial data and stolen medical-related data (Clough, 2015). The question that needs academic debate is "why do cyberattacks happen?; "What are the motivations of the hackers?" In essence, the risk-reward trade-off for cybercrime is very attractive. It is evident that cyberhackers (our 'hackers') constantly and rapidly monitor the movements of their targets, waiting for the opportunity to steal (or attack), but in a way as to ensure an acceptably low likelihood of being detected, caught and/or prosecuted. In the cyber-sphere many attacks can be executed relatively cheaply. The sophistication of low-costs electronic devices such as smartphones and tablets, broaden the hacker's attacking scope. Moreover, the trend towards digitisation of business process and functions from sales to production and outsourcing of services in remote locations make the system vulnerable to cyber risk. The abuse of technological innovations coupled with the internal frauds committed by employees in many instances has increased the frequency and sizes of cyber-attacks. Consequently, the human element relevant to cybercrime is vitally important to investigate in order to mitigate the cyber risk (Roux, 2015).

With the rise of cyber-attacks several state and regional regulators initiated to control organisational activities to combat the frequency and severity of cyber events. For example, ~~T~~the new generation of regulations in relevant areas (e.g. intellectual property) have restricted organisations' ability to fully protect their stakeholders' data and confidentiality. Failure to do

so, has caused them to breach customers' confidentiality, causing substantial financial and reputational losses. There is evidence that cyberattacks are carried out by well-educated gangs at private, organisation and even by states, but also by 'tech-savvy' self-starters, operating out of their bedrooms in their parent's homes. When an organisation reaches to a certain level of wealth and value either in economic and reputational terms, it becomes vulnerable to cyberattacks. In the financial industry, the hackers look for weaknesses in the control and security over operational transactions, though probably not having much, if any influence on the amount of wealth they can manipulate. This, and the inherent quality of security being largely under the control of the 'insiders' in the organisation.

As stated earlier, cybersecurity has also become a national policy priority where the national governments have initiated laws and regulations in efforts to protect private businesses, individual citizens and public bodies from cyber-attacks. In the United Kingdom for instance, the government published its 'National Cyber Security Strategy 2016 to 2021' that set out its plan to make the country more secure and resilient in cyberspace. It pledged to invest £1.9 billion over five years in defending the country's systems and infrastructure, deterring adversaries, and developing a whole-society capability (H M Government, 2016). In the USA, strengthening the security and resilience of cyberspace is an important mission of the homeland security. It has taken comprehensive initiatives combat cybercrime in order to protect critical infrastructure[3]. In 2015, the European Union approved a directive to ensure a common level of network and information security (NIS) throughout the EU Member States.

The remainder of this article is organized as follows: Section 2 discusses the interdisciplinary literature on cybersecurity. Section 3 develops a simple, abstract cybersecurity model from a game-theoretic perspective. Section 4 performs an illustrative empirical case study to test the model. Finally, Section 5 concludes the article and identifies opportunities for future work.

[3] Further information is available on https://www.dhs.gov/topic/cybersecurity (accessed: 10th April, 2017)

Section 2: Literature review

The following articles will be used to present the study's literature:

Author(s)	Paper title	Industry/sector focus	Findings
Ogut, Raghunathan, & Menon (2011), Risk Analysis	Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection	Insurance	In this article the authors examined the scope of cyber (information) security risk insurance to protect firms as a part of their cyber security risk management programme. They described the issue within the capacity, complexity and interplay of three agents i.e. firms, government and insurers. They found that the firms invest less than the social optimal levels in self-protection and, most importantly, the insurers are unable to observe (or verify) firms' self-protection levels for the correlated risks, in particular, even the governments (i.e., social planners) either provides a subsidy to the firms or charge tax on insurers. They concluded that the existing imperfect insurance market is insufficient to achieve the efficient outcome in cyber security risk management.
Henry & Haimes (2009)	A Comprehensive Network Security Risk Model for Process Control Networks	Engineering	In order to protect the distributed process control networks (PCN) from cyberattacks, the civil infrastructures, in particular, the authors developed a Network Security Risk Model (NSRM) with the capability of capturing the relevant dynamics of cyber-attacks. Their model provided a means of evaluating the effectiveness of candidate risk management policies by modelling the frequency and severity of cyber risk after the implementation of candidate measures.
Santos, Haimes & Lian (2007)	A Framework for Linking Cybersecurity Metrics to the Modelling of Macroeconomic Interdependencies	Supply Chain Management	With the argument of the systemic nature of the technical interdependencies of cyber risk among industries and critical infrastructure sectors the authors developed an interdependency-based risk analysis framework for cyber-attacks to supervisory control and data acquisition (SCADA) systems for the use of disaster planning and management purposes. The result provided a foundational framework for modelling cybersecurity scenarios for the oil and gas sector.

Author(s)	Paper title	Industry/sector focus	Findings
Andrijcic & Horowitz (2006)	A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property	Business management	The paper focussed on the loss in intellectual property as long-lasting effects of cybercrime committed by foreign perpetrators. In order to determine the potential macro-economic consequences of cyber-attacks due to stolen IP from U.S. companies as well as their likely sources the authors presented a two-part International Consequence Analysis Framework.
Rao, Poole, Ma, He, Zhuang & Yau (2016)	Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models	Computing infrastructures	The authors proposed a game-theoretic attack-defence model and studied the strategic interactions between attackers and defenders within the context of network and computing infrastructures. They found that the Nash equilibrium under uniform costs in both cyber and physical components is computable in polynomial time, and provides high-level deterministic conditions for the infrastructure survival. They tested the attack-defence model with the probabilities of successful attack and defence, and of incidental failures.
Davis, Garcia & Zhang (2009)	Empirical Analysis of the Effects of Cyber Security Incidents	Marketing	Focussing on the potential economic effect of data breaches the authors tested if this economic cost motivates the online businesses to increase their investment to combat the cyber security incidents on web traffic. They found that this is not the case as the credit card companies takes the risk of security breaches and the risk-averse customers pay the premium.

Section 3: The Model

This model assumes there are three players: an organisation (*o*), a hacker (*c*) and the State (*s*). The organisation has a property right over assets that yield (it) utility. It may either be a private company, public sector organisation, or even an individual. The same assets are also attractive to the hacker and they will attempt to acquire some portion of these, illegally. [4] The State, as the upholder of the Law, obtains utility from successfully prosecuting and punishing the hacker who has been detected by the organisation attempting to steal its assets.

It is assumed that all the players share the same general saturation utility function:

$$U(X) = \alpha X^{\gamma} \ (0 < \alpha < 1 : 0 < \gamma < 1)$$

Total utility increases in X, but at a decreasing rate i.e. marginal utility tends towards zero as each extra unit of X is obtained. This establishes an upper limit to the amount to be stolen in a single operation, as illustrated in *Figure a*. [5] Each player has their own specific utility function:

$$U(X_o) = \alpha_o X^{\gamma_o} \qquad \textbf{[1.1]}$$

$$U(X_c) = \alpha_c X^{\gamma_c} \qquad \textbf{[1.2]}$$

$$U(X_o) = \alpha_o X^{\gamma_o} \qquad \textbf{[1.3]}$$

As the players are operating in a world of uncertainty, each one has to optimise their *expected* utility arising from their actions:

$$\overline{U}(X) = h(X)U(X)$$

Where *h(X)* is a probability density function of the 'success' each player has in achieving their objective, in either preventing, acquiring or punishing the (theft of) value of the assets stolen, *X*.

[4] By 'value' we regard any tradeable proceeds from the activity. This may, obviously be actual 'cash' that can be moved from one account to another or 'goods' than can be shipped and misdirected without proper payment. It may also include the acquisition of data (product details, customer details, financial accounts), either acquired directly by a competitor, or on its behalf by a third party. The hacker may offer back stolen goods to the organisation in return for a cash payment. The hacker's aim may be to obtain a benefit from bringing down the organisation, either by draining it of resource, or destroying its reputation. This benefit may be pecuniary (e.g. the elimination of a commercial competitor or enforcement agency) or non-pecuniary (e.g. the elimination of a political rival or detested organisation). In any case, we can convert any benefit to *utility*.

[5] The amount acquired (and associated utility derived) may be sufficient for all time, or may be consumed over time implying that the hacker will require to return to attempt to repeat their previous feat.

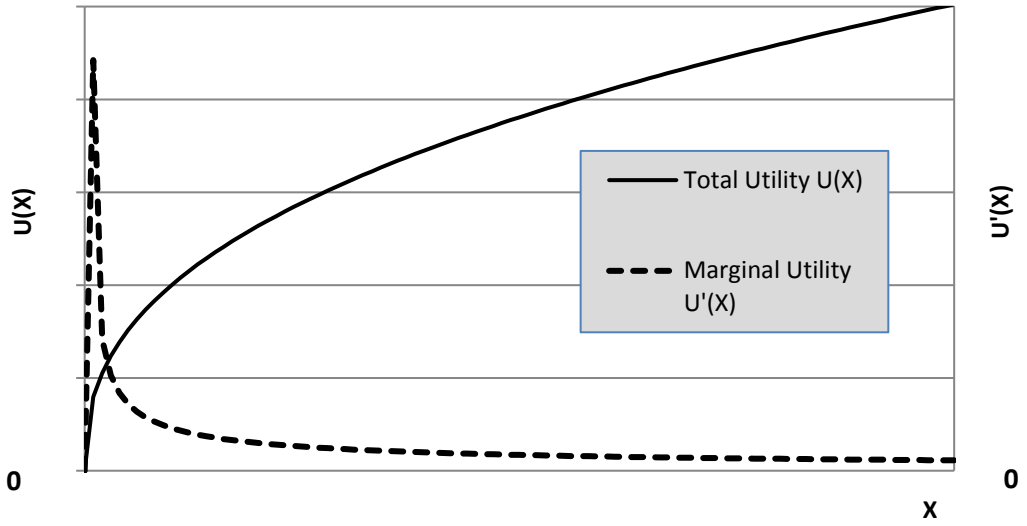


Figure a Saturation Utility Function

Amongst others, Bliss (2000) suggests a functional form for the cdf, H(X), viz

$$H(X)=\frac{1}{(1+\alpha X)^{\beta}}$$

- which exhibits the same general shape as the total utility function in *Figure* a, with an upper limit of 100%. Each player selects a value under their control (*X**) that *conditionally* optimises their expected utility, $\overline{U}\left(X^{*}\right)$.

$$\overline{U}_{o}\left(X_{o}^{*}\right)=h_{o}\left(X_{o}^{*}\right)\alpha_{o}X^{\gamma_{o}} \qquad \textbf{[2.1]}$$

$$\overline{U}_{c}\left(X_{c}^{*}\right)=h_{c}\left(X_{c}^{*}\right)\alpha_{c}X^{\gamma_{c}} \qquad \textbf{[2.2]}$$

$$\overline{U}_{s}\left(X_{s}^{*}\right)=h_{s}\left(X_{s}^{*}\right)\alpha_{s}X^{\gamma_{s}} \qquad \textbf{[2.3]}$$

Figure b illustrates the typical trajectories of expected payoff and the associated expected utility and the shared optimising value, X^{*}.

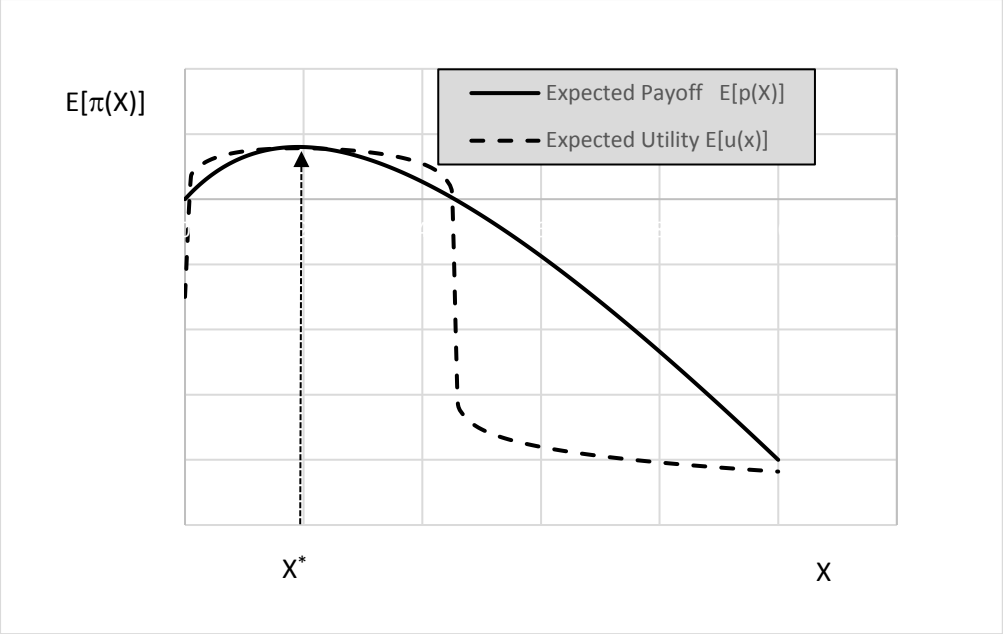


Figure b Expected Payoff & associated Utility Functions

We now consider each of the players' motives and optimising actions in turn, as well as the nature of the conditional interdependence between them.

The organisation

The organisation has, at any one time, a property rights over assets to the value X, that are vulnerable to cyber-theft. It can erect either or both two stages of defence: (i) Prevention, and (ii) Detection. As *Figure c* illustrates, some attempts by the hacker to illegally acquire the assets will be stopped at the Prevention Stage. Some attempts will successfully avoid that stage and attempt to acquire a portion of the assets, but some of these will be detected and blocked. Other attempts, however, will be sufficiently sophisticated (or just 'lucky') to avoid detection and allow the hacker to steal some of the X.

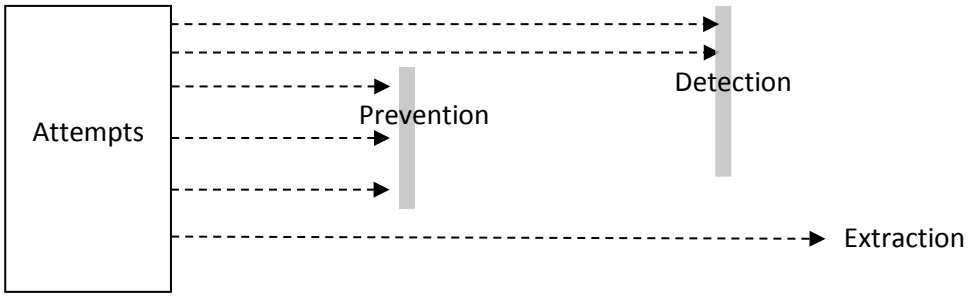


Figure c Protection and Detection defences

Prevention aims to shield a percentage of the otherwise, at-risk assets. The organisation allocates a certain amount of *X* to the prevention effort, that then determines the percentage of assets that will be completely protected from the cyber-hacker. It is assumed that it will become increasingly difficult to increase the level of protection, requiring ever more extra resource to do protect the more accessible assets. Thus, the general relationship between protection expenditure and the degree of protection is the same in nature to the saturation utility function as depicted in *Figure a*: more and more additional resource has to be devoted to protect the ever harder-to-protect assets This establishes an upper limit to the amount the organisation will devote to prevention defence.

Detection defence aims to identify and negate those incidents that have been successful in overcoming the prevention effort, before they extract the targetted assets. It is assumed that the greater the resource devoted to detection (*D*) the more likely attempts will be detected (and the hacker rendered liable to punishment by the State). It is also assumed that the probability is not linear in *D*, but may increase at an ever declining rate, never reaching 100%. A plausible form for the *detection function* cdf, *H(D)*, would be:

$$H(D) = \frac{(1+\tau_0 D)^{\beta} - 1}{(1+\tau_0 D)^{\beta}} \qquad \textbf{[3.1]}$$

and its corollary, the *avoidance function, H'(D) = 1 – H(D)*:

$$H'(D) = \frac{1}{(1+\tau_0 D)^{\beta}} \qquad \textbf{[3.2]}$$

Where τ_0 and β are parameters that relate the amount spent on detection and the proportion of assets shielded. *Figure d* illustrates detection function's trajectory as *D* is increased, with the marginal probability falling at an ever-increasing rate, towards zero.

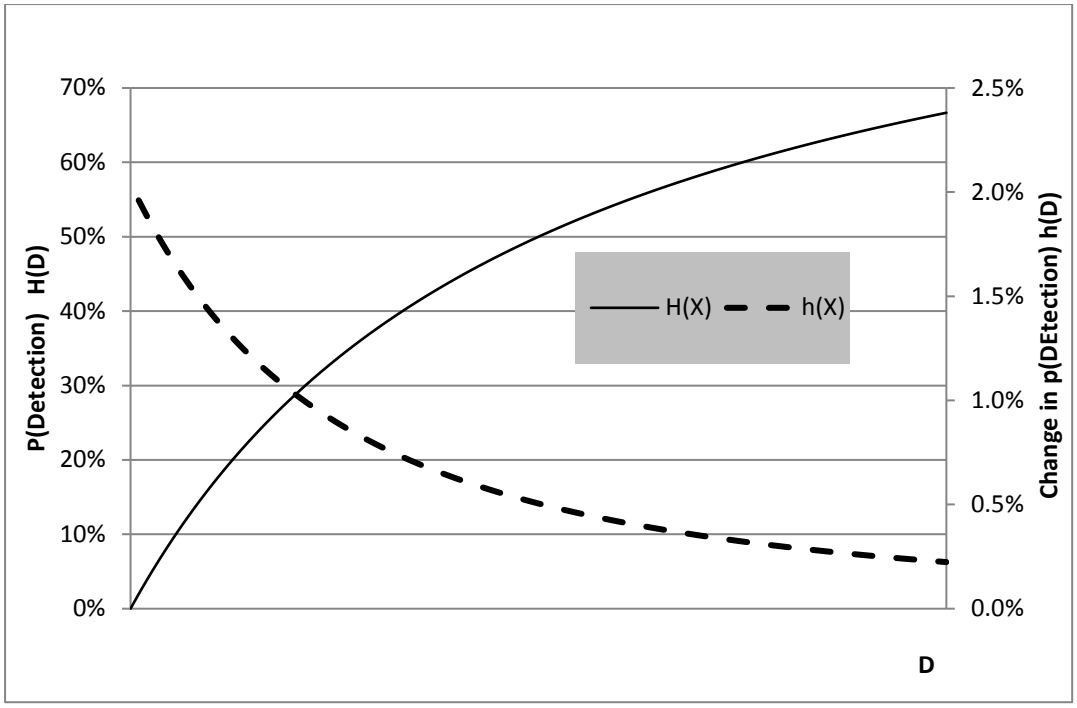


Figure d Detection expenditure and the probability of detection

Taken together, it appears that total security over all of the organisation's assets is impossible and that is inevitable that the hacker will enjoy some success in acquiring some portion of them. The problem for the organisation is therefore to select the optimising values of *P* and *D* that, together, maximise the expected utility from the expected loss of some proportion of its assets. **[2.1]** is therefore:

$$\underbrace{\max\left(\overline{U}_o\right)}_{P,D\in\Re} = \alpha_o\left(X^P - \left(P + D + \frac{X^U\hat{\delta}_c}{(1+\tau D)^\beta}\right)\right)^{\gamma_o}$$
$$\textbf{subject to}\left(P+D\right) < X$$

where $X^P = X\left(\alpha_P P^{\gamma_P}\right)$ and $X^U = \left(X - X^P\right)$.

X^P is the amount of protected assets, X^U the resulting unprotected assets, $\hat{\delta}_c$ is the organisation's current belief about the proportion of X^U the hacker will attempt to acquire. A key point to note is that the organisation's choices of *P* and *D* are *conditioned by* α_0 and γ_0 and *conditional upon* $\hat{\delta}_c$. It is assumed that the organisation can derive α_0 and γ_0 with sufficient accuracy. However, any mismatch between $\hat{\delta}_c$ and the actual proportion the hacker is attempting to steal (δ_c) implies that the calculated P^* and D^* will, in fact, turn out to be a sub-optimal given the hacker's intentions. This point we will be considered in the empirical illustration later.

The hacker

The hacker's incentive in attempting to extract value from the organisation has already been considered, namely optimising a version of **[2.2]**. The hacker knows that the organisation will both seek to protect some proportion of its assets otherwise at risk, and monitor the rest that are exposed. The hacker will attempt to acquire some proportion of these exposed assets $\left(\delta_c\right)$ in the hope that they can avoid detection with a probability determined by **[3.2]**. Should they be detected, they will fail to acquire any of the assets and then face the risk of a State-inflicted punishment, if convicted. Thus, they have to form beliefs as to the amounts the organisation is spending on protection $\left(\hat{P}\right)$ and on detection $\left(\hat{D}\right)$ and the severity of the punishment, as measured by the hacker's perception of the State's punishment-to-crime ratio, $\hat{R}$. This hacker will calculate what they believe to be the optimal proportion of the assets to acquire $\left(\delta_c^*\right)$ given their beliefs being the expected utility from attempting to steal just a little more wealth from the organisation against the expected probability of being discovered stealing it and the value of the punishment to be inflicted upon them. Formally, their version of **[2.2]** is:

$$\underbrace{\max\left(\overline{U}_c\right)}_{0\le\delta_c\le 1}=\frac{\alpha_c\left(\hat{X}^U\delta_c\right)^{\gamma_c}}{\left(1+\left(\hat{\tau}_0\left(\hat{X}^U\delta_c\right)\right)\right)^{\beta_0}}-\frac{\alpha_c\left(\hat{X}^U\delta_c\hat{R}\tau_s\right)^{\gamma_c}}{\left(1+\left(\hat{\tau}_0\left(\hat{X}^U\delta_c\right)\right)\right)^{\beta_0}e^{\hat{R}}}$$

As with the organisation, any mis-match between these beliefs and reality will imply a sub-optimal selection of δ_c which will be considered in the empirical application section.

The State

The state's objective is relatively simple: to maximise society's expected utility from convicting and punishing hackers detected by the organisation. The state determines the value of the punishment as a multiple of the value of the (attempted) theft, *R* ($0 < R < \infty$). It is assumed, however, that the probability of a conviction (*H(C)*) falls as *R* increases, in the style of *Figure e*. It can be supposed that hackers (and their advocates) will defend themselves more robustly the more severe the potential punishment (including absconding from the legal territory) and/or that Society may regard excessive punishment (e.g. the Death penalty) as undesirable and elect officials who will moderate the punishments. [6]

[6] They will also rail against a regime that is deemed to be too 'soft' and demand an increase in *R* to a satisfactory level.

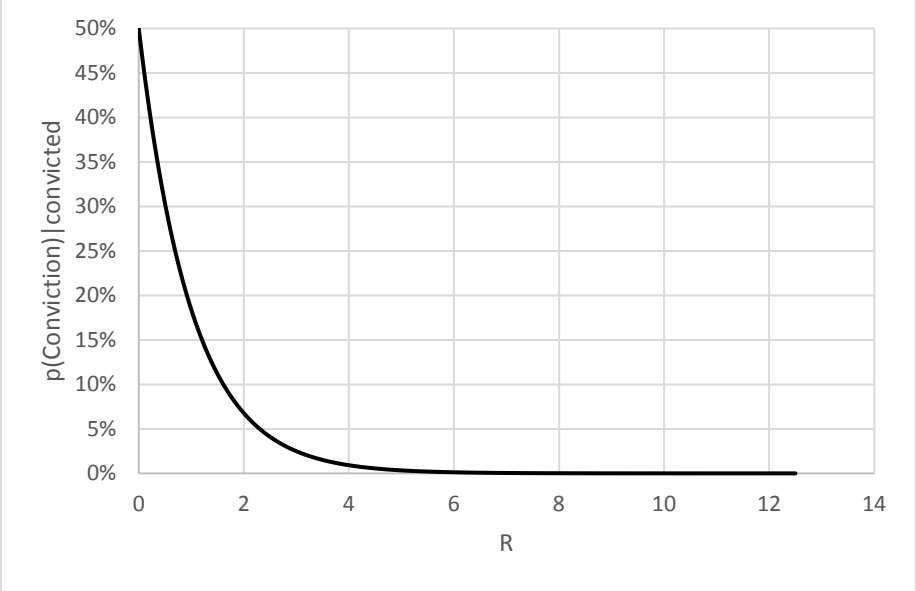


Figure e Probability of Conviction, given detection

The State has to incorporate its current beliefs about the organisation and the hacker to select the 'optimal' punishment-to-crime ratio (R^*). As it can only convict hackers that have been detected, it seeks to optimise their version of **[2.3]**: [7]

$$\underbrace{\max\left(\overline{U}_s\right)}_{R\in\Re}=\left(\frac{\tau_s\left(\left(\hat{\tau}_o\hat{X}_P\hat{\delta}_C\right)^{\beta_c}-1\right)}{e^R\left(\hat{\tau}_o\hat{X}_P\hat{\delta}_C\right)^{\beta_c}}\right)$$

- where τ_s is the maximum probability of a conviction, itself a function of the quality of the legal system. As with the organisation and the hacker, any mis-match between the State's beliefs about their parameters will result in a sub-optimal punishment régime.

[7] For the purposes of simplicity, it is assumed that the State uses the same belief as the hacker with respect to the organisation's parameter, τ_o.

Section 4: Illustration of the Risk Model

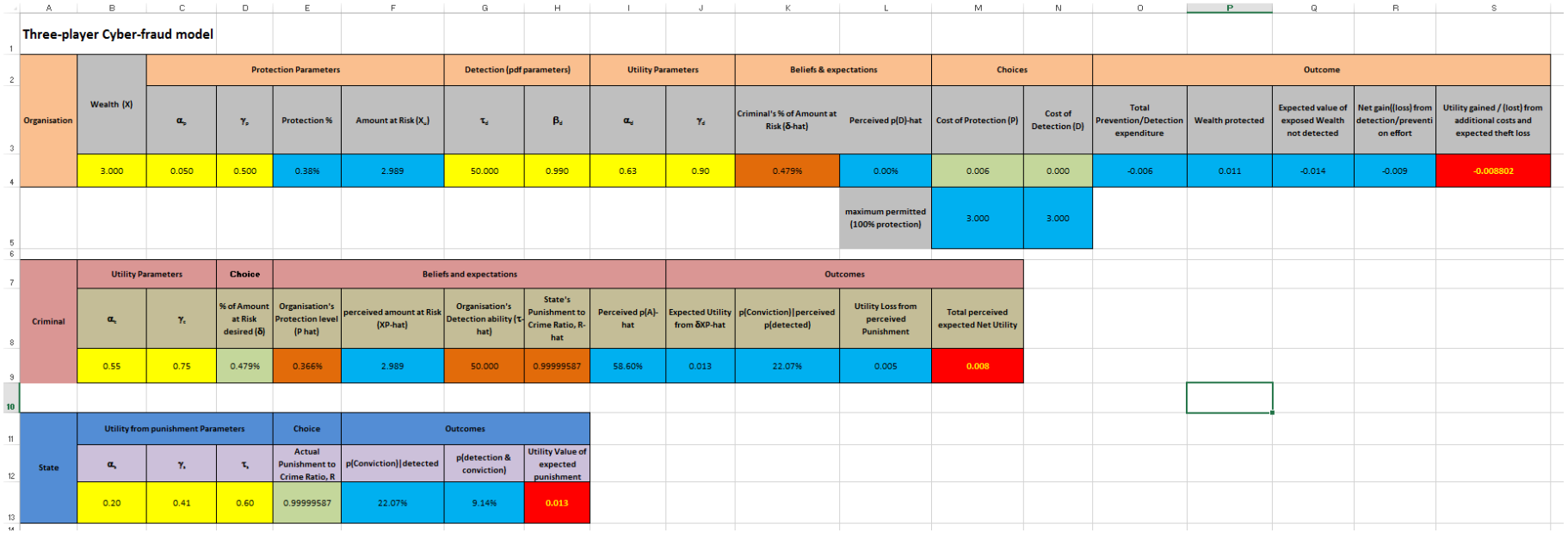
In order to illustrate the player-learning process in practice, an Excel-based model was constructed (*Figure f)* to demonstrate the process to equilibrium, where that equilibrium is dependent upon the players' beliefs about each other. Realistic parameters were entered for each player, including initial belief parameter values that were made deliberately different from the actual parameters each player employed. Each player's expected utility function was optimised in turn, starting with the organisation, then the hacker, then the State in the first phase.

For illustrative purposes, we assume that in the absence of any hard information, the organisation forms the naïve belief that the hacker will attempt to acquire *all* of its unprotected assets $\left(\hat{\delta}_c = 1\right)$. Given that belief and its utility parameters, it finds it optimal to devote £0.0066 and £0.225 of its £3 of assets to protection and detection respectively. This shields a little over 0.4% of the assets and, it believes, gives it a 91.6% probability of detecting any attempt to steal the assets. This maximises its expected utility to $\overline{U}_o^* = -0.319$. We consider below whether or not this forms part of a (Bayes-)Nash Equilibrium outcome.

At the same time, the hacker forms a naïve belief regarding the proportion of the assets that will be accessible to it: 5% (≠99.6%) and that τ_o equals 40 (when it, in fact, equals 50) and that the State's punishment-to-crime ratio (*R*) is 1-1 (when it, in fact 0.999-1). It finds it optimal to attempt to acquire 0.842% of the assets, rather less than the 100% that the organisation believes it is trying to acquire! Its conditional maximum expected utility is $\overline{U}_c^* = 0.013$

The State, for its part has no particular incentive to conceal its parameters, and, given these and its beliefs about the organisation and the hacker, sets the punishment-to-crime ratio to 0.999 and obtains an expected utility gain of $\overline{U}_s^* = 0.013$.

Focussing on the organisation and the hacker, do these first-pass optimisations form a (Bayes-)Nash Equilibrium? The answer has to be 'No', as had the organisation realised that the hacker intended to steal only 0.842% of its unprotected assets and not 100%, it would have found it optimal to spend 0.006 on Prevention defence (≠ 0.007) and 0.002 on Detection (≠ 0.225). It would then have achieved an optimum expected utility of $\overline{U}_o^* = -0.018$ (≠ -0.319). Similarly, the hacker, over-estimates the proportion of assets the organisation will protect (5% versus



Three-player Cyber-fraud model

Organisation	Wealth (X)	Protection Parameters				Detection (pdf parameters)		Utility Parameters		Beliefs & expectations		Choices		Outcome				
		α_p	γ_p	Protection %	Amount at Risk (X_r)	τ_d	β_d	α_d	γ_d	Criminal's % of Amount at Risk (δ-hat)	Perceived p(D)-hat	Cost of Protection (P)	Cost of Detection (D)	Total Prevention/Detection expenditure	Wealth protected	Expected value of exposed Wealth not detected	Net gain((loss) from detection/preventi on effort	Utility gained / (lost) from additional costs and expected theft loss
	3.000	0.050	0.500	0.38%	2.989	50.000	0.990	0.63	0.90	0.479%	0.00%	0.006	0.000	-0.006	0.011	-0.014	-0.009	-0.008802
											maximum permitted (100% protection)	3.000	3.000					

Criminal	Utility Parameters		Choice	Beliefs and expectations					Outcomes			
	α_r	γ_r	% of Amount at Risk desired (δ)	Organisation's Protection level (P hat)	perceived amount at Risk (XP-hat)	Organisation's Detection ability (τ-hat)	State's Punishment to Crime Ratio, R-hat	Perceived p(A)-hat	Expected Utility from δXP-hat	p(Conviction)|perceived p(detected)	Utility Loss from perceived Punishment	Total perceived expected Net Utility
	0.55	0.75	0.479%	0.366%	2.989	50.000	0.99999587	58.60%	0.013	22.07%	0.005	0.008

State	Utility from punishment Parameters			Choice	Outcomes		
	α_s	γ_s	τ_s	Actual Punishment to Crime Ratio, R	p(Conviction)|detected	p(detection & conviction)	Utility Value of expected punishment
	0.20	0.41	0.60	0.99999587	22.07%	9.14%	0.013

Figure f Excel Model: main screen

0.406%), given its mis-perception of τ_o and *R*. Accordingly, it should instead have set δ_c = 0.479% (≠ 0.842%), which would have resulted in an expected utility gain of $\overline{U}_c^* = 0.010$ (≠ 0.013).

If the game were repeated, in the sense that the players observe the outcome from the first pass, realise their misperceptions regarding the others' parameters, and update their beliefs, we might expect them to iterate closer and closer to each other, to a point where we achieve a (Bayes-)Nash equilibrium: that is, the players' beliefs are in accordance with the actual parameters and are all optimising, given the others' actions. How many plays are required to bring all the players to this points depends on the length of each 'round', how well each one learns about the others' parameters, and to what extent they revise their beliefs for the next play. *Figures g* and *h* plot the expected 'optimal' utility trajectories for the organisation and hacker as they close the gaps between them (read each figure from right to its left). In this case, the organisation would see its expected utility rise as they converge with the hacker, though the hacker's would decline.

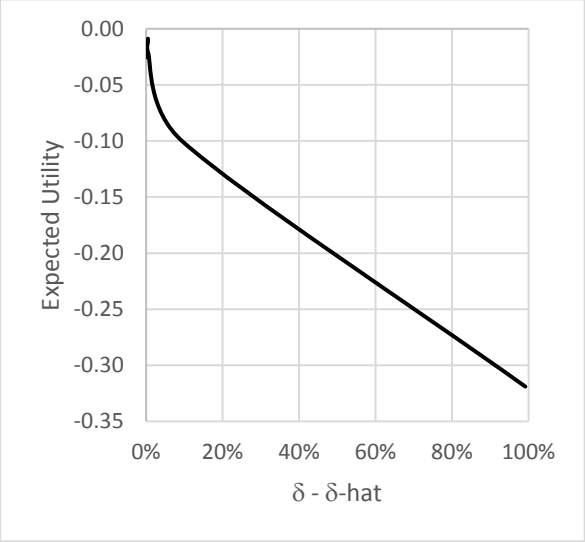


Figure g organisation's Perception Gap (hacker's δ)

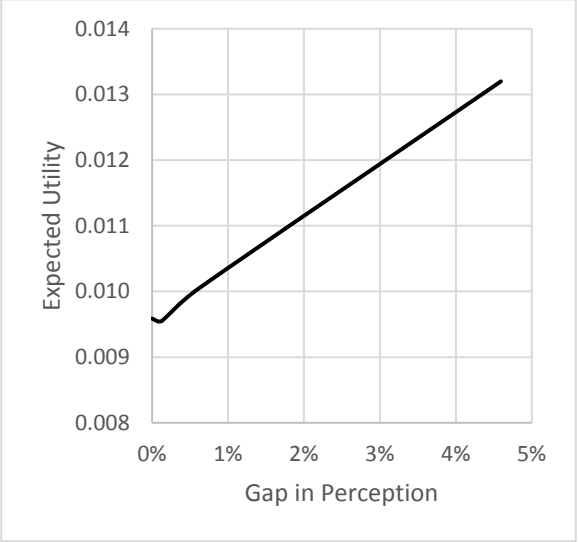


Figure h hacker's Perception Gap (% assets protected)

Of course, this is due to the assumptions made in the model, including the illustrative parameterisations. It might be argued that the hacker, therefore, has no incentive to update their beliefs about the other players. Game Theorists will always point out that any action that emanates from incorrect beliefs cannot be part of a stable equilibrium outcome, and that, in effect, all players will eventually be forced together.

Conclusion

The issue of cybercrime, via the 'hacking' of victims' computer-based systems is an ever-increasing problem. While the technical aspects of these crimes are relatively new, the underlying incentives of the involved players are centuries old. For the hacker, it is the utility to be gained from the wealth acquired, taking into account the penalties for being caught. For the organisation, it is the utility gained from the assets it successfully defends from theft. The State obtains utility from apprehending hackers and maintain Law and Order in its territory. Each of the three players conditionally optimise their own utility, based on their current belief about how the others will play: for the hacker, they form beliefs about how much effort the organisation will go to in protecting its assets and how the State will punish it, if apprehended and convicted. The organisation will estimate the hacker's utility function, which will determine the amount they will attempt to Steal.

We show here, via a simple model with synthetic but plausible parameters, that mistaken players' beliefs about each other cannot yield a stable equilibrium outcome, but that with repeated rounds of the game, they will eventually converge. Whatever the equilibrium is, it probably implies that some amount of assets will be acquired illegally by the hacker, as both the organisation and the State may not find it optimal to drive this to zero.

Bibliography

Christopher Bliss (2000) "The Smash-and-Grab Game", paper presented to the 2000 Annual Conference of the Royal Economic Society, St.Andrews

Clough, J. (2015) Principles of Cybercrime, 2nd edition, Cambridge University Press, Cambridge

Shari Lawrence Pfleeger and Deanna D Caputo (2012) "Leveraging behavioural science to mitigate cyber security risk**",** Computers & Security, Vol. 31, pp. 597-611

Kim-Kwang Raymond Choo (2011) "The cyber threat landscape: Challenges and future research directions", Computers & Security, Vol. 30, pp. 719-731

Jason Mallinder and Peter Drabwell (2014) "Cyber security: a critical examination of information sharing versus data sensitivity issues for organisations at risk of cyber-attack", Journal of Business Continuity & Emergency Planning, Vol. 7, No. 2, pp. 103-111

Hulisi Ogut, Srinivasan Raghunathan, and Nirup Menon (2011) "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection**",** Risk Analysis, Vol. 31, No. 3, 497-512

H M Government (2016) "National Cybersecurity Strategy 2016-2021", Accessed on 14th April 2017 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Eva Andrijcic and Barry Horowitz (2006) "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property**",** Risk Analysis, Vol. 26, No. 4, pp. 907-923.

Kelic, Andjelka; Collier, Zachary A; Brown, Christopher; Beyeler, Walter E; Outkin, Alexander V (2013) "Decision framework for evaluating the macroeconomic risks and policy impacts of cyber-attacks"**,** Environment system and Decisions, Vol. 33, No. 4, pp. 544-560

Rao, Nageswara S. V. (2016) "Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models", Risk Analysis, Vol. 36, No. 4, pp. 694-710

Ginger Davis; Alfredo Garcia; Weide Zhang (2009) "Empirical Analysis of the Effects of Cyber Security Incidents", Risk Analysis, Vol. 29, No.9, pp. 1304–1316

Christian Biener, Martin Eling and Jan Hendrik Wirfs (2015) “Insurability of Cyber Risk: An Empirical Analysis”, The Geneva Papers on Risk and Insurance, Vol. 40, No. 1, pp. 131–158

Mike McGuire and Samantha Dowling (2013) “Cyber-crime: A review of the evidence” Research Report 75, Home Office, United Kingdom

Cyril Roux (2015) “Cybersecurity and cyber risk”, speech to the Society of Actuaries in Ireland Risk Management Conference, Dublin, 30 September 2015. Available on http://www.bis.org/review/r151002d.pdf and https://next.ft.com/content/97034429-65d2-3341-8e26-71acc3917562

Rohini Tendulkar (2013) “Cybercrime, securities markets and systemic risk”, Staff Working Paper, IOSCO, available at http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

Financial Times (2015) “Top financiers voice concerns on extent of risks to banks”, FT City Network debates cybercrime, available at https://next.ft.com/content/b1e350c4-a27b-11e5-bc70-7ff6d4fd203a

Caroline Baylon, Roger Brunt and David Livingstone (2015) “Cyber Security at Civil Nuclear Facilities Understanding the Risks Cyber Security at Civil Nuclear Facilities: Understanding the Risks”, Chatham House Report, available at https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf