Issues & Studies© 48, no. 1 (March 2012): 85-119.

Responsive Regulation and the Reporting of Information Security Incidents—Taiwan and China

LENNON YAO-CHUNG CHANG

As most software used by government agencies and companies is proprietary, malicious computer activity targeting breaches in that software can be likened to a pandemic of an infectious disease in the cyber world. When a breach occurs, the consequences can be widespread and damaging because the damage can spread rapidly. Therefore, cybercrime prevention needs to involve all users in a cooperative effort, with warnings and information on countermeasures distributed to users in order to prevent the "disease" from spreading when unprotected computers encounter an attack. This cooperative effort relies heavily on all institutions reporting information security incidents. Based on institutional theory, together with regulatory pluralism and responsive regulation theory, this paper examines the pluralized regulatory approach adopted to promote a system for sharing reports of information security incidents in Taiwan and China. An expanded model of regulatory enforcement and a strengths-based pyramid are proposed and used as a framework for discussing existing systems for encouraging the reporting of information security incidents.

KEYWORDS: institutional theory; responsive regulation; information security; incident reporting; expanded regulatory pyramid.

LENNON YAO-CHUNG CHANG (張耀中) is an assistant professor at the City University of Hong Kong and an associate investigator at the ARC Centre of Excellence in Policing and Security, the Australian National University. He is interested in cybercrime, cyber security, responsive regulation, and crime prevention. He can be reached at <yclchang@cityu.edu.hk>.

* * *

As most private- and public-sector organizations use proprietary software, cybercrime can easily have a "chain reaction"—hacking into one system means hacking into other systems as well. Malware spreads like a communicable disease in the general community: the malicious software or tool will constantly replicate itself and find new victims. If we cannot stop this kind of malicious activity, it will transplant itself into other systems and cause further damage.

Take the case of Google which was attacked by Chinese hackers in January 2010. This attack was dubbed "Operation Aurora" by MacAfee.[1] Microsoft admitted to a breach of security in its Internet Explorer 6.0 (IE 6.0) program, which enabled it to be used as the vector for this sophisticated hacking event. However, Google was not the only company to suffer from the attack. MacAfee warned that as many as thirty other companies were hacked, ranging from software firms to firms in the financial and defense sectors.[2]

Just as cybercrime is becoming "wikified,"[3] so too should crime prevention.[4] Brenner[5] used the term "distributed security" to emphasize that government, individual, and organizational users and computer architects should all share responsibility for cybersecurity. Similarly, Chang[6] proposed the idea of "wiki crime prevention" to address the need for mass collaboration between the government and private sectors to facilitate the

[1]Due to a belief that this was the name used by the hackers.

[2]"Microsoft Admits Explorer Used in Google China Hack," *BBC News*, January 15, 2010, http://news.bbc.co.uk/2/hi/technology/8460819.stm (accessed January 18, 2012).

[3]David S. Wall, "Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime (revised May 2010)," *Information, Communication & Society* 11, no. 6 (July 2008): 861-84.

[4]Chang, Yao-chung, "Weiji shi fanzui yufang—cong richang shenghuo lilun tan wanglu fanzui yufang moshi" ('Wiki' crime prevention—what routine activity theory teaches us about cybercrime prevention), *Fanzuixue qikan* (Journal of Criminology) (Jiayi) 12, no. 2 (December 2009): 87-116.

[5]Susan W. Brenner, "Distributed Security: A New Model of Law Enforcement," *Journal of International Law* 8, no. 5 (2004): 7-25.

[6]Chang, "Weiji shi fanzui yufang," 105.

sharing of information on security incidents and the establishment of prior warning schemes. Although different terms are used by different scholars, they all recognize the importance of collective surveillance and collaboration in the fight against cybercrime. They also acknowledge the inadequacy of a national approach to preventing the dissemination of malware and they emphasize the urgent need to establish cooperation between the public and private sectors.

Indeed, countries such as the United States, Australia, Taiwan, and China are now establishing systems for reporting information security incidents aimed at preventing the dissemination of malware and reducing the potential harm of cybercrime.[7] These systems build cooperation with the private sector to secure the critical information infrastructure from cyber attack. Plural regulatory methods are used to facilitate the reporting of security incidents. These methods range from voluntary to compulsory reporting and from punishment to incentives.

This paper will analyze the mechanisms and regulations used to promote the reporting of information security incidents in both Taiwan and China. Based on the framework of institutional theory and responsive regulation, it will demonstrate the nature of the regulatory mechanisms and identify to what extent these mechanisms have been used to facilitate or regulate the reporting of information security incidents.

Institutional Theory and Responsive Regulation

Institutional theory questions how social choices are shaped, mediated, and channelled by the institutional environment.[8] According to this theory, in the commercial environment, a company's decisions are strongly

[7]Yao-chung Chang and Joanne Wu, "Cong Meiguo shiwu jingyan lun woguo de zi'an shijian tongbao yu zixun fenxiang jizhi" (Study on information security incident reporting and information sharing mechanism in Taiwan—from the perspective of the U.S. experience), *Keji falü touxi* (Science and Technology Law Review) (Taipei) 20, no. 8 (August 2008): 39-61.

[8]Andrew J. Hoffman, "Institutional Evolution and Change: Environmentalism and the U.S. Chemical Industry," *Academy of Management Journal* 42, no. 4 (August 1999): 351-71.

influenced by "a set of legitimate options which determine the group of actors composing the firm's *organizational field*."[9] Decisions are not based purely on the firm's internal arrangement but are also shaped by the norms, rules, and beliefs imposed upon the firm from outside.

An "organizational field" is defined by institutional theorists as a set of interdependent organizations participating in the same cultural and social subsystem. It may include constituents such as government, critical exchange partners, sources of funding, professional and trade associations, special interest groups, and the general public.[10] Hanna and Freeman argue that the constituents are in some respects alike, in particular those "classes of organizations which are relatively homogenous in terms of environmental vulnerability."[11] That is, they might share a common fate and need to cooperate with each other even though they are competitors.

Along the same lines as Hanna and Freeman, Hoffman argues further that, rather than being formed around common technologies or common industries, some organizational fields are formed around issues that bring together various field constituents with disparate purposes.[12] Indeed, it is not necessary for the constituents in an organizational field to share the same beliefs and attitudes. For example, chemical manufacturers and environmentalists may be part of the same organizational field yet compete with each other.

Constituents are bound together in three fields, or three pillars: the regulative, nominative, and cultural-cognitive (which are explained below) (see table 1). These three pillars coexist and are interconnected with each other, but any one of them can be dominant at any given time.[13]

---

[9]Ibid., 351.

[10]See, for example, Paul J. DiMaggio and Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* 48, no. 2 (April 1983): 147-60; W. Richard Scott, *Institutions and Organizations: Ideas and Interests*, 3rd ed. (London: Sage, 2008).

[11]Michael T. Hannan and John Freeman, "The Population Ecology of Organizations," *American Journal of Sociology* 82, no. 5 (March 1977): 934.

[12]Hoffman, "Institutional Evolution and Change," 352.

[13]Ibid., 351-52.

Table 1
Three Pillars of Institutions

	Regulative	Normative	Cognitive
Basis of compliance	Expedience	Social Obligation	Taken-for-grantedness Shared Understanding
Basis of order	Regulative rules	Biding Experience	Constructive Schema
Mechanisms	Coercive	Normative	Mimetic
Logic	Instrumentality	Appropriateness	Orthodoxy
Indicators	Rules, laws, sanctions	Certification, Accreditation	Prevalence, isomorphism
Affect	Fear, Guilt/ Innocence	Shame/ Horror	Certainty/confusion
Basis of legitimacy	Legally sanctioned	Morally governed	Culturally supported, conceptually correct

Source: Scott, *Institutions and Organizations*, 51.

Similar ideas have been proposed in the form of the concepts of " regulatory pluralism" and "responsive regulation." Concerning the former, Gunningham and Grabosky indicate that there is a variety of regulatory instruments available for use in forming a policy, such as command and control regulation, self-regulation, and voluntarism. Although each instrument can stand alone, a combination of instruments could be more effective.[14] In as similar way, Braithwaite argues that "responsive regulation requires regulators to be responsive to the conduct of those they seek to regulate in deciding whether a more or less interventionist response is required."[15]

Both regulatory pluralism and responsive regulation are approaches designed to improve the regulation of corporations, while institutional theorists start from a totally different angle, discussing the formation of an institution or institutional field. Despite the differences, we can see that these three pillars of institutional theory correspond to the ideas of regula-

[14]Neil Gunningham and Peter Grabosky, *Smart Regulation: Designing Environmental Policy* (Oxford: Oxford University Press, 1998), 251.

[15]Valerie Braithwaite, "Responsive Regulation and Taxation: Introduction," *Law and Policy* 29, no. 1 (January 2007): 4.

Table 2
Comparison of Institutional Theory, Regulation Pluralism, and Responsive Regulation

	Pillars		
Institutional theory	Regulative	Normative	Cognitive
Regulatory pluralism	Command and control regulation	Self-regulation	Voluntarism
Responsive regulation	Sanction	Shame	Education or persuasion

tory pluralism and responsive regulation (see table 2). They all focus on pluralism of regulation and favor approaches such as self-regulation or voluntarism when punishment is neither the only nor necessarily the best way of regulation.

The Regulative Pillar

Following on from DiMaggio and Powell who state that "organizational change is a direct response to government mandate," the regulative (or legal) aspects of institutions take the form of regulations which guide organizational actions by coercion or threat of legal sanctions.[16] That is, the central ingredients of the regulatory pillar are force, sanction, and expedience responses. Organizations accede to them to avoid punishment which may come from noncompliance. For example, in order to conform to environmental regulations, manufacturers adopt new pollution control technologies; similarly, physicians or forensic physicians report cases or suspected cases of infectious diseases because of the requirements of health laws.

However, a common response to the regulative pillar is, what are the organization's interests? The capability of regulators and the cost and expense of monitoring compliance is of concern to many organizations. Questions such as these might lead to a reduction in the compliance rate.[17]

[16]DiMaggio and Powell, "The Iron Cage Revisited," 150.

[17]Scott, *Institutions and Organizations*, 52-53; Hoffman, "Institutional Evolution and Change," 353.

Gunningham and Grabosky also point out the strengths and weaknesses of command and control regulation. Because of its clear and precise standards, they argue, command and control regulation is likely to be successful in some circumstances, but they also highlight some common problems which contribute to its limited effectiveness. These include regulators who might not have a comprehensive and accurate knowledge of the workings and capacity of a particular industry; an absence of incentive; the cost and difficulty of enforcement; resistance to what is perceived to be the heavy hand of regulation; its vulnerability to political manipulation; and the way it leads to increasing administrative complexity and a proliferation of laws.[18] Scott summarises these problems thus:

> A stable system of rules, whether formal or informal, backed by surveillance and sanctioning power that is accompanied by feelings of fear/guilt or innocence/incorruptibility is one prevailing view of institutions.[19]

In order to secure compliance, a "carrot and stick" approach is usually adopted. In other words, the punitive laws and regulations used in this pillar are often tempered with rules which give organizations an incentive to obey.

Moreover, government itself need not necessarily play the role of theregulator; it might vest that option in a neutral third party such as an independent compliance monitor or surrogate.[20] By doing this, the government may avoid criticism that it lacks industry knowledge and the capability to regulate. This option may also reduce costs and make enforcement easier.

The Normative Pillar

The normative pillar of institutions stems from professionalism. This has been interpreted as the collective struggle of the members of an occupation to define the conditions and methods of their work and to establish

[18]Gunningham and Grabosky, *Smart Regulation*, 44-46.
[19]Scott, *Institutions and Organizations*, 54.
[20]Gunningham and Grabosky, *Smart Regulation*, 101.

a cognitive base to legitimize their occupational autonomy.[21] This usually takes the form of rule-of-thumb, standards of operation, occupational standards, and educational curricula. These conditions are complied with by organizations out of a moral or ethical obligation to conform to the norms established by universities, professional training institutions, and trade associations.[22]

Likewise, Gunningham and Grabosky use the term "self-regulation" to describe this concept. As mentioned above, organizations may follow the standards established by "professionals." However, Gunningham and Grabosky agree that it is uncommon to see pure self-regulation without any external intervention. They refer to Rees's idea and identify three forms of self-regulation[23]: voluntary or total self-regulation (without government involvement), mandated self-regulation (involving direct government involvement), and mandated partial self-regulation (partial government involvement).

With respect to the strengths and weaknesses of self-regulation, Gunningham and Grabosky state that compared with command and control regulation, "self-regulation offers greater speed, flexibility, sensitivity to market circumstances, efficiency, and less government intervention." Because of the characteristics of self-regulation, "it might be regarded as a form of 'responsive regulation': regulation which responds to the particular circumstances of the industry in question."[24]

On the other hand, criticism of self-regulation tends to focus on its weakness, its often ineffective methods of enforcement, and its lenient

[21]See, for example, Magali Sarfatti Larson, *The Rise of Professionalism: A Sociological Analysis* (Berkeley, Calif.: University of California Press, 1977); Randall Collins, *The Credential Society: A Historical Sociology of Education and Stratification* (New York: Academic Press, 1979); DiMaggio and Powell, "The Iron Cage Revisited."

[22]Hoffman, "Institutional Evolution and Change," 353.

[23]Gunningham and Grabosky, *Smart Regulation*, 51; Joseph V. Rees, *Reforming the Workplace: A Study of Self-regulation in Occupational Health and Safety* (Philadelphia, Penn.: University of Pennsylvania Press, 1988).

[24]Gunningham and Grabosky, *Smart Regulation*, 52; Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford: Oxford University Press, 1992), 4-7.

punishments. Parker argues that "the pure 'voluntary' compliance or self-regulation is rare, or perhaps non-existent." For self-regulation to be effective there must be some motive that encourages organizational compliance, such as public image, leadership, or benefit.[25]

Gunningham and Grabosky also argue that a self-regulatory scheme will work best where "there is a degree of coincidence between the self-interest of the individual company or industry, and the wider public interest." Furthermore, if enterprises are aware of others' behavior and can detect noncompliance, or know if others have a history of noncooperation (such as within an existing association), and when clients value compliant behavior and can identify compliant firms, then self-regulation within an industry is likely to succeed.[26]

The Cultural-Cognitive Pillar

The third pillar identified in institutional theory is the cultural-cognitive element. It is argued by cultural-cognitive theorists to be the most important element of institutionalization. Zucker argues that institutionalization is rooted in conformity—conformity with taken-for-granted aspects of everyday life, rather than conformity with sanctions (whether positive or negative), or conformity with a "black-box" internalization process.[27]

Indeed, not all compliance derives from coercive authority or self-regulation. It is believed that compliance often occurs when other types of behavior are unthinkable. It can also occur when routines are followed because they are taken for granted as "the way we do things."[28] DiMaggio and Powell use the words "imitation" and "modelling" to describe this effect. They argue that imitation is encouraged when organizations face uncertainty, such as an ambiguous goal or an unclear solution.[29] This kind

[25]Christine Parker, *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge: Cambridge University Press, 2002), 76.

[26]Gunningham and Grabosky, *Smart Regulation*, 53-54.

[27]L. G. Zucker, "Organisations as Institutions," in *Research in the Sociology of Organizations*, ed. Samuel B. Bacharach (Greenwich, Conn.: JAI Press, 1983), 5.

[28]Scott, *Institutions and Organizations*, 58.

[29]DiMaggio and Powell, "The Iron Cage Revisited," 151.

of imitation or modelling is sometimes diffused through the turnover or transfer of employees.

In terms of the corresponding concept within regulatory pluralism, the term "voluntarism" has been used. Unlike command and control regulation, in which is embedded coercion, sanctions, or self-regulation, and which usually occurs under pressure from customers or an industry association, some enterprises voluntarily submit to compliance simply because they think they are doing the right thing. This relies on their enthusiasm and goodwill.[30]

Gunningham and Grabosky argue that a voluntarist program is usually initiated by government, or government may be involved in the program and may play a role. They state that, although voluntary agreements between government and individual enterprises take the form of "non-mandatory" agreements, they are not really non-mandatory at all. They recognize these as "an innovative form of command and control."[31] So many nonmandatory programs still contain coercive elements, although these may take the form of incentives, rather than sanctions, to encourage individual enterprises to join the program. Equally, the individual enterprise might be under strong pressure (reputational risk) to join the program.

Strengths-Based Strategies

From the discussion above, we can see that the "carrot and stick" approach is frequently used in responsive regulation, whether in command and control regulation, self-regulation, or voluntarism. Positive incentives and rewards, alone or in combination with regulations, play an important role in inducing organizations to comply or to follow the correct institu-

[30]Neil Gunningham and Darren Sinclair, "Integrative Regulation: A Principle-Based Approach to Environmental Policy," *Law & Social Inquiry* 24, no. 4 (Autumn 1999): 853-96.

[31]Gunningham and Grabosky, *Smart Regulation*, 56.

tional path. However, Grabosky[32] argues that the carrot and the stick can be used individually or together, depending on the situation:

> Carrots and sticks need not be inextricably linked. Nor are they invariably independent. Their respective use, alone or in combination, will vary according to the risk they are intended to control, the target of the incentive in question, or the wider regulatory context in which they exist.[33]

Incentives may be distinguished by their material nature. Grabosky[34] indicates that they may entail a transfer payment or alternative financial benefit, or symbolic recognition, or some other consideration. An incentive could be material (monetary), such as a tax credit or financial subsidy; it could be symbolic (nonmonetary) such as a prize, praise, or immunity from prosecution or punishment; or it could be a combination of these elements.

Nonetheless, there may be some side effects to the offer of incentives. Grabosky argues that authorities, when contemplating the use of an incentive system, should also be wary of the vulnerabilities within that system such as subversion or abuse. Therefore, he expresses the view that "nonmonetary incentives appear to have considerable promise" where they "encourage one to focus on the moral rather than the material aspects of compliance."[35]

Braithwaite holds a similar view and argues that informal praise—inspectors giving a word of encouragement when they see an improvement—seems to have unequivocally positive effects.[36] However, while Grabosky suggests that incentives and rewards might fit into the model of the regulatory enforcement pyramid proposed by Ayres and Braithwaite, in that they attract the attention of those who are nonchalant or lack

---

[32]Peter Grabosky, "Regulation by Reward: On the Use of Incentives as Regulatory Instruments," *Law and Policy* 17, no. 3 (July 1995): 257-82.

[33]Ibid., 270-71.

[34]Ibid.

[35]Ibid., 237.

[36]John Braithwaite, "Reward and Regulation," *Journal of Law and Society* 29, no. 1 (March 2002): 12-26.

awareness,[37] John Braithwaite argues that "attempts to replace punishment with reward in a regulatory pyramid tend to be illusory," because "the reward strategy thus introduces incentives to cheat on reporting."[38]

Braithwaite et al. propose a strengths-based pyramid similar to the regulatory enforcement pyramid. Using Malcolm Sparrow's ideas on "pick problems and fix them," this strengths-based pyramid is based on "pick strengths and expand them." And instead of becoming immersed in guaranteeing a minimum standard, the strengths-pyramid tries to maximize quality by pulling the standard up through a ceiling.[39]

As shown in figure 1, the two pyramids are only linked to each other at the bottom. The adjoining sides of the pyramids are sequential alternatives rather than complementary. Regulators should decide which pyramid to use only beyond education and persuasion (bottom level). If the regulatee is doing a good job, then the strengths-based pyramid might be used to encourage him to keep going. However, if education and persuasion did not work well, Braithwaite suggests, the regulatory enforcement pyramid should be used instead.

Since these two pyramids are sequential alternatives rather than complementary approaches, they should not be used at the same time. However, regulators can switch between the two pyramids when they think it is suitable to do so.

Braithwaite et al. state that the strengths-based pyramid is different from the multisided pyramid proposed by Gunningham and Grabosky. That pyramid is based on different regulators and they should not be confused.[40] Similar to the strengths-based pyramid constructed according to the model of regulatory enforcement by Ayres and Braithwaite,[41] the

[37]Grabosky, "Regulation by Reward," 272; Ayers and Braithwaite, *Responsive Regulation*, 35-41.

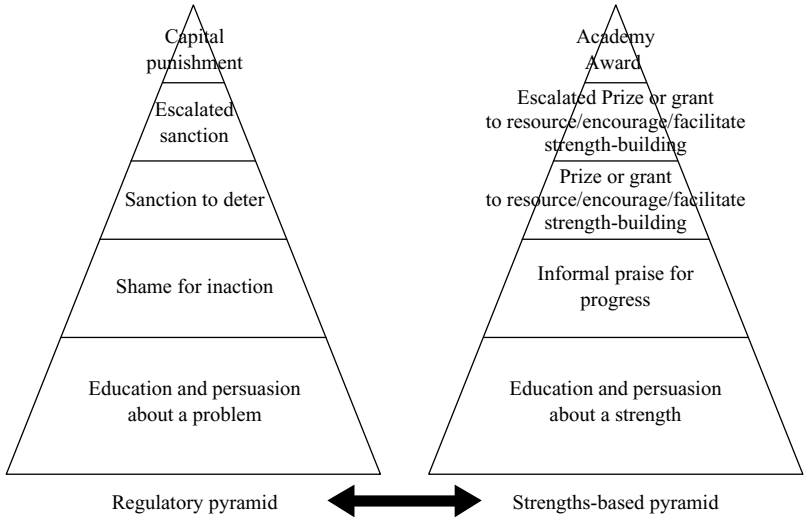
[38]Braithwaite, "Reward and Regulation," 22.

[39]John Braithwaite, Toni Makkai, and Valerie Braithwaite, *Regulating Aged Care: Ritualism and the New Pyramid* (Cheltenham: Edward Elgar, 2007), 318.

[40]Ibid., 315-20; Gunningham and Grabosky, *Smart Regulation*, 398.

[41]Ayers and Braithwaite, *Responsive Regulation*, 35.

Figure 1
Comparison of a Regulatory Pyramid and a Strengths-based Pyramid



Source: Braithwaite, Makkai, and Braithwaite, *Regulating Aged Care*, 319.

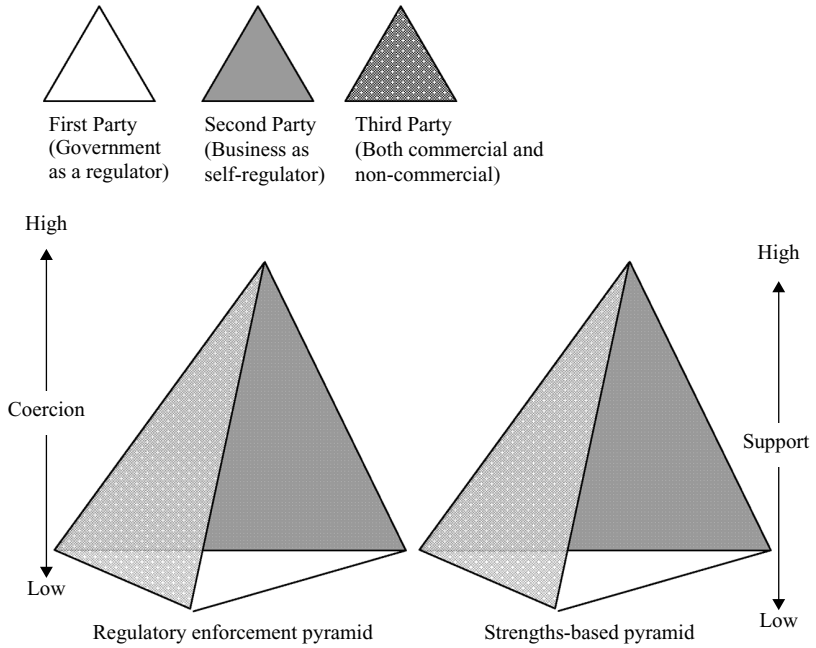
multi-sided regulatory pyramid has been constructed by Gunningham and Grabosky[42] to expand the idea of regulation.

Gunningham and Grabosky argue that escalation up the pyramid is possible even when the regulator is not a state. Therefore, they believe that it would be useful to conceive their pyramid as having three faces: first party (government as regulator), second party (business as self-regulator), and third parties (both commercial and noncommercial).[43]

These two different ways of thinking have their respective merits and their ideas are not mutually exclusive. Gunningham and Grabosky state that, under regulatory pluralism, the state need not be the only regulator. Both self-regulation and voluntarism can apply. States may play some role in this plural regulatory scheme, but they are not absolutely the regulator.

[42]Gunningham and Grabosky, *Smart Regulation*, 398.
[43]Ibid.

Figure 2
Regulatory Enforcement and Strengths-based Pyramid—Expanded Model



Source: modified from Gunningham and Grabosky, *Smart Regulation*, 398.

And Braithwaite et al. argue that, apart from the regulatory enforcement pyramid, the strengths enforcement model might also be helpful where organizations are adopting institutions.[44] They need not conflict with each other. Rather, they are sequential alternatives. They can operate simultaneously to foster a regulatory environment and provide a greater level of choice.

Gunningham and Grabosky explain how the three faces work in the regulatory enforcement pyramid (see figure 2). There may also be three faces to the strengths-based pyramid. In that case, there would be six faces

[44]Braithwaite, Makkai, and Braithwaite, *Regulating Aged Care*, 315-20.

within the two pyramids: Enforcement-1 to Enforcement-3, and Strength-1 to Strength-3, where enforcement and strength mean the regulatory enforcement pyramid and the strengths-based pyramid, respectively, and 1-3 refers to which party acts as the regulator, as indicated by Gunningham and Grabosky.[45]

However, different faces can be used at the same time to regulate or encourage behavior. Take the regulation of removal companies in Taiwan for example. Enforcement-1 is used to regulate the behavior of removal companies, and if removal companies are dishonest or do not provide a good service, they are fined or they have their licences suspended by the government. However, this model does not work very well and the market is still chaotic. There are still disputes between removal companies and customers. Fraud and threatening incidents often occur, giving the industry the reputation of "moving-hoodlums" (**搬家流氓**).

Since 1996, a private non-profit foundation called the Tsuei Ma Ma Foundation for Housing and Community Service (**崔媽媽基金會**) has published the *Quality Moving Company List*. The foundation regularly evaluates removal companies and recommends the good ones. It is a voluntary program, so not every removal company is evaluated. Only those who submit their information to the foundation are evaluated and listed.

As Gunningham and Grabosky have said, "the challenge in designing voluntary mechanisms is to build, rather than hinder, the development of a custodial ethic."[46] In the above example the Tsuei Ma Ma Foundation is trying to build up norms for the removal industry and to encourage quality removal companies to keep their behavior and reputation to a high standard. Even the government body that regulates such firms, the Consumer Protection Committee, is supportive of the foundation's list and encourages citizens to use the companies it recommends.

Because of the work of both the nonprofit foundation and the government agency, combined with "word of mouth," more and more people who

[45]Gunningham and Grabosky, *Smart Regulation*, 398.
[46]Ibid., 59.

are planning to move house check the foundation's website and select a removal firm that it recommends. Removal companies are thus incentivized (or pressured) to submit themselves for evaluation and possible recommendation by the foundation.

Companies that have already received a recommendation are encouraged to maintain their standards, and thus this mechanism can aid the development of a removal company's customer service institution. It might be seen as the formation of an institution by praise through a third party (Strength-3). Pressure from customers may also encourage the development of self-regulation (Strength-2) in the removal industry.

Existing Models for Sharing Reports of Information Security Incidents in Taiwan and China

From the above discussion of institutional theory and responsive regulation, we can see that organizations may adopt an institutional program according to the requirements of command and control regulation or self-regulation, or they may sometimes just take their model for granted. And we can also see that both the stick and the carrot play important roles in encouraging organizations to adopt an institutional program. These discussions will be helpful when establishing a prior warning system for information security incidents.

Currently there are programs in both Taiwan and China to encourage the reporting of information security incidents. For example, the Taiwanese government has promulgated the Measures on National Information and Communication Security Incident Reporting and Responses to encourage the reporting of incidents within the government. In China, the Mechanism on Trojan and Botnet Monitoring and Disposal requires Internet service providers (ISPs) to report any unusual data flows they may have monitored. There is also some self-regulation and voluntarism. Some of the programs have a top-down approach while others are organized from the bottom up. Some have compulsory reporting mechanisms which are government-mandated, others have developed under pressure from the

industry, and still others have evolved voluntarily.

The Regulative Pillar in China

The regulative pillar uses coercion or threats from government to force organizations to form institutions. Sanctions are usually applied if an organization fails to follow these laws or regulations. With respect to information security incidents, rewards and other positive incentives are also used by governments to encourage enterprises and government agencies to submit reports.

In China, there are regulations which require organizations or enterprises to report information security incidents as they occur or when they are discovered. These include the Special Regulations on Commercial Bank Information Disclosure (**商業銀行資訊披露特別規定**), the Mechanism on Trojan and Botnet Monitoring and Disposal (**木馬和僵屍網路監測與處置機制**) and the Measures on Internet Information Security Incident Reporting (**互聯網網路安全資訊通報實施辦法**).

Special Regulations on Commercial Bank Information Disclosure: These regulations were promulgated by the China Securities Regulatory Commission in 2008 with the aim of ensuring that commercial banks disclose significant events that might put their business or share price at risk. According to Article 16 of the regulations, commercial banks are required to report any operational risks, including risks caused by internal procedural problems, employee problems, and problems within their operating systems. If a bank intentionally or fraudulently fails to report, a fine of between RMB300,000 and RMB600,000 is applied (equivalent to US$50-120,000). However, the purpose of this reporting is to let shareholders know what is happening to the bank, rather than to establish a prior warning system.

Mechanism on Trojan and Botnet Monitoring and Disposal: This mechanism, which came into practice in June 2009, is used by the Chinese government to prevent the spread and influence of botnets and Trojan horses. It requires all ISPs in China to report instances of such activity to the Bureau of Communications Security under the Ministry of Industry and Information Technology, with a copy being sent to the National Com-

puter Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC).

After receiving a report, CNCERT/CC analyzes the event, and with the cooperation of the Information Security Research Institute and other enterprises and international organizations, shares suggestions on how to deal with the problem with other ISPs. CNCERT/CC will also send a notice to the owner of the infected system and ask them to take proper measures to get rid of the malicious code.

Measures on Internet Information Security Incident Reporting: These measures were enacted at the same time as the above mechanism, but whereas the Mechanism on Trojan and Botnet Monitoring and Disposal is focused solely on the reporting of botnets and Trojan horses, these measures cover all kinds of information security incidents. More private organizations have been included as gatekeepers.

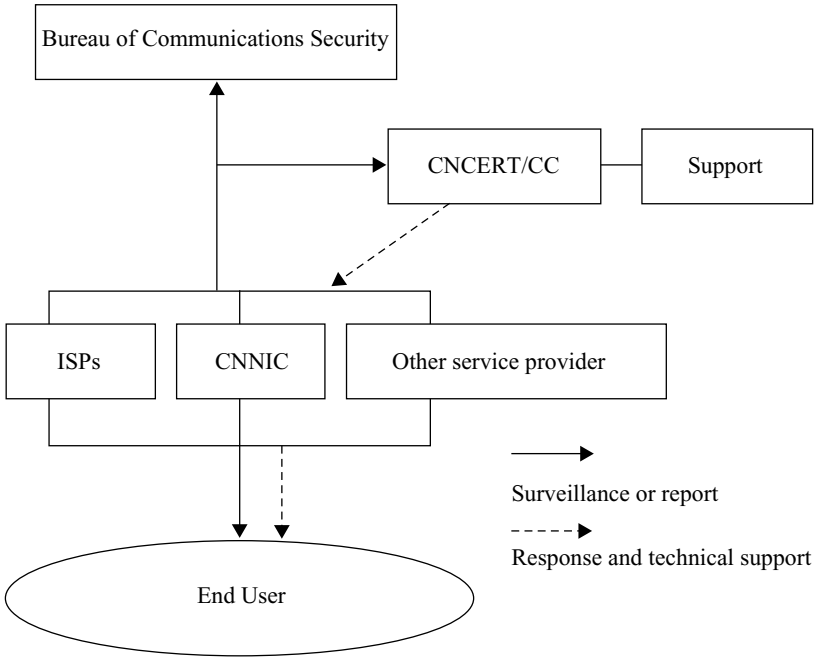
In addition to ISPs, all Internet platform providers and search engines (such as Yahoo, Google, and Baidu), Internet data connectors, and the China Internet Network Information Center (CNNIC) and its service institutes, are required to monitor and report information security incidents that occur in their area. They report these incidents to the Bureau of Communications Security and send a copy to CNCERT/CC (Article 7).[47] The content of the report should include a brief description of the incident, a rough evaluation of any damage and impact, the control measures that have been adopted, and any other related issues (Article 14).

As it does with the Mechanism on Trojan and Botnet Monitoring and Disposal, CNCERT/CC has the task of analysing the incident and responding to it, with the support of other public and private information security agencies and other international information security organizations.

These two regulations make no mention of punishments or rewards. These are addressed in the Strategies for Information Security Incident Reporting and Response (**互聯網網路安全應急預案**) and the Emergency Response Law of the People's Republic of China (**中華人民共和國突發事**

[47]For the duties of each of these organizations, please see appendix 1 of the Measures on Internet Information Security Incident Reporting.

Figure 3
Model of Compulsory Reporting System—China



件應對法). These are laws upon which the two regulations are based, and they promote the "carrot and stick" approach as a way of boosting the reporting rate. According to Article 5.2 of the strategies, an organization or individual with an excellent record of reporting and responding will be rewarded. Those who fail to report or who are careless in their reporting will be punished. More specifically, according to Articles 63-65 of the Emergency Response Law, an organization that fails to report, or which makes a false report, will suffer administrative sanctions which may include licence suspension or revocation.

The Regulative Pillar in Taiwan

The Taiwan government has promulgated various command and control measures to promote reporting. In particular, its has addressed

reporting by government agencies and critical parts of the information infrastructure.

Guidelines on Reporting Significant Contingent Incidents in Banks: Under these guidelines, it is compulsory to disclose any contingent incidents (including information security incidents) which might cause serious harm or significant loss to a bank. Once the incident has been discovered, the official in charge must report directly to the Banking Bureau of the Financial Supervisory Commission. Within one week, the official must send a report to the bureau which includes details of the incident, its impact, and the subsequent measures adopted.

Like China's Special Regulation on Commercial Bank Information Disclosure, the purpose of the guidelines is to let the Banking Bureau, the shareholders, and the general public know what has happened to a bank and how the problem was dealt with. It is not a prior warning system. There is no feedback after the initial reporting.

Measures on National Information and Communication Security Incident Reporting and Responses (**國家資通安全通報應變作業綱要**): These measures were introduced by the National Information and Communication Security Task Force (**國家資通安全會報**)[48] in 2009 to control security incidents that occur in government agencies and important public or private industries. They are similar to the Federal Information Security Management Act of 2002 in the United States and require the immediate reporting of incidents and the prompt adoption of adequate responses.

Although they are intended to deal with security incidents in both the public and private sectors, these measures only have command and control powers over government agencies. However, the private sector, in particular highly regulated industries such as banking and telecommunications, is welcome to join in information sharing.

According to the measures, each government agency and institution must create a position of chief information officer (CIO) and a deputy CIO

[48]This task force was established in 2001 by the Executive Yuan with the purpose of devising policies on national information and communication security, enhancing the information and communication security environment, and boosting national competitiveness.

to take charge of information security and other related issues. The CIO should also designate a contact point within the agency to receive reports and responses.

Chapter 3 of the measures regulates the procedure for reporting incidents. When an information security incident occurs or is discovered, the individual in charge of information security must report the incident to their superior (such as the CIO) and to the National Information and Communication Security Task Force via the website of the National Computer Emergency Response Team (TWNCERT). After receiving such a report and any request for technical support, TWNCERT will assist the agency by providing damage recovery procedures.

The report should include details of the incident, the impact level, and whether or not technical support is needed. The reporter should also evaluate the seriousness of the incident and its influence on other critical infrastructures.

Information security incidents are not easily discovered by outsiders if an agency does not want to publicize the problem. In order to prevent agencies from covering up incidents, the government in Taiwan has adopted strategies that provide services rather than imposing regulations and that focus on rewards rather than punishments. According to Chapter 6 of the measures, no punishments, only rewards and praise, have actually been used.

In order to prevent an incident from spreading and thereby doing more damage, Chapter 6.1 of the measures allows for those agencies that submit a timely report to be commended and rewarded. On the other hand, those agencies that fail to report incidents are subject to "rectification counselling."

The Normative Pillar in China

The normative pillar, or self-regulation, refers to compliance by organizations out of an ethical or moral obligation to follow the standards established by universities, professional training institutions, and/or trade associations. It might appear in different guises and be mandatory, voluntary, or some combination of the two.

Apart from command and control regulations that mandate reporting, self-regulation is also used by some industries in China for information incident reporting. This includes the Self-Regulation Agreement against Malicious Software (**抵制惡意軟體自律公約**) promulgated by the Internet Society of China and the Guidelines for the Banking Industry on Contingency Planning (**中國銀行業營業網點服務突發事件應急處理工作指引**) published by the China Banking Association.

Self-regulation Agreement against Malicious Software: This agreement[49] was introduced in December 2006 to prevent the spread of malicious software. Most of the large telecommunication companies and ISPs, such as China Telecom, CNNIC, Yahoo, Baidu, and Sina, voluntarily signed up to the agreement.[50] As the agreement is organized and promoted mainly by the industry itself and there is no government involvement, it can be identified as a voluntary form of self-regulation.[51]

Signatories are required to protect the cyberspace environment and to do their best to control malicious software. If malicious software is found by a member-company, the company undertakes to report its discovery to the Internet Society of China and to share that information with other companies (Articles 13-15).

There is no direct provision for incentives in the agreement—whether positive or negative. However, Article 21 identifies an indirect punishment (or positive incentive) that may encourage some companies to participate. According to Article 21, if malicious software is found to have originated with a nonsignatory company, the society will publicize the name of the software and the company that has manufactured it and draw it to the atten-

[49]The malicious software that is the subject of this agreement is, according to Article 2, different from malicious code, such as viruses, worms, or Trojan horses, which is designed only for the purpose of committing crime. Instead, it is defined as software which does not allow its users to uninstall it or that does not allow users to decide whether to install it or not.

[50]Kai-Fu Chang, "32 jia qiye qianshu zilü gongyue, huaqing yu eyi ruanjian jiexian" (32 companies signed the self-regulation against malicious software), *CBI News*, December 29, 2006.

[51]Joseph Rees, *Reforming the Workplace: A Study of Self-regulation in Occupational Health and Safety* (Philadelphia, Penn.: University of Pennsylvania Press, 1988), 11.

tion of the public. However, if the software has originated with a signatory of the agreement, the problem will be rectified before the public is notified. The incident will only be publicized if a signatory fails or is unwilling to fix the problem. Therefore, in order to protect their reputation, and to avoid criticism from the public, software producers are encouraged to sign the agreement and become members of the Internet Society of China.

Guidelines for the Banking Industry on Contingency Planning: Whereas the Self-Regulation Agreement against Malicious Software combines voluntarism with shaming, these guidelines compel banks to self-regulate in terms of reporting contingent Internet security incidents.

Unlike the Self-Regulation Agreement which was drafted mainly by the Internet Society of China and which members can sign up to voluntarily, the guidelines, which were announced on July 7, 2009 by the China Banking Association, are more self-mandated. Since they are a product of the Emergency Response Law, all members of the China Banking Association are required to follow them.

According to the guidelines, banks are required to report any contingent incidents (including information security incidents) to a competent authority (Articles 1-3). Article 5 requires that banks should also report incidents to other banks which may have been affected.

In terms of incentives, Article 20 suggests that a member bank should reward individuals or sections that have done well in incident reporting and punish those who failed to report or who do not follow the reporting guidelines.

The Normative Pillar in Taiwan

The Measures on National Information and Communication Security Incident Reporting and Responses paved the way for self-regulation in industries involved in critical infrastructure. The Bankers Association of the Republic of China also provides a level of self-regulation in terms of bank security and safety. Both of these instruments might be used to further promote the reporting of information security incidents.

Measures on National Information and Communication Security Incident Reporting and Responses: These measures are aimed at setting up

Table 3
Incident Reporting and Responses by Sector—Taiwan

Sector	Authority in Charge	Range
National defence	Ministry of National Defence	National defence system
Administrative institutions	Research, development and Evaluation Commission	Administrative agencies
Academic institutions	Ministry of Education	School and research institutes
Utilities	Ministry of Economy	Electricity, petro, water and gas industry
Transportation industry	Ministry of Transportation	Telecommunication, post and transportation services
Financial affairs	Ministry of Finance	Finance, customs and trade institutions
Banking and securities services	Financial Supervisory Commission	Financial services industry
Health and medical	Department of Heath	Health and medical institutions
Communication and broadcasting sectors	National Communication Commission	Communication and broadcasting industry

a prior warning system within government agencies and critical infrastructure. Learning from presidential directive PDD 63 and the Federal Information Security Management Act (FISMA) in the United States, the Taiwan government is also seeking to encourage industries involved in critical national infrastructure to establish their own information sharing and analysis centers (ISACs) as a platform for reporting and sharing information about security incidents. Such measures build national resilience—the capacity to recover quickly from an attack and reduce its impact.

Critical infrastructure industries are categorised into nine sectors: national defense, administrative institutions, academic institutions, utilities, transportation, finance, banking and securities, health and medical, and communication and broadcasting (see table 3). Certain government agencies (usually the central authority in charge of that industry) are delegated to encourage and promote the establishment of ISACs. In this way,

these measures can be identified as a means of mandated self-regulation for designated government agencies in Taiwan.

Some government agencies are required to report incidents, whereas other government agencies and private enterprises may join an ISAC if they want to. The measures do not allow for enterprises to be forced to join, although incentives, such as a free integrity test and an incident response exercise, are used to encourage them to do so. Of course, enterprises that join the scheme may also receive technical support on system recovery and warnings of future attacks. They will also be advised of appropriate ways to prevent attacks.

Although there is direct government involvement in the measures, they are still identified as being voluntary for non-designated government agencies and the private sector.

Bankers Association of the Republic of China: This association has not drawn up any guidelines or regulations governing incident reporting. However, there are other forms of self-regulation that might be used to encourage member-banks to share information on security incidents.

For banks in Taiwan, social responsibility is an important element in the running of their businesses, and in addition to maximizing their benefits to shareholders, they are expected to take a lead in such areas as obedience to the law, the promotion of progress on economic and environmental issues, and other not-for-profit activities. Both the Self-Regulation Treaty for Members of the Bankers Association of the Republic of China and the Corporate Governance Guidelines for Banks emphasize the importance of social responsibility. Although there are no articles in the Self-Regulation Agreement relating to information sharing, Article 22 allows for rewards or commendations for members of the association who help to maintain the operation of the financial markets. So if a bank shares knowledge of an information security incident with other banks, and by so doing prevents those banks from suffering losses, that bank may be rewarded or commended by the association.

Indeed, a system of self-regulation and prior warning already exists with respect to fraud, as banks are required under the Operating Procedure on Warning of Fraudulent Accounts to report any movement of funds into

or out of certain accounts which the police or the courts suspect are being used for fraud. These transactions must be reported to the police as well as to the banks to which the money is moved. This information-sharing model might be helpful when establishing a prior warning system for reporting information security incidents.

The Cultural-Cognitive Pillar in China

In addition to regulated or self-regulated reporting systems, there are other voluntary information-sharing schemes in China and Taiwan. Some enterprises submit reports voluntarily because they deem it necessary or helpful to society. Moreover, they might be rewarded for sharing this information. We have already seen that China has very detailed regulations on incident reporting. CNCERT/CC plays a very important role in compulsory reporting scheme, and enterprises which do not come within the scope of this system also share information if they think it necessary.[52]

Computer emergency response teams (CERTs): An enterprise may choose to report an incident to *CNCERT/CC*, even if they are not required to do so. For example, a bank may submit an online report about a contingent incident to CNCERT/CC and seek help from them. After analyzing the incident, CNCERT/CC will respond to the report and share the information on its website or through emails to its subscribers. The response will include suggestions on possible solutions or preventive measures.

There are some CERTs which focus on a specific industry or group. For example, the China Mobile Computer Network Emergency Response Technical Team/Coordination Center (CMCERT/CC), which is a member of the Forum of Incident Response and Security Teams (FIRST), deals with voluntary reports on information security incidents from the telecommunication sector. The Education and Research Network Computer Emergency Response Team (CCERT), which is a member of the Asia Paci-

[52]Some big antivirus or information security companies (such as Symantec or Cisco) also provide services to their users in the form of incident reporting and response, although this kind of service is mostly available only for their own customers. For this reason, it will not be included in the discussion here.

fic Computer Emergency Response Team (APCERT), provides a platform for educational institutes to report their information security incidents.

Informal sharing: There is also informal information sharing among the information technology divisions of different companies. For example, interviewee C001[53] indicated that IT managers and IT employees catch up with each other at irregular intervals and share information about what is happening in the area of security and how to deal with it. Indeed, C001 usually received the latest information about viruses or other malicious activities by talking with IT managers in other companies. When asked why they were willing to share such information, he said it was because they were often old friends and did not want their friends to get into trouble:

> We share because we are suffering from the problem and want our friends to take proper measures before they are attacked or damaged. It is human nature to tell your friends how to avoid trouble, isn't it? (C001_08).

C001's words fit the cultural-cognitive pillar of institutional theory and Zucker's idea that conformity is rooted in the "taken-for-granted."[54] C001 specifically mentions that sharing with friends is normal behavior. They share information security problems with their friends so their friends can avoid experiencing the same problem.

C001 was not the only interviewee to share information with his friends on information security incidents and malicious activities. C003-2 also admitted to the existence of private information sharing. C003-2 said that some companies might not be willing to share information formally

---

[53]The data used in this paper were collected in the Greater China Area (Taiwan, China, and the Hong Kong Special Administrative Region) in 2008 and 2009. Thirty-eight interviews (including four focus groups, one in China and three in Taiwan) with a total of forty-four interviewees were conducted in Taiwan and China during this period. Interviewees were selected on the basis of their work experience or background, in particular, people with knowledge of information security and cybercrime. These included, but were not limited to, IT professionals in government agencies and private companies, police officers, prosecutors, and other professionals in cybercrime and information security, such as professors, managers of legal compliance in companies, and information security experts in big accounting firms which audit information security and conduct staff training in organizations. All those interviewed in Taiwan were coded with the letter "T" while those in China were coded with the letter "C." The number following the letter refers to the case record. For example, T001 means the first interview conducted in Taiwan.

[54]See Zucker, *Research in the Sociology of Organizations*, 2-5.

and publicly. However, they are willing to share their problems and experiences with good friends or others they trust:

> They might not be willing to report in accordance with the institution. However, they meet with others who are also working in the industry. They might share their problems at their meetings. . . . With their good friends or others in the same industry they would share privately information about what is happening and maybe how to prevent it. (C003-2_12)

C003-2 highlighted one case in the securities industry in southern China which shows how this informal sharing works within the industry:

> I have heard about this kind of information sharing in the security industry in a southern province. The stock exchange in Shenzhen (**深圳**) has developed a sharing platform. It provides a service to other securities companies in the area and shares the issue with other members of the platform. Because they are all in the securities industry and involved in online trading, they are all facing similar information security problems. (C003-2_18)

The Cultural-Cognitive Pillar in Taiwan

Like its counterpart in China, The Taiwan Computer Emergency Response Team Coordination Center (TWCERT/CC) plays an important role in voluntary incident reporting. The interview data also contain examples of informal sharing between trusted groups in Taiwan.

TWCERT/CC: Although there are two CERTs in Taiwan, TWNCERT and TWCERT/CC, only TWCERT/CC provides a voluntary information-sharing platform to the public. TWNCERT only deals with government agencies and enterprises involved in critical infrastructure which have joined as members.

TWCERT/CC runs a voluntary reporting platform for end users to report incidents, vulnerabilities, and breaches. When it receives a report of an information security incident, it analyzes it and helps the reporter to fix the problem or tells them what measures need to be taken. Additionally, it will share that information on its website and through its email subscriber list.

Although TWNCERT does not provide a platform for the public to report incidents, it does share information on incidents, vulnerabilities, and breaches with everyone on its website, where it also provides advice and instructions for removing malicious code. It also provides patches for software.

Informal sharing: Informal sharing within trusted groups occurs in Taiwan as well as in China. Interviewee T012 said he likes to share his experiences with others. He likes to help them and prevent them from experiencing the trouble he has experienced. T017 said that she had concerns about the formal information sharing required by the government, but she would definitely share information about a security incident or malicious activity with her friends and bring the problem to their attention. This is a good example of informal guardianship:

> When I find out about or hear about an incident, I contact my colleagues and tell them to keep an eye out for the problem and maybe take some measure to prevent it. I might not report formally, but there are some informal channels for dealing with this problem. (T017_14)

T023, from a different industry, also indicated the existence of an informal information-sharing channel:

> We have an informal channel for sharing information about security incidents. We usually exchange experiences and learn from others on management issues. Sometimes when I am on a work trip and visit other companies, we will discuss the difficulties and problems we face. From the discussion, I can learn from them about what happened in their company and how they dealt with the problem. (T023_09)

However, when asked how the informal channel was built up, T023 said that *guanxi* (connections) and trust played a very important role in its formation:

> I know most of the IT managers in other companies. The IT manager in "A" company used to be my colleague when I was working at "B" company. So too was the other guy who is now the IT manager in "C" company! However, it is a private channel. Others will only share information with you when you know them well. I will never get information from "D" company because I don't know the guy working there! Guanxi is very important! (T023_09-10)

That is to say, sharing is limited to a certain group of people. They will not share information with those they are not familiar with, and nor will they receive information of incidents from strangers. T023 indicated that he would only share information with friends and it was impossible for him to get information from someone he did not know.

Discussion: Enforcement vs. Strength

From the discussion above, we can see that all three pillars have been used during the formation of reporting and response institutions in China and Taiwan. As Gunningham and Grabosky[55] have suggested, these methods of regulation may be even more effective when used in combination with each other than they are when used alone.

Enforcement-1 vs. Strength-1

As per command and control regulation, we can see that both Enforcement-1 and Strength-1 are used in the design of the Chinese reporting system (see the discussion above of the regulatory enforcement and strengths-based pyramids in figure 2). Although reporting is compulsory, the government offers rewards to companies which do well in reporting as well as punishing those who fail to report. Moreover, the support offered by CNCERT/CC in terms of analyzing the reports and responding to all ISPs might also induce ISPs to report incidents that they have monitored.

The Measures on National Information and Communication Security Incident Reporting and Responses use strengths-based measures (Strength-1) to promote reporting by government agencies. However, the Regulatory Enforcement Pyramid has also been secretly used. As discussed above, if a government official fails to report, then administrative sanctions might be applied against him. This is particularly the case when serious damage has been caused because of his failure to report or if he intentionally covers up the incident (Enforcement-1).

Enforcement-2 vs. Strength-2

In terms of self-regulation, we can see examples of Enforcement-2 and Strength-2. The Self-Regulation Agreement against Malicious Software uses "shaming" strategies to encourage telecommunication or telecommunication-related enterprises to sign up to the agreement. According

[55]Gunningham and Grabosky, Smart Regulation, 398-401.

to Braithwaite, this is an example of the use of enforcement power, rather than strength power, to form the institution (see figure 1). Moreover, because it is regulated by an association, which is defined by Gunningham and Grabosky as a second party, it can be seen as using Enforcement-2 as an instrument to form the institution.[56]

Similarly, Enforcement-2 and Strength-2 have been recommended by the China Banking Association through its Guidelines for the Banking Industry on Contingency Planning to encourage (or threaten) individuals or sections in a company to report information security incidents.

Self-regulation in Taiwan uses strength and power instead of punishment. The government's aim of setting up ISACs within all industries involved in critical infrastructure through the Measures on National Information and Communication Security Incident Reporting and Responses was initially thwarted when it realized that it could not force enterprises to report incidents. Therefore, incentives and rewards were used instead to encourage enterprises to join the information-sharing scheme.

The Self-Regulation Treaty for Members of the Bankers Association of the Republic of China also uses rewards and commendation to encourage banks to act in the public interest and to demonstrate corporate responsibility. In this case, the strengths-based pyramid was probably used, instead of the regulatory enforcement pyramid.

Enforcement-3 vs. Strength-3

The voluntary reporting to CERTs by enterprises or individuals may be seen as a good example of Strength-3. There is no punishment if an enterprise fails to report to a CERT if they are not required by law and regulation to do so. On the other hand, if they do report an incident, they may get support from the CERT in solving the problem.

We can also predict potential Enforcement-3 power. Recalling the examples of informal information sharing among trusted groups, such as good friends or friends within the same industry, we can imagine that a

[56]Ibid., 398.

"free-loader," someone who only wants to receive information but is unwilling to supply it, might be expelled from the trusted group. This would be an example of the use of Enforcement-3 power to regulate people within a trusted group.

Conclusion

This paper examines how regulations are used to govern or facilitate the reporting of information security incidents in Taiwan and China. It proposes a new expanded model of regulatory enforcement and the strengths-based pyramid. By examining regulatory responses to the reporting of information security incidents, the study shows how this expanded model can be used to explain regulatory behavior. It will be interesting to see how this expanded framework is used in the regulation of other institutional behaviors to which it is applicable. Some research has already been done in Australia on tax compliance and aged care provision using these pyramids. However, little research has been carried out into how plural regulations might be used for regulating different institutional behaviors in the greater China area. Therefore, further research of this kind could also focus on these other areas, for example, the framework used to regulate removals companies.

Both regulatory enforcement and strengths-based methods are used to encourage the reporting of information security incidents. Regulators use a "carrot and stick" approach. On the one hand, regulators try to force businesses and government agencies to report incidents by punishing them when they fail to report; on the other hand, they try to give the reporters support by showing them how to develop resilience and waiving potential administrative sanctions. In addition to the system of government regulation, there are mechanisms for reporting information security incidents within industries and among individual employees. Based on trust and pressure from other companies or institutions in the same industry or personnel in other companies/institutions, these mechanisms support the strengths and enforcement regulations which facilitate information ex-

change and reporting within the industry.

To sum up, plural regulatory mechanisms are used by China and Taiwan to promote the reporting of information security incidents. However, as such incidents are sometimes very sensitive, some entities prefer not to report them as the publicity involved may cause them more harm than any potential punishment. This clearly impedes the efficacy of the expanded model. Thus, future research might examine the factors that influence the decision whether or not to report. Additionally, an evaluation of the reasonableness and effectiveness of these regulatory mechanisms and an examination of which regulatory mechanisms are favored by those that they regulate are also important. Only by determining the main concerns of agencies that report information security incidents will we be able to encourage more institutions to report.

BIBLIOGRAPHY

Ayres, Ian, and John Braithwaite. 1992. *Responsive Regulation: Transcending the Deregulation Debate*. Oxford: Oxford University Press.

BBC News. 2010. "Microsoft Admits Explorer Used in Google China Hack." *BBC News*, January 15. http://news.bbc.co.uk/2/hi/technology/8460819.stm (accessed January 18, 2010).

Braithwaite, John. 2002. "Reward and Regulation." *Journal of Law and Society* 29, no. 1 (March): 12-26.

_____, Toni Makkai, and Valerie Braithwaite. 2007. *Regulating Aged Care: Ritualism and the New Pyramid*. Cheltenham: Edward Elgar.

Braithwaite, Valerie. 2007. "Responsive Regulation and Taxation: Introduction." *Law and Policy* 29, no. 1 (January): 3-10.

Brenner, Susan W. 2004. "Distributed Security: A New Model of Law Enforcement." *Journal of International Law* 8, no. 5:7-25.

Capeller, Wanda. 2001. "Not Such Neat Net: Some Comments on Virtual Criminality." *Social and Legal Studies* 10, no. 2 (June): 229-42.

Chang, Kai-fu (**張凱富**). 2006. "32 jia qiye qianshu zilü gongyue, huaqing yu eyi ruanjian jiexian" (32**家企業簽署自律公約, 劃清與惡意軟件界線**, 32 com-

panies signed the self-regulation against malicious software). *CBI News*, December 29. http://www.cbinews.com/university/showcontent.jsp?articleid=48377.

Chang, Yao Chung (**張耀中**). 2009. "Weiji shi fanzui yufang: cong richang shenghuo lilun tan wanglu fanzui yufang moshi" (**維基式犯罪預防：從日常生活理論談網路犯罪預防模式**, 'Wiki' crime prevention: what routine activity theory teaches us about cybercrime prevention). *Fanzuixue qikan* (**犯罪學期刊**, Journal of Criminology) (Jiayi) 12, no. 2 (December): 87-116.

_____, and Joanne Wu (**吳兆琰**). 2008. "Cong Meiguo shiwu jingyan lun woguo de zi'an shijian tongbao yu zixun fenxiang jizhi" (**從美國實務經驗論我國的資安事件通報與資訊分享機制**, Study on information security incidents reporting and information sharing mechanism in Taiwan—From the perspective of the U.S. experience). *Keji falü touxi* (**科技法律透析**, Science and Technology Law Review) (Taipei) 20, no. 8 (August): 39-61.

Collins, Randall. 1979. *The Credential Society: A Historical Sociology of Education and Stratification*. New York: Academic Press.

DiMaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48, no. 2 (April): 147-60.

Ericson, Richard V. 2007. *Crime in an Insecure World*. Cambridge: Polity Press.

Grabosky, Peter. 1995. "Regulation by Reward: On the Use of Incentives as Regulatory Instruments." *Law and Policy* 17, no. 3 (July): 257-82.

Gunningham, Neil, and Peter Grabosky. 1998. *Smart Regulation: Designing Environmental Policy*. Oxford: Oxford University Press.

Gunningham, Neil, and Darren Sinclair. 1999. "Integrative Regulation: A Principle-Based Approach to Environmental Policy." *Law & Social Inquiry* 24, no. 4 (Autumn): 853-96.

Hannan, Michael T., and John Freeman. 1977. "The Population Ecology of Organizations." *American Journal of Sociology* 82, no. 5 (March): 929-64.

Hirsch, Paul M. 1997. "Sociology without Social Structure: Neoinstitutional Theory Meets Brave New World." *American Journal of Sociology* 102, no. 6 (May): 1702-23.

Hoffman, Andrew J. 1999. "Institutional Evolution and Change: Environmentalism and the U.S. Chemical Industry." *Academy of Management Journal* 42, no. 4 (August): 351-71.

Larson, Magali Sarfatti. 1977. *The Rise of Professionalism: A Sociological Analysis*. Berkeley, Calif.: University of California Press.

Parker, Christine. 2002. *The Open Corporation: Effective Self-Regulation and Democracy*. Cambridge: Cambridge University Press.

Rees, Joseph V. 1988. *Reforming the Workplace: A Study of Self-regulation in Occupational Health and Safety*. Philadelphia, Penn.: University of Pennsylvania Press.

Scott, W. Richard. 2008. *Institutions and Organizations: Ideas and Interests*, 3 ed. London: Sage.

Tapscott, Don, and Anthony D. Williams. 2007. *Wikinomics: How Mass Collaboration Changes Everything*. London: Atlantic Books.

Wall, David S. 2008/2010. "Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime (revised May 2010)". *Information, Communication & Society* 11, no. 6 (July): 861-84.

Zucker, L. G. 1983. "Organizations as Institutions." In *Research in the Sociology of Organizations*, edited by Samuel B. Bacharach, 1-47. Greenwich, Conn.: JAI Press.