Ivano Bongiovanni Follow
InfoSec, Risk Management & Policy in the Digital Age_Fellow @ University of Glasgow & Digital Fellow @QUT PwC Chair in Digital Economy_Views are my own
Dec 10, 2017 · 9 min read

The dilemma of research in cybersecurity management

What does cybersecurity have to do with 'A Beautiful Mind'?

I have recently attended one of the most eminent management conferences in the world. In these international events, thousands of academics, professionals, experts and curious people gather to share their current research, illustrate their latest advancements, spread their cutting-edge ideas or simply look for connections and some good food in an interesting new city. I played my part in the conference's industrious beehive and I presented a paper of mine. But really, I wasn't there for that. I was looking to gain some insights on my current focus area, the **management of cybersecurity in modern organisations.**

Let's get this straight: Information Security (IS) is *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."* Cybersecurity (CS) is *"The ability to protect or defend the use of cyberspace from cyber attacks."* (NIST, 2013, p. 94 and p. 58). Practically speaking, the former also includes physical information security threats (e.g. an outsider

physically intruding an organisation to steal data), while the latter focuses on threats to, and from, the cyberspace. Now that the house is in order, back to my conference.

Around 3,500 academic papers were presented at the conference. The overall quality was very good, with interesting, solid pieces of management research showcased. Now, how many of those papers were on CS? One hundred? Fifty?

> ***Two. 2. About 0.06%.***

Although not providing a definitive conclusion on the interest, mass and quality of current research in CS, this number seems to strengthen a matter of fact: there is not enough research in CS management. Let's try to unpack this.

A matter of perspective?

Why a global management conference does not host a relevant quantity of research in CS? I have two connected answers to this:

A: CS does not belong to management. *So what does it belong to*?

B: There is simply not enough research on CS management.

Let's sort out the first one, by looking at the four perspectives under which CS is mainly considered in current research.

1. Typically, CS is investigated by researchers in **information systems** because it is traditionally thought to be a *technical issue*. Did you get hacked? Well, probably your company didn't have the right firewalls in place. Or your *Intrusion Detection System* (IDS) didn't pick up the latest malware that hit your network. The technical aspects of CS mainly refer to understanding the technical dynamics of cyber-threats and designing appropriate mitigation tools (for example cryptography and Supervisory Control and Data Acquisition).

2. CS is also quite well explored from a **legal perspective**, focusing on the concept of cyber-crime and exploring its implications in terms of both offenders' behaviours and repercussions on victims. Cyber-crime (which clearly differs from CS, as it has been brilliantly pointed out in this article) is mainly investigated utilising methodological tools from psychology, criminology and sociology.

3. Associated with the previous, **behavioral sciences** are investigating what factors drive people's decisions when they face potential cyber-threats (for instance, spear phishing). These studies operate a sort of reverse social engineering and unpack the reasons why, based on phenomena such as, for example, *channel factors* and *habituation,* employees may systematically ignore software update warnings or download potentially malicious email attachments (check this short story out to know more about this).

4. Finally, in the current, post-Cold War, international environment, characterised by highly asymmetric distribution of power, another *nuance* of CS that is attracting increasing attention is the concept of cyber-warfare. This relatively new perspective, explored in the **international relations** domain, aims at understanding how international security can move to a digital environment and play its 'balance of power' with completely digitised weapons.

And CS management? Well, there is not much in this space. Yet, a plethora of elements naturally create a *raison d'etre* for exploring CS as a managerial issue:

- The importance of human factors in CS;
- The long-term, strategic impact on the business that cyber-attacks can have (for example, in terms of reputation);
- The need for companies to get their *cyber-crisis communication* right (Uber provided the latest example);
- The budget limitations that some companies impose on CS, sometimes considered *another entry in the risk register.*

The table below provides an illustration of the aforementioned CS disciplines, with sample research questions and focus areas.

	CYBERSECURITY				
Discipline	**Information Systems**	**Criminology/Psychology**	**Behavioural Economics**	**International Relations**	**Management**
Main focus	Technical cybersecurity	Cyber-crime	Online behaviours	Cyber-warfare	Cybersecurity Management
Sample research question	*What cyber-defenses best protect critical infrastructures from cyber-threats?*	*What types of rewards do hackers seek?*	*Why some employees put in place unsafe behaviours when using corporate IT?*	*What countries actively support groups of hackers?*	*Will cybersecurity become a strategic organisational function?*
Examples	SCADA	Fraud	Complacency	Cyber-terrorism	Cyber-risk assessment
	Cryptography	Financial crimes	Habituation	Hacktivism	Strategic cybersecurity
	Intrusion Detection Systems	Online predation	Present bias	Cyber-espionage	Cybersecurity governance

Cybersecurity disciplines with examples

So, we were saying '*there's not enough research in CS management*'. Why is this the case? We have outlined a couple of reasons so far, but let's now face another one: organisations do not like to share information about what they may not have done properly. And research in management is mainly about talking to companies and unpacking what they do. In my recent research, I have experienced instances in which questions about cyber-risks have raised barriers around commercial in confidence information.

Sharing is (not) caring: A cyber-prisoners' dilemma

The reason why companies generally don't want to share information about their CS (in the form of threat intelligence, best practices, track records of security breaches, etc.) relates to the previously mentioned reputational impact that companies fear so much. One of the resulting issues is that **research struggles to progress**, especially in the field of CS management, which largely depends on what organisations are keen to share. This sounds like another *information asymmetry* issue and, to further unpack '*why companies don't share*', I have applied some '**game theory 1.0**'.

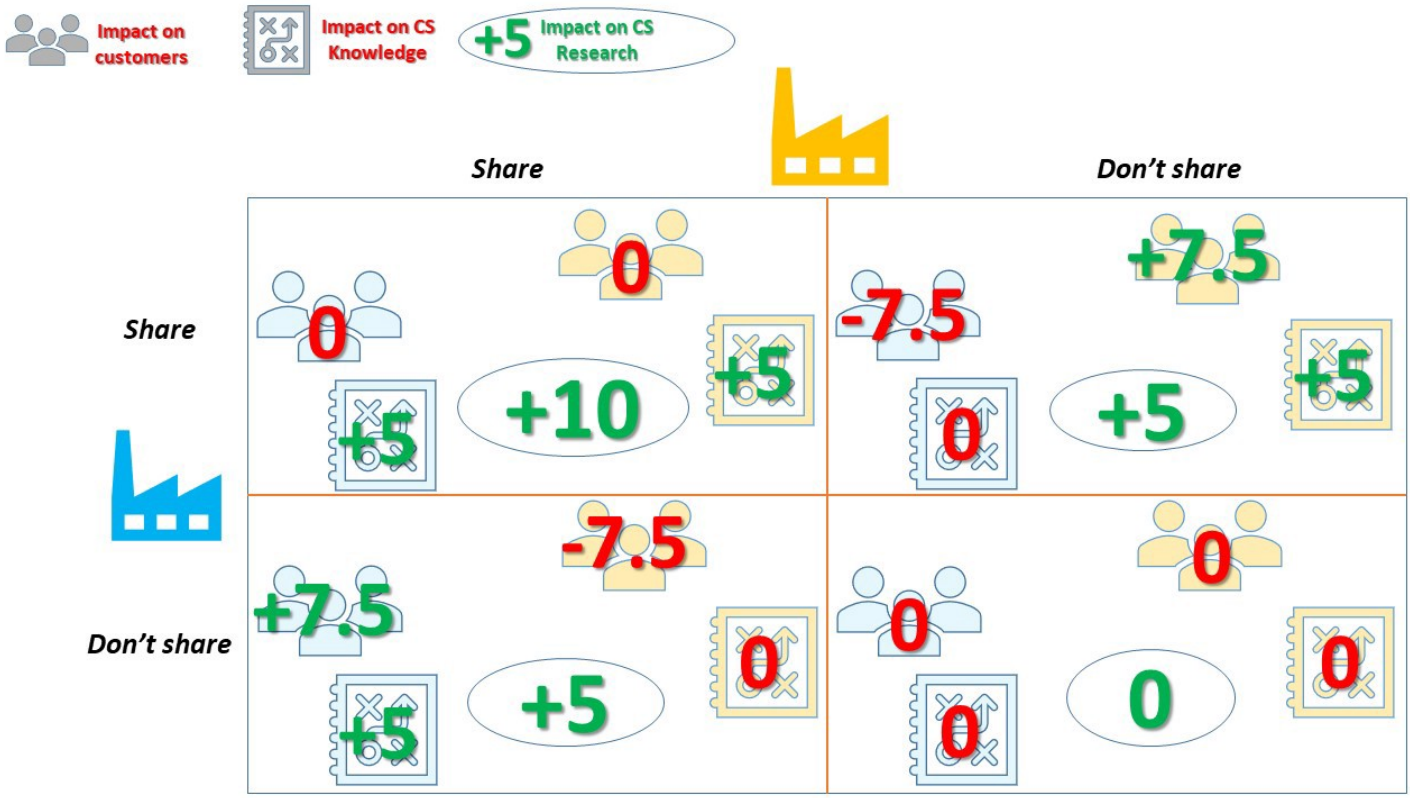
Imagine an economy in which, for simplicity, only two companies exist (A and B). These companies operate in the same market and are constantly trying to steal each other's customers. They are both very digital and concerned about CS. In this economy, the overall progress of research in CS depends on how much company A and B share about CS: the breaches they had in the past, their defences, their mitigation strategies, etc. The government is the champion of CS research, which constitutes one of the forms of *public good* that the government intends to pursue.

Now, imagine that both companies are attacked by a hacker who manages to steal their customers' personal details (identity, address, password, etc.). Each company now faces a dilemma: *do I share with the world that I have been hacked or do I keep it for myself?* The decision to share has two impacts: **on CS research and on customers**.

First, when both companies share, the government obtains the highest amount of CS information and CS research (as well as practice) is at its best. When one company shares, while the other one doesn't, the latter increases its knowledge on CS (by learning something from the other company), while the former's knowledge remains unchanged (they haven't learnt anything they did not know).

Second, sharing influences competition, as it alters the amount of customers of a company. Customers would likely *switch* to the competitor, if they knew that the company they have been loyal to has been hacked and their data are compromised. As a result, when one company shares and the other one doesn't, the latter is likely to attract some of the customers of the former. Conversely, when no company shares, or both companies share, the change in customers' balance is null.

The figure below illustrates this simple *prisoners' dilemma* applied to CS research, with **an exemplar quantification of the gains and losses obtained by each company in every situation**. In terms of CS knowledge, we hypothesise that sharing or not sharing produces either '0' (the competitor doesn't share) or '+5' (the competitor shares) in terms of CS knowledge. Negative values are not considered, as we assume knowledge cannot be lost. In terms of customers, sharing or not sharing produces '-7.5' (the company shares, but the competitor doesn't, so customers from the former are captured by the latter), '0' (both companies share or don't share, with no impact on customers), or '+7.5' (the company doesn't share, but the competitor does, so customers from the latter are captured by the former). Numbers are arbitrary, but the gain or loss in terms of customers (+ or -7.5) is higher than the gain or loss in terms of CS research (+ or - 5), to represent how companies are generally more worried about their sales than their CS. The sum of CS knowledge gained by the two companies determines the impact on general CS research (0; +5; or +10), which, it is worth repeating, is in the government's utmost interest.



A cyber-prisoners' dilemma

This ***cyber-prisoners' dilemma*** provides an illustration of the conflicting interests of private companies and the government (the champion of the public good, CS research). The two companies have a two-fold incentive in not disclosing information: they want to avoid losing customers and they want to possibly capture some of the competitors' ones (top-right and bottom-left quadrants in the figure above) This dramatically clashes with the interests of the government, which wants to avoid the bottom-right quadrant in the above matrix and pushes towards the top-left (where the most CS research is conducted). How can the government do so?

Australia's Notifiable Data Breaches Scheme

To *facilitate* collaboration in a naturally competitive environment, one of the government's sole weapons is to *enforce* it. Through compliance mechanisms, public and private organisations are pushed to conform to prescribed behaviours, or they risk hefty fines.

Australia is experiencing similar dynamics in CS, with the Notifiable Data Breaches Scheme (NDB) entering into force on the 22nd February 2018. The NDB basically obliges some public and private organisations to disclose instances of data breaches they suffered from. The NDB has two main, direct objectives. First, as a mitigation strategy, it aims at

improving the control that individuals have on their data, by allowing them to act (e.g. 're-secure' their online information) upon data breaches. Second, as a deterrent strategy, it intends to push organisations to strengthen their information security. The compliance mechanism behind the NDB includes fines up to $360,000 and $1.8 million for individuals and corporations, respectively, that fail to conform. Together with achieving its two primary goals, **the NDB can facilitate CS research, raise consumers' awareness around CS issues, and increase organisational accountability and transparency.**

Even before entering into force, the NDB has attracted significant debate in the CS community. I will not address such debate here, but I will try to sketch some of the implications that the Scheme could bring:

- Given the stronger emphasis that the NDB will likely bring on the reputational repercussions of CS, organisations will need to re-think their **CS as a potentially strategic component of their business** (e.g. as a competitive factor);
- Involved organisations will need to address their **cyber-crisis communication** capabilities and learn how to appropriately communicate breaches they have been affected by. Traditional crisis management can provide some interesting lessons on this;
- Smaller organisations, that don't necessarily have sufficient resources, will need to **explore collaborative options** to face the increasing impact that data breaches could potentially have on their business. Collaborative platforms such as AusCERT and CS start-ups can provide interesting solutions in this space.

When I speak to cyber-risk owners, the general perception I get is that the NDB is a positive, first step towards a more solid CS legislation, for Australia to 'catch-up' with countries (e.g. the US or the UK) that are more 'experienced' in this space. **From a research perspective, the NDB can be a promising instrument towards more information sharing**. Good news for my current research, which is exploring some of the aforementioned paradoxes of CS management, in order to understand the extent to which CS will be an operational or a strategic component of public and private organisations.

. . .

At the PwC Chair in Digital Economy at QUT, we are conducting research to understand the changing impact that cybersecurity will have on public and private organisations. In particular, we are talking to CIOs and CISOs to understand how strategic cybersecurity is likely to become in the immediate future.

Read more from the PwC Chair in Digital Economy team.