

The Mindset and Management for Mastering Financial Stability in the Cyber Frontier

by Karl Frederick Rauscher*

1. Introduction

Cyber security is rapidly emerging as a strategic priority for businesses, governments and consumers around the world, and with its central role in societies, the financial sector is front and center in this drama.¹ But is the concern justified? Are the dangers real? Is the attention of time and resources necessary? Is the financial sector prepared to face whatever trouble is in store?

There are even deeper core issues for central banks: What are the supervisory and regulatory roles in this new frontier? How can supervisory and regulatory authorities control risk without inhibiting innovation? As the public trust in financial systems must be maintained while they undergo the digital revolution, can central banks avoid playing a leadership role?

The Asia-Pacific region is a major force in cyber matters, being a prolific supplier of Information and Communication Technology (ICT), the host of the world's largest netizen populations, and an increasingly important voice on international cyber security policy.² Thus cyber security matters are not foreign, but on the contrary, an indigenous subject for the region.

After establishing the need for central bank due diligence and leadership in regard to cyber security, this paper provides an introduction to key concepts that position strategies for mastery based on the right mindset and management approaches.

2. Background

The emerging electronic world offers a plethora of innovation and the chance to do things that prior generations only dreamed of. But aside from dreams, ICT's tangible impact is clear, evidenced by its high correlation with economic benefits for societies. The Internet is both a major component of Gross Domestic Product (GDP) for over 70 percent of global GDP and a major factor in GDP growth.³ The desires for e-government, e-commerce and e-banking are surging forward. The momentum for technology uptake has no end in sight. Yet inherent in this new environment are brand new hazards for stewards of civilization. We have welcomed relatively unfamiliar elements into our most intimate dealings. Artificial intelligence, pervasive connectivity and instantaneous transmissions are now part of our front and back offices, part of our peripheral and core operations and part of our public and most restricted communications. A downside of the use of these powerful means has been a rapid rise of e-theft, e-crime and e-fraud (see Insert A, page 38).

This paper submits that the financial sector, and in particular, its leading institutions such as central banks, must step up to face what are very real dangers of

reliance on ICT to financial stability. After establishing the need for due diligence for cyber security, the paper introduces the key elements of a mindset for mastering cyber security. Next, the current approaches are explored and contrasted with the key elements of a management system that is likewise designed for mastery. Finally, practical next steps are offered to build confidence in taking the first hard steps toward improving a cyber security mindset and management system, no matter where on the maturity curve an institution or economy may be. While this paper is not a vehicle for prescribing specific regulations, it does provide key characteristics of supervisory and regulatory approaches that will be most effective.

The following discussion does not repeat readily available, general information about cyber security. Rather it advances the discussion to those few defining issues that will ultimately determine excellence in managing financial stability. It is worth noting upfront that the guidance offered here challenges the mindset and management status quo of practitioners of even the most developed economies by identifying defects in common perspectives and practices. Thus this paper submits that the cyber frontier is indeed dangerous and concerns are justified, however it offers a new approach and higher benchmark for effective resource utilization.

3. Importance of Cyber Security Due Diligence

The financial sector is undergoing a profound electronic transformation. Even with this dramatic change, banking customers rely on financial institutions to protect their assets. This is inherent in the banker-customer relationship. The challenge to maintain that trust is higher than ever before, as a brief reflection on history portrays.

The path that economies have traversed from bartering with goods and services, to precious metals, to a self-defined currency, has now arrived at essentially *invisible* stored information as the means of transaction and record keeping. As it has been travelled in history, this course has required evermore trust along the way. The value of a lamb or day's labor was tangible to the buyer and seller in ways that precious metal was not, yet the convenience and portability of this innovation were a trade-off that history welcomed.⁴ The subsequent transition to a paper currency was a larger leap of trust; indeed some are still not comfortable with it. Yet this innovation similarly introduced multifarious benefits as its worldwide adoption gives evidence. Like the previous transformations, the present one ushers in a wide range of benefits that enable economies to thrive like never before. Farmers in remote villages struggling in underdeveloped economies use mobile smart phones to check true market value of chickens they bring to market; investors issue voice commands via their equally smart phones to buy and sell stock as they multitask; deal-clinching handshakes and smiles are facilitated by confirming real-time account transfers a half a world away; and central banks settle lifeline transactions with private institutions each day via computers, databases and software controlled algorithms. For each of these and the other countless scenarios, are numerous modes of failure that can devastate the trust of users: the market quote can be hacked and falsely presented, the trading platform can be manipulated with a bias,

an account could be compromised and liquidated and settlement systems can crash. While there are many participants in the sector that must contribute to securing ICT infrastructure, above all, due diligence by central banks in ***preserving trust in the invisible electronic currency at the core*** of the financial system is vital to financial stability.

The operations of banks and other regulated financial services providers have intense reliance on electronic data. Their investments in ICT are nontrivial as high quality data management and data analytics are critical prerequisites to prudent risk management and strategic and tactical decision-making. Banks' competencies in protecting the integrity of their information technology control environment and customer data security are critical to avoiding serious financial loss or reputational damage. Due diligence in preserving financial stability cannot be accomplished without due diligence in cyber security matters. The simple truth is that modern ***banking is inseparable from ICT***. Accounting, transactions, trading, investments, interest calculations, lending, deposits, withdrawals, payments, clearing, settlements ... are all accomplished electronically. The requirement is *not* a diligence that can be delegated to "the IT room". On the contrary, board rooms must step up to increased awareness and responsibility for the stability, security, reliability, resilience and robustness of what is now the core fabric of their operations. As the author heard one Indian bank Chief Operating Officer (COO) observed, "we are really an IT company wearing the skin of a bank."

The Bank for International Settlement (BIS) Basel Committee on Banking Supervision introduced operational risk as an element of the first of its "Three Pillars" of sound banking practice. The Basel II Accord defines *operational risk* as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."⁵ In modern banking, "processes" are largely performed via electronic means. Likewise, "people" perform their various functions in a banking environment via electronic means. Even the banking "systems" are implemented by electronic means.

The inescapable conclusion is that due diligence in ***cyber security is central to operational risk management***. Furthermore, "external events" can have a direct or indirect impact on financial stability via ICT. Examples of the financial sector being shocked by external events include the 2006 and 2009 severing of undersea cables in the Luzon Strait and the 2001 9-11 terrorist attack on New York City.

The due diligence of ***central banks can have a positive influence*** as they recognize and respond to cyber security issues, i.e. to their respective spheres of influence: private banks and other financial institutions.⁶ This influence follows from the general stature of the central banks as being the *conscience* of financial stability and thus an assumed role model, as well as from the unique functions of lender of last resort, supervisor and regulator, the exact combination of which depend on a given institution. Thus cyber security is a vital consideration for the three core objectives of central banking: monetary stability, financial stability and, safe, secure

and efficient payment and settlement systems. Payment and settlement systems rely on a flawless electronic transfer to ensure smooth functioning. Conversely, negligence in this area can have a negative impact and influence. As prioritized by the G20, the 2007-08 Global Financial Crisis (GFC) reform agendas of international regulatory standard-setters for the financial services industry have been primarily focused on more fundamental financial stability and prudential matters, such as the Basel III capital and liquidity standards. This prioritization has led to deferral of international policymakers' consideration of other important regulatory policy issues such as cyber security. As will be shown below, there are major aspects of the status quo in supervisory approaches regarding operational risk that can be improved.

The current situation can be further summarized as one where the banks are not homogeneous, generally operating with good management practices, dealing with the risks they are aware of, and implementing common practices that have limited effectiveness.⁷ Furthermore, ICT oversight commonly involves stakeholders, procedures, accountability, and other mechanisms of sound risk management. However, as a whole, the situation demands a closer strategic involvement from their boards to make sure the proper organizational attention and oversight are being pursued. While there are many priorities for oversight, cyber security is one that deals directly with reputation, which in turn deals with public confidence. Any time there is a crisis situation, there are two effects: (i) the actual loss, if any; and (ii) the potential longer term impact of public confidence, which can be reflected in numerous ways (e.g., customer turnover, reduced stock price). With cyber security, a single event can take but an instant but have long lasting damages.

Thus cyber security due diligence is important for central banks because (i) public trust in electronic currency at the core of the financial system is essential, (ii) banking is inseparable from ICT, (iii) operational risk management requires it, and (iv) leading institutions can have a positive influence on the financial system. Banks that manage cyber security effectively will satisfy customers, fulfill regulatory expectations, avoid costs of excessive exploitations, protect brand reputation, and maintain a competitive advantage. Management expert Peter Drucker taught that "Management is doing things right; leadership is doing the right things."⁸ Now that we have established that cyber security due diligence is "doing the right thing", we next turn to "doing things right", first by considering the right mindset.

4. Mindset for Mastering Cyber Security

Having a right mindset is the first step in being prepared for managing cyber security. There are several key concepts, which if acknowledged at the onset, have a long-term benefit for managing cyber security effectively. These concepts, each of which is a corollary to a hazard to be cautioned against, are worth covering deliberately here because, though they may seem quite obvious, are actually commonly overlooked, or otherwise not perceived with much clarity. The landscape of internal and external ICT infrastructure that routine banking relies on is highly complex and continuously

evolving. These concepts are reference points to assist navigating that complexity and evolution. Once grasped these concepts can serve as a trusted touchstone when considering options for managing cyber security. Surprisingly, each of these concepts is often missed by practitioners in even the most developed institutions and economies; thus their value is useful throughout the full range of the cyber security management maturity curve.

4.1 A Mindset to Achieve Control

Classical quality control principles, which in the past century have transformed the productivity and quality across the complete spectrum of sectors around the developed world, have not yet been applied well to cyber security. One of the key principles of modern quality management is seeking and establishing controls that can accomplish performance improvements when needed.

Caution 1: Reactive Management Fosters Instability

We begin with a big picture of the major trend dynamics across the ICT landscape, namely, technology (T), technology adoption (A), criminal exploitation of technology (X) and management of technology risk (M). Management here refers to the development and implementation of policies and practices to ensure uncompromised assets and services. Figure 1 illustrates the relationship between these trends relative to each other and their respective rates of advancement over time.⁹ Amongst these four trends, there are six potential inter-relationships. The sequencing of these trends is as follows:

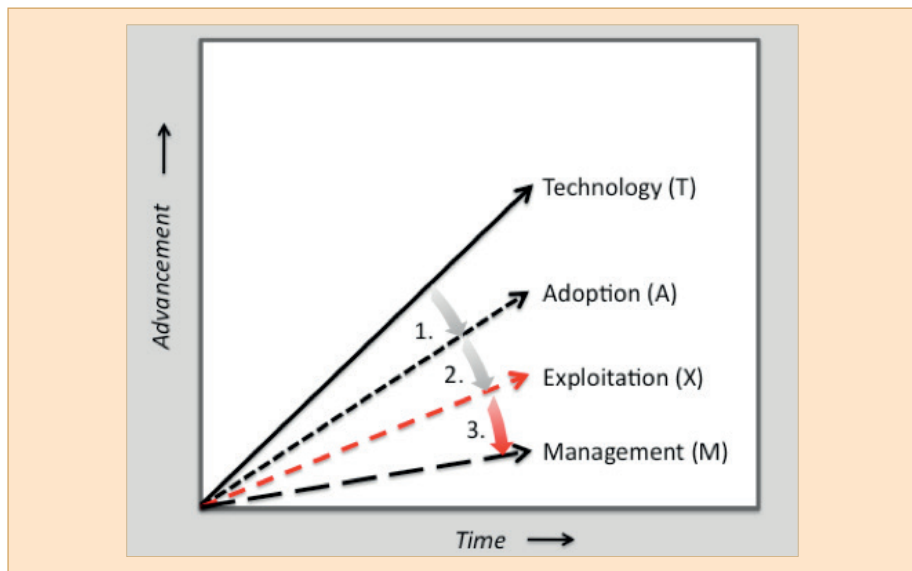
- | | |
|--|---------|
| 1. Technology drives technology adoption | [T → A] |
| 2. Technology adoption enables criminal exploitation | [A → X] |
| 3. Management responds to the criminal exploitation | [X → M] |

The third relationship is what is fundamentally problematic with the big picture. The reactive posture of key management activities enables cyber crime to thrive.¹⁰ The primary reason why management (M) is presently lagging and has the slowest rate should be obvious. The primary impetus for management (M) as routinely practiced in government and industry is the need to react to a problem, in this case criminal exploitation (X).

There are 3 major concerns with this orientation. First, it is costly, as reacting to a growing problem is rarely an efficient strategy. Second, it is unstable, because malicious actors are only making use of a subset of the full set of possible exploitations at any given point in time. The complement of remaining exploitations can at any time be discovered and exercised and further deteriorate the integrity of a financial system or institution. Third, it propagates a less desirable philosophy and balance of core competencies, both within an institution and amongst the external resources that are positioned to assist the institution. While rapid response skills will always be needed,

the preponderance of such when there are limited resources results in an undesirable trade-off that gives up more leveragable competencies such as proactively deployed science, technology, engineering and mathematics (STEM). Loading up on a reactive posture is *not* a winning mindset when the number of sources and the number of types of threats are growing faster than your own capabilities in an environment of pervasive global connectivity.

Figure 1. Dynamics of the ICT Infrastructure Landscape with Reactive Management



The first and second relationships cannot be altered, i.e., adopting technology requires it to exist, and exploiting technology requires it to be deployed. However, the third relationship can be turned. This opportunity is picked up next in the discussion and presented as the corollary to Caution 1, along with the remaining three inter-relationships, i.e. technology and management [T&M], technology and exploitation [T&X] and adoption and management [A&M]. These three relationships are neglected in the reactive management paradigm.

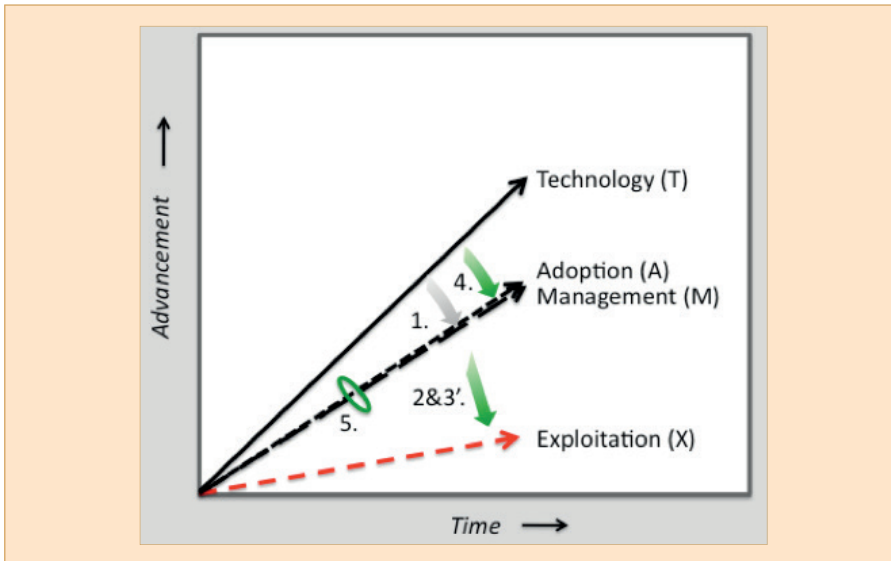
Concept 1: Coordinate Technology Adoption with Technology-Informed Management

In a mindset prepared for mastering cyber security, still at the forefront is the fact that technology (T) drives technology adoption (A). However, the following relationships are now significant (Figure 2):¹¹

- | | |
|--|---|
| 4. Management is informed of Technology | $[T \rightarrow M]$ |
| 5. Technology Adoption and Management Are Coordinated | $[A \leftrightarrow M]$ |
| 2&3'. Coordinated Technology Adoption and Management Impede Exploitation | $[(A \leftrightarrow M) \rightarrow X]$ |

The drive to achieve control positions management planning and resource application earlier in the technology deployment lifecycle. This is enhanced with intelligence regarding the technology.¹²

Figure 2. Dynamics of the ICT Infrastructure Landscape with Proactive Management



4.2 A Mindset that Acknowledges Strengths and Weaknesses

Since it is well established that the use of ICT in banking is not going away, there are some *unfriendly* trends from a cyber security management perspective, that must be lived with. Once we accept these hard realities, we can use their constraints to concentrate available rigor effectively in the solution space.

*Caution 2: Connectivity, Complexity and Criticality*¹³

The recent **connectivity** accomplished by the Internet thus far, though breathtaking, is not plateauing, but rather on the verge of an explosion far greater than what we have seen to date. The Internet Protocol Version 4 (IPv4) allows for approximately 4.3 billion unique addresses.¹⁴ This current address architecture provides approximately enough addresses for each person on the planet (~7 billion), but not enough. Responding to this address exhaustion, and anticipating the Internet of Things (IoT), IPv6 is now being deployed at various stages around the world. IPv6 provides an astronomical number of unique addresses (hundreds of undecillions); if there were one thousand more people on the planet, *each* could have *one trillion times one trillion* unique addresses on the Internet!¹⁵ Why so many addresses? Electrical engineers and other stewards of the Internet's future envision that anything deemed important will be networked: vehicles, appliances, cattle,

nanotechnology in bloodstreams, etc., thus is the future IoT. Each “thing” will thus potentially be connected to banks and other financial institutions, with the possibility for all sorts of creative billing and financing models, which leads us to the next foreboding trend.

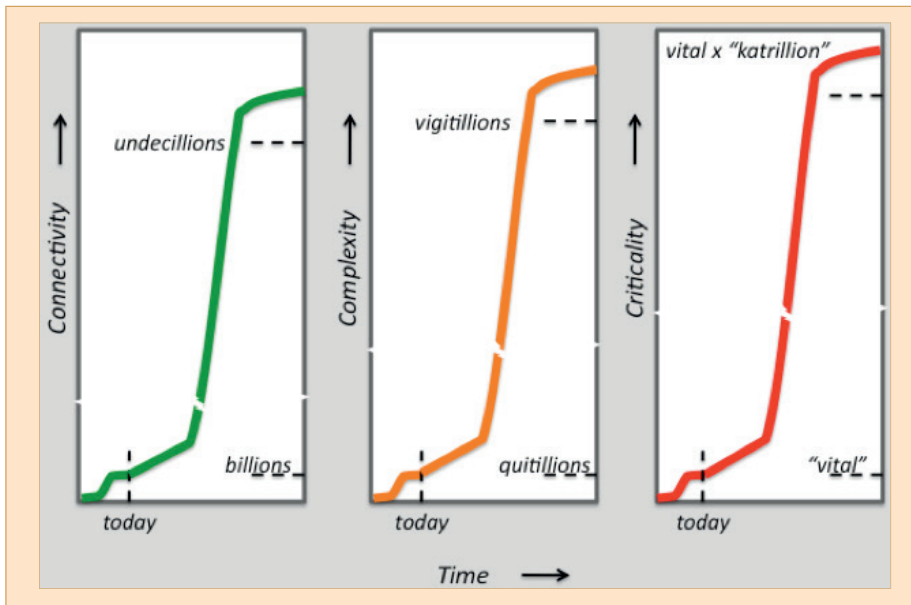
The **complexity** of the Internet is overwhelming. Presently, the number of potential interacting pairs of endpoints on the Internet with IPv4 is referred to as *quintillions* (a number with 18 zeros after it); this number grows to *trillions of vigintillions* (76 zeros after it) with IPv6.¹⁶ Moreover these numbers just represent the potential connecting entities – the complexity is still vastly greater as it will involve much anticipated elaborate interactions. So the explosion of connectivity, is even further “outnumbered” by the trend of complexity, which is further impelled by such features as open platform architectures that enable user-generated applications, reliance on artificial intelligence to make decisions from complex “big data” analysis, interactions among machines that are empowered to manage the background tasks of our lives (including finances) and new business models that integrate real-time information from sensors, inventories and market supply and demand like never before.¹⁷ Intelligent, networked technology will be a decisive enabler as competitive edges are defined by the ability to make decisions a split second faster than a competitor. Already, the new informed capabilities are being dubbed “smart grid”, “smart living”, “smart healthcare”, “smart weapon”, “smart government”, “smart banking”, etc. The advantages of “being smart” will increasingly drive reliance on advanced ICT for everything that is important, which leads us to the next disruptive trend.

In light of the above, consumers are poised to continue demanding convenient delivery channels for banking services that may introduce new material risk factors. Banks’ financial soundness depend on their ability to understand and manage such risks to maintain consumer confidence and a favorable reputation.

The supply chain for ICT is still another aspect of the complexity trend, as the software, systems and services relied upon are delivered by an intricate web of interdependencies that crisscross the globe.

There is coming a need for important things to be done faster, better and cheaper. Advanced ICT offers this. Thus the third unstoppable trend is for **criticality** to be ever increasing; i.e. ICT must to be more secure and more reliable because we are counting on it more today than yesterday.

Summing up the above, it is evident that the practice of cyber security due diligence will only become much harder as connectivity, complexity and criticality skyrocket. Given its central role, the banking industry cannot avoid the hard realities of these trends. Furthermore, there is no solution presently employed to counteract the difficulties presented by these trends (Figure 3).

Figure 3. Unstoppable Trends of Connectivity, Complexity and Criticality*Concept 2: Solution Space of the Asymmetric and Finite*

Given how there are unstoppable long-term trends making cyber security due diligence more difficult, and that there are no solutions being widely deployed to neutralize the challenges of any one of these trends, a calm mindset is needed that will be deliberate in identifying fulcrums on which to leverage an advantage. Economical solutions will need to be orthogonal to the massive dimensions described above, in order to avoid costs that also follow the explosive growth rates. Thus possible attributes of the solution space that can survive this harsh arena are those that can add significant value in ways that are asymmetrical to the overwhelming tsunami of connectivity and complexity underway. Viable paths forward will be those that find insights akin to scientific constants that are not tracing the exponential curves, but rather have a finite nature. Winning strategies will thus have a mindset that recognizes innovation leveraging the asymmetric and the finite.

4.3 A Mindset for Completeness and Accuracy

As one of the few areas with growing budgets, there are no lack of cyber security products and services on the market.¹⁸ In addition to the private sector, governments have likewise prioritized cyber security as an issue to be addressed, putting forth high level policy statements and initiatives, which often cite the importance of the issue for national economic interests.¹⁹ Meanwhile, the financial sector has several initiatives underway that include guidance for cyber security assessments or other checklists and best practices. One notable example is Canada's Office of the Superintendent of Financial Institutions 2013 publication of a cyber security self-assessment.²⁰ Delving

into all of these outputs, one gets the sense that the efforts are at a relatively early stage, coming short of mastery. The language and descriptions lack the earmarks of performance benchmarks and expectations for certain control of the situation when investments of resources are made. As an aggregate, these outputs also both reflect a high respect for cyberspace as a medium and convey a sense of mystery as to its nature, combining to reveal a lack of confidence that completeness and accuracy can be achieved.

Caution 3: Abstractions Are Deceptive

In technology, as in other fields like economics, it is often beneficial to make use of simplifications of a complex subject in order to convey a particular point. In this regard, analogy, patterns, and models are useful in enabling efficient knowledge transfer. There are many instances in the practice of cyber security where abstractions are utilized. These include protocol standards that define the acceptable inventory for given fields, threat modeling that anticipate the interests of a hacker, or statistical risk analyses based on historic events, to name a few. These abstractions are often very useful, and even necessary at times. However, a miscalculation is made when the abstraction is believed to be the same as reality. The basic limitation with nearly all abstractions is that they are at best a shadow of reality, and at worse, they can convey inaccurate aspects of reality.

Variations from Plan Are Inevitable

One common misfortune is when one relies upon an abstraction that is based on how things are *supposed* to work (e.g., a protocol specification). In other words, things may work perfectly on paper and according to plan, but what is happening on paper is not what is happening “on the ground.” History is ripe with such examples of a failure to adequately anticipate variance. One example that lies at the roots of modern cyber security is the German Enigma machine, which enabled secure communications in World War II. The Germans were convinced that the Enigma’s advanced encryption was uncrackable. No one would have the time or mathematical ability to work through all possible combinations that it could generate when coding a message. The way it was *supposed* to work per plan, maybe so. However, operators of the typewriter-like boxes did not always follow procedures, being either forgetful or lazy. This variance, when combined with another oversight, led to the big break for hacking into the Enigma. The other insight came to Allied code breakers when they recognized that daily weather forecast broadcasts from German U-boats in the North Atlantic followed a consistent format. The variation of actual from intended use led to a compromise of the security of Germany’s most sensitive communications. In this case, the failure had a positive benefit of bringing an earlier end to the war.

Historic Analogies Are Limited

A second common shortcoming of abstractions is that they can be overly reliant on experience. Experience being so valuable, it must not be discounted. However,

the caution here is to *not inflate* its value, such that it is esteemed as being a sufficient intellectual basis for preparedness for the future. The common disclosure made to personal investors comes to mind: “past performance is not indicative of future performance.” This axiom applies well to cyber security, as there are new permutations of attacks, literally, every day. Though not a cyber-related example, given that its features have been so studied, it is worth considering here a more recent example from history: the September 11, 2001 terrorist attacks on New York City. Prior to these attacks, expressed concerns about unsecured cockpit doors did not resonate with the model for evaluating risk. Why? The threat model for airplane hijacking prior to 9-11 did not account for the latent vulnerability of cockpit door access and a willingness of hijackers to sacrifice their lives for the mission. No one had tried this before, so the threat model missed it. The threat-oriented perspective dominates much of the cyber security industry. There are countless companies that provide ever-faster capabilities to learn about the latest threats and incrementally react better to them. It is very important for a cyber security strategy to make use of such experience and historic knowledge, but it is not enough because it can be assumed that there are always latent failure modes, as Concept 3 will further assert below.

Extensions Beyond Usefulness Cause Error

A third problem with abstractions is that they can just plain convey a fallacious notion. This is probably seldom the intent, but rather a collateral or derivative effect. A present day example is the popular term “cloud”, which refers to distributed processing and data storage across networks that can span a region or even the world. Since the mid-1980s network engineers drew cartoonish clouds on whiteboards when they were in a situation where they did not want to elaborate on the details of a network, but rather wanted the focus of attention to the systems or devices on the network peripheral. It was convenient; in this context no harm was done. However, the use of a cloud for simplification has turned the term into a buzz word of ICT market-wide (i.e. worldwide) proportions!

A few years ago while attending a major international cyber security conference in Beijing, the author heard the Chief Technology Officer (CTO) of a popular Internet company make a 30-minute presentation on “the cloud” that was based on the principles of different types of real clouds (e.g., cirrus, stratus, cumulonimbus). It was interesting, but had no basis in reality. Distributed computing and processing is *not* a cloud, *nor like* a cloud. Other than the initial simplification on the whiteboard, the parallels are not beneficial. The concern is not based on a single speech; sadly, but far from it. Far too few stakeholders, whether they are individual customers or the managers of large financial institutions, really understand what is happening when they rely upon a “cloud” service. A Silicon Valley-based survey found there is gross ignorance about what the so-called cloud is, even in the most developed societies, and even amongst those that are using “cloud-based” services for banking.²¹ Given the priority of maintaining trust for financial stability, vast gaps in understanding like this are a public relations crisis waiting to happen. Due diligence, at least in the financial services sector, should not allow conversations to remain at the “cloud” level. Banks need insights into the inside of

these clouds, assurance of diverse physical routes, geographically-acceptable data storage locations, access control practices, redundancy, etc.

In review of the above, abstractions have useful function but at some point must be seen as a crutch to be abandoned. Understanding these limits is crucial to avoiding major oversights that, if exploited, could lead to compromise of financial ICT systems or services. When the stakes are high, as they are for the financial stability of an economy, operational risk management should be based on the tightest possible understanding of reality, even if new training and extensive rigor are required.

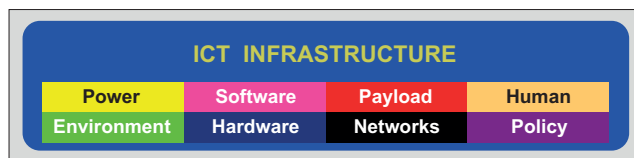
Concept 3: Reality-based Framework is Essential

The need for a sound and effective framework is introduced in the Basel “Core Principles for Effective Banking Supervision”, which articulates an Operational Risk, Principle 25, as follows:

“The supervisor determines that banks have an adequate operational risk management framework that takes into account their risk appetite, risk profile and market and macroeconomic conditions. This includes prudent policies and processes to identify, assess, evaluate, monitor, report and control or mitigate operational risk on a timely basis.”²²

Working from a foundation tightly coupled with reality is essential, making it possible to most effectively “identify, assess, evaluate, monitor, report and control or mitigate” cyber security risk. But how can a leader of financial institutions, whose primary expertise is not science, engineering or technology, accommodate such a need? How can this be practically achieved on a broad scale?

This concept does require a commitment by the most affected to learn new things; this is unavoidable. The key is that asymmetric approaches for grasping the core set of principles are available, thus making the task practicable. One framework that has been proven to be both accurate as a reflection of reality and effective in supporting proactive management of cyber security is the Eight Ingredient (8i) Framework (Figure 4). Its basic assertion is that cyberspace, or ICT infrastructure, consists of eight ingredients: environment, power, hardware, software, network, payload, human and policy (or more completely: Agreements, Standards, Policies and Regulations –ASPR) (Insert B).²³ Any seven ingredients would be too few, and a ninth is not needed. The 8i Framework is crucial in that its ingredient approach is asymmetric to the big trends, meaning it does not change, despite the exploding numbers. The 8i Framework is also accurate relative to reality, meaning that it avoids the pitfalls of abstractions discussed above, by not overextending itself beyond its range of accuracy, remaining grounded in the simple reality that cyber space has a finite number of distinct ingredients. The 8i Framework also brings completeness with its constant eight ingredients, which hold not only for the previous century of electronic communications but also for the foreseeable future.²⁴

Figure 4. Eight Ingredient (8i) Framework










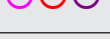
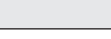
The more convinced a mindset is of the need for the strictest possible alignment with reality, the stronger it is positioned to master cyber security and avoid excessive risk. The next set of benefits that can be derived from this approach is that each of the eight ingredients has a finite set of intrinsic vulnerabilities.²⁵ This is significant because the only way that a threat can have a negative impact is to exercise one of the intrinsic vulnerabilities, of which there are on the order of one hundred, a very manageable quantity. The means by which the most common forms of cyber security threats do harm can be shown to be associated with one or more of the intrinsic vulnerabilities of the eight ingredients (Insert A). Furthermore, it could be stated that *all* systemic risk related to ICT is tied to one or more of the finite set of intrinsic vulnerabilities. The unwelcome news is that with cyberspace there are *new* risks for the financial sector originating from these intrinsic vulnerabilities. Further, none of these intrinsic vulnerabilities can be completely removed – they are always there. The good news is that there is a finite set of intrinsic vulnerabilities and thus the overwhelming complexity of cyberspace now has a handle from which we can get a firm grip.














Like other dimensions of risk management, ICT risk is often considered in a cost-benefit context. One of the implications of this consideration is the extent to which some functions may be outsourced. For example, a smaller bank may find developing the same internal capabilities as a large bank to be cost prohibitive. In light of this, central banks supervisory and regulatory measures should anticipate the need for flexibility in implementing the above concepts into due diligence strategies.













One unifying theme of this paper is that financial institution leaders must take more responsibility and accountability. Securing ICT systems and services is the business, the mission and the job of a financial institution in the modern world. Fortunately, there are cautions and key concepts that can serve a leader well in making rapid progress on the cyber security management curve.











Like other dimensions of risk management, ICT risk is often considered in a cost-benefit context. One of the implications of this consideration is the extent to which some functions may be outsourced. For example, a smaller bank may find developing the same internal capabilities as a large bank to be cost prohibitive. In light of this, the central bank's supervisory and regulatory measures should anticipate the need for flexibility in implementing the above concepts into due diligence strategies.

**Insert A. Examples of Cyber Security Threats Financial
Services Institutions Face**
(for their operations or for their customers' use of their services)

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Account Aggregation	Consolidation of multiple online financial accounts from banks, billers, brokerages, etc. providing a “one-stop” site (increases consequences of a compromise)	
ATP	Advanced persistent threats involve coordinating multiple methods of identifying and exploiting a target's vulnerabilities over an extended period to do harm	
Backdoor	A method of avoiding detection while bypassing normal authentication for accessing a system	
Bloatware	Accumulation of unused software programs that remain after de-installation and become a risk for exploitation	
Botnet	Collection of networked programs communicating with each other in order to perform tasks	
Browser Hijacking	Unauthorized modification or control of a web browser's settings	
Cryptoviral Extortion	The use of public-key encryption technology to encrypt a user's data and withhold the session key until a condition is met (e.g., payment)	
Data Breach	Unauthorized access to restricted-access data	
DDoS	A distributed denial of service attack makes use of the capacity limitation of an enterprise network ingress with extreme traffic loads	
Defacement	A hack on a website that changes its appearance or content	
Drive-by-Download	Software functionality that is loaded onto a user's device, without their knowledge intentionally	

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Hacking	Gaining access to an asset in cyberspace without the presumed required knowledge or official credentials	
Identity Theft	The use of another's identity in cyberspace	
Imposter Applications	An application placed in an app store that masquerades as a commercial application	
Insider Threat	A person inside an organization with access to ICT whose conflicting interests are poised to harm the organization	
Keyloggers	Recording the keystrokes of a device in a covert manner	
Kleptography	The practice of stealing information without being detected	
Malware	(Malicious software) software code that is intended to do harm	
MITM	Man-in-the-Middle is active eavesdropping where the unauthorized party is inserted between sender and receiver and can emulate traffic coming from either direction	
MITMO	Man-in-the-Mobile compromise allows unauthorized party to control a mobile device and communications (i.e. texting) to and from it without the user's knowledge	
Phishing	Use of electronic communications to masquerade with trusted identity to capture sensitive information	
Ransom-ware	Software that takes unauthorized control of a device, or some part of it (i.e. data), until a payment made, or some other condition is met	
Rogue Application	Software program that misleads end users to believe that it is a well-known or otherwise safe application	
Rooting	Gaining privileged control (root access) on an operating system	

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised
Rootkit	Software designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer	
Smishing	(SMS phishing) the use of mobile phone text messaging to trick user into providing sensitive information	
Sockpuppet	A false online identity	
Spam	electronic messages in any form that are widely distributed in high volume and are uninvited by the recipient; often the vehicle of malicious code	
Spoofing	An electronic communication with a forged sender address	
Spyware	Software that is running on a device unbeknownst to its user to gather information	
SQL Injection	A code injection technique where malicious Structured Query Language are populated into an entry field for execution	
Steganography	The practice of using hiding information within a larger profile of information, such as an image	
Trojan	Software that contains concealed functionality	
Virus	Software code that attaches itself to software programs, replicates itself and spreads to infect other files or programs	
Vishing	Use of voice communications to trick an individual to give up personal or financial information	
Worm	A standalone malware computer program that replicates itself in order to spread to other computers	

Threat	Description	Ingredients with Intrinsic Vulnerabilities Exercised	
Zero-Day	A threat that exploits a vulnerability in a software program prior its developers having a chance to implement a patch for the software	 	
Key to Ingredient whose Intrinsic Vulnerabilities are Exercised			
 Environment	 Software	 Payload	 Human
 Power	 Hardware	 Network	 ASPR

5. Management for Mastering Cyber Security

The previous section emphasized three areas of consideration for creating a mindset to master cyber security. This is the beginning of a journey, the departure point. There is of course much more that must be done. The discussion now briefly turns to additional strategic suggestions for managing with due diligence.

Senior Leadership

Financial stability is now vitally reliant upon due diligence throughout the ranks of financial institutions. Indeed the trustworthiness of the financial institution is inseparable from the trust in the integrity of the institution's computers, online services and electronic data. Thus, no less than the heart of financial stability, the public trust, is at stake when cyber security strategies are designed, cyber security policies are deployed and cyber security vigilance is pursued. Such criticality requires the most senior management of banks to be actively engaged in ensuring cyber security due diligence.

Best Practices

Best practices are a highly preferred method of knowledge transfer when dealing with fast advancing technology due to the speed with which they can be developed; i.e. relative to regulation and standards, which take much longer (Figures 1 and 2). A key to managing best practices development is to focus on addressing the intrinsic vulnerabilities, independent of specific threat knowledge. This concept may seem subtle when it is first read, but its effect when guiding a security strategy is profound. The tangible benefits are reduced cost, higher performance and a foundation for achieving control. Best practices strategies should include both countermeasures for preventing the exercise of an intrinsic vulnerability as well as ameliorate the impact should prevention fail.

Holistic Picture

All causes of harmful events need to be considered, without bias. It follows when focusing on intrinsic vulnerabilities, as opposed to threats, that the intent (or lack of an animated intent) is less relevant than the need to avoid a compromise. Operational risk should be objective, avoiding bias toward prioritizing malicious acts, relative to unintentional or natural disaster-caused events. However it is a seemingly universal preoccupation to pay much more attention to malicious acts relative to natural disasters.

“I am not angry - except perhaps for a moment before I come to my senses - with a man who trips me by accident; I am angry with a man who tries to trip me up even if he does not succeed. Yet the first has hurt me and the second has not.”²⁶

This is a common experience and demonstrates our preoccupation with malicious human threats in a way that is not related proportionally with risk or impact. To date, by far, most disruptions in service occurred from unintentional events.²⁷

Performance Measurement

It is most essential to measure what matters, not what is most convenient. This sometimes is in contrast to the common practice of measuring conformance to industry common practices. The ultimate evaluation of the effectiveness of a cyber security program should be based on the actual performance (i.e. counting actual compromises) relative to benchmarks.²⁸

Because actual events may (fortunately) still be rare events, their statistical frequency may be rare. It is therefore important that oversight boards not overreact to a single event based on its visibility, but rather make judgments based on a sound understanding of the statistical variability associated with such performance statistics.

Select Partners Wisely

With cyber security becoming a growing market, there are many companies eager to offer their products and services. Just an observation of the number of new companies emerging in the industry over such a short period of time makes the depth of expertise questionable across the aggregate. It is important to select partners who share a mindset to mastery, making it smaller, even though such a strategy is counter to the business interest of firms whose revenue generation is directly correlated with a thriving cyber security problem.

Developing Economies

Developing economies are of special concern as they are consistently targeted by malicious actors to be used to set up botnets and otherwise become the sources of attacks.²⁹

Developing economies should also be cautious of uncritically following the examples of developed economies with the assumption that their practices represent the soundest approaches. On the contrary, with their limited resources, developing economies must be strict in their disciplined use of existing resources, not having the luxury to lose money to strategies that are reactionary, overextending an abstraction or otherwise limited in effectiveness.

Regional Initiative

In cyberspace there are no national borders. With this in mind, it has been said, “we are all in this together” and “we are only as strong as our weakest link”. It thus follows that international cooperation can be quite beneficial to all involved. The benefits of such cooperation include increased awareness of trends, more effective best practices, coordination in solving cross-border issues, and other efficiencies related to progress on the maturity curve of mastering cyber security due diligence. A practical first step toward reaping these benefits is to begin with regional-level collaboration. With the overarching aim to improve the security of stability of ICT infrastructure in the Asia-Pacific region, central bank leaders are encouraged to consider both problems and solutions that they can bring to such a discussion and take advantage of opportunities to engage with their peers. The anticipated important output of such collaboration includes harmonious supervisory and regulatory policy frameworks with regards to cyber security due diligence, which does well to serve the public good and confidence in the stability of the region’s financial systems.

In summary, the banking community must answer the question “how should this cyber security challenge be met?” It is tempting to answer this question with a description of how the challenge *is currently* being met. But that is a different answer than how it *should* be met. Both responses have been explored throughout this paper. It is the general consensus by experts that the bad actors are winning up to this point.³⁰ There are ample demonstrations via frequent media reports of embarrassing breaches of financial records across a wide range of commercial entities. It is thus quite evident that the malicious actors who are on the offense have enjoyed the advantage despite all that is commonly deployed to date. It is time to turn the tables.

Insert B. Ingredients, Intrinsic Vulnerabilities & Events (Examples)

Ingredient	Description	Intrinsic Vulnerability*	Historic Event
Environment	Physical location of ingredients	Accessibility	Unauthorized device installed in Barclays internal network (2013) ³¹
Power	Electrical supply for hardware and environment	Loss of potential	Northern India power blackout precedes central bank cutting growth outlook by 11 percent (2012) ³²
Software	Programs providing functionality	Accessibility	U.S. Federal Reserve web site loses control of web site to hacktivists (2012) ³³
Hardware	Cables, semiconductor chips, electronics	Susceptibility to physical damage	Undersea cable cuts cause catastrophic shock Hong Kong financial systems (2006, 2009)
Payload	Information transported on infrastructure	Emulation	ANZ Bank in Vietnam is one of many banks whose customers received phishing emails (ongoing) ³⁴
Network	Configuration of nodes and their interconnection	Capacity limits	Targeted DDoS attacks on U.S. banks (2012-2013) ³⁵
Human	Involvement in entire ICT lifecycle	Cognitive – ability to be deceived	Fiji students open fake accounts with information obtained from social networking sites (2014) ³⁶
ASPR (Policy)	Inter-entity arrangements enabling behavior anticipation	Predictable behavior due to ASPR	A Man-in-the-Middle insertion enables unauthorized transfers from a Philippines bank account (2012) ³⁷

* In these examples there is often more than one intrinsic vulnerability exercised by the threat; e.g. the Payload example also involves the Human intrinsic vulnerability of cognition, i.e. being able to be deceived.

6. Conclusion

The previous pages reviewed compelling motivations for the financial services sector, and especially leading institutions like central banks, to be resolved in their commitment for cyber security due diligence. Reasons were established for why this effort is needed now, without delay. The limiting characteristics of current approaches were contrasted with the optimum approach in the context of a mindset and management for mastery. For a starting mindset, cautions and corresponding corollaries were offered for three areas, namely: a mindset for control, for discernment of strengths and weaknesses and for completeness and accuracy. How should we then proceed?

The biggest themes of this paper are that (a) we must accept the fact that cyber security is here to stay as a growing challenge, (b) the current methods are having insufficient results, (c) central banks play a central role in preserving financial stability for their sector and respective national economies, and (d) having a strategic mindset is vital to give commercial banks the best opportunity to convert their limited resources into the best results in a sustainable fashion.

Notice

In regard to the actions called for this article, leaders of central banks and other financial authorities of the Asia-Pacific region will convene to discuss regulatory expectations with respect to banking cyber security risk controls at the:

SEACEN Cyber Security Summit 2014
“Demystifying Cyber Risks: Evolving Regulatory Expectations”
25-26 August 2014

Sasana Kijang, Bank Negara Malaysia
 Kuala Lumpur, Malaysia

For more information, please contact: enquiries@seacen.org

Acknowledgement

The author expresses gratitude here to Stephen Malphrus (ret.) and Wayne Pacine of the U.S. Federal Reserve for their valuable insights through years of tutelage in previous collaborations.

-
- * **Karl Frederick Rauscher** is the first Ambassador & Chief Architect of Cyberspace Policy of the Institute of Electrical and Electronics Engineers (IEEE), and serves as a Commissioner of the G8-initiated Global Information Infrastructure Commission (GIIC), and is in an advisor to senior leaders, including for the financial services sector, on five continents. He has served as CTO and Distinguished Fellow of the EastWest Institute and has facilitated the development of over 1,000 world-class best practices for reliable and secure communications systems, networks and services. He is a lifetime Bell Labs Fellow, cited for achieving the first “6 9’s” (99.9999% availability) for a real-time network system, and has 50 patents/pending. In 2013, *The New York Times* editorial board cited his guidance for China-U.S. bilateral cybersecurity cooperation in *Fighting Spam to Build Trust* as recommended reading for President Obama and President Xi.

Endnotes

1. The global cyber security market is estimated at \$77 billion in 2013 and projected to grow to \$120 billion by 2017. "Cyber-Security Market (2012-2017)," marketsandmarkets.com, Retrieved: 31 March 2014.
2. China's Huawei is the largest communications equipment supplier in the world ("Who's afraid of Huawei?" *The Economist*, 3 August 2012, Retrieved: 3 August 2012). India is similarly one of the world's largest producers of software. China has the largest number of mobile phone users (1.3+ billion) and Internet users (600+ million); India has the second largest number of mobile phone users (1.1+ billion) and third largest number of Internet users (150+ million); other countries in the top 20 of either category include Bangladesh, Indonesia, Japan, Philippines, South Korea, Thailand and Vietnam.
3. Estimates of 3.4 percent of GDP, and 10 to 20 percent of growth, Per: Manyika, James and Roxburgh, Charles, (2011), "The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity," McKinsey Global Institute.
4. Bartering required a coincidence of wants.
5. Basel II: Revised international capital framework.
6. The term "central bank" used here and throughout to include alternative designations of "reserve bank" or "monetary authority."
7. Common practices include a focus on confidentiality, integrity and availability (CIA); applying a defense-in-depth strategy that involves layers (physical, network, operating system & application layers) of ICT systems; continuous monitoring and the use of automated tools (e.g., firewalls, intrusion prevention systems, anti-spam & anti-malware filtering); and an incident response team. More advanced organizations are also proactively engaged in cyber security collaboration with the critical infrastructure they rely upon (energy, communications, government, etc.) and periodic exercises.
8. Drucker, Peter F., (2003), "The Essential Drucker: The Best of Sixty Years of Peter Drucker's Essential Writings on Management," Collins Business.
9. The introduction of the relative comparison of advancement was first introduced in a presentation to the 2010 FIRST Technical Colloquium, Beijing, "The Rise of the 8th Ingredient- the Imperative of Addressing the International Policy Gap in Cyberspace."

10. While the author is very much aware that institutions have in place many proactive practices in their design and operation of ICT for security and reliability, the predominant posture across the financial and other critical sectors is one of reaction to the latest threats being presented.
11. Note that the sixth relationship, not discussed yet involves technology and exploitation (X). While malicious actors certainly have the opportunity to be earlier learners of emerging technology, and do make use of the opportunity, they do not have the controls of adoption and therefore this relationship [T&X] falls behind a coordinated adoption and management [A&M] capability.
12. The cost of perfect policy may not be desirable from a cost-benefit analysis, i.e. the cost of a minimal amount of loss due to criminal exploitation may be more tolerable than the price of achieving the ideal policy. The cost would include not only the direct expense associated with policy development but also the cost of delayed deployment of technology in a competitive environment.
13. The author credits Phil Reitingner with this alliteration for these three concepts.
14. $2^{32} = 4,294,967,296$ based on using a 32-bit (4-byte) address scheme.
15. $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$ based on using a 128-bit (16-byte) address scheme.
16. Using the formula: $[n(n-1)]/2$, for IPv4: $[2^{32}(2^{32}-1)]/2 \sim 9.2 \times 10^{18}$; for IPv6: $[2^{128}(2^{128}-1)]/2 \sim 5.8 \times 10^{76}$.
17. The number of apps for both the Android and Apple devices is on the order of magnitude of one million.
18. Billed as the world's largest annual cyber security conference, the RSA draws a growing number of suppliers of products and services. The RSA 2014 exhibit hall featured approximately 150 vendors appealing to tens of thousands of security practitioners.
19. Examples include the 2014 Chinese government announcement of a new Central Internet Security and Informatization Leading Group to be led by President Xi, the 2013 European Commission "Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity", the 2013 "U.S. President Executive Order - Improving Critical Infrastructure Cybersecurity"; India's 2013 proposed "National Cyber Security Policy."

20. Office of the Superintendent of Financial Institutions Canada, (2013), "Annex - Cyber Security Self-Assessment Guidance," The Financial Service Roundtable (FSR) is a U.S. private sector organization that provides information for its members (see www.bits.org/publications/home/BITSProjects.pdf), Retrieved: 31 March 2014.
21. Half of Americans (51 percent) believe that stormy weather interferes with cloud computing. When asked what "the cloud" is, a majority responded it's either an actual cloud (specifically a "fluffy white thing"), the sky or something related to the weather (29 percent). A majority of Americans (54 percent) claim to never use cloud computing. However, 95 percent of this group actually does use the cloud. Specifically, 65 percent bank online, 63 percent shop online, 58 percent use social networking sites such as Facebook or Twitter. Frank Packer and Haibin Zhu, (2012), "Most Americans Confused by Cloud Computing According to National Survey," Wakefield Research, August.
22. Basel Committee on Banking Supervision, (2012), "Core Principles for Effective Banking Supervision," Bank for International Settlement.
23. Rauscher, Karl. F., (2004), "Protecting Communications Infrastructure," Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2.
24. If a technology would be introduced that integrated an additional ingredient, it could be easily included in the framework.
25. Rauscher, Karl. F., (2004), "Protecting Communications Infrastructure," Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2.
26. Lewis, C.S., (1952), "Mere Christianity," Book 1 Right and Wrong as a Key to the Meaning of the Universe.
27. Network Reliability Steering Committee (NRSC) Annual Reports, www.atis.org.
28. Rauscher, Karl Frederick and Erin Nealy Cox, (2013), "Measuring the Cybersecurity Problem," EastWest Institute.
29. Examples of such targeting includes Africa, India, and Eastern Europe.
30. Menn Joseph, (2014), "Hackers Winning Security War: Executives," Reuters, San Francisco, 2 March.
31. Dixon, Hayley, (2013), "Barclays Hacking Attack Gang Stole £1.3 Million, Police Say," The Telegraph, London, 20 September.

32. Daniel, Frank Jack, (2012), "India Power Cut Hits Millions, Among World's Worst Outages," Reuters, New Delhi, 31 July.
33. Riley, Charles, (2013), "Hackers Access Federal Reserve Website, Data," CNNMoney, 7 February.
34. www.anz.com/vietnam/en/personal/ways-bank/internet-banking/protect-banking/internet-security-threats/, Retrieved: 2 April 2014.
35. Menn, Joseph, (2013), "Cyber Attacks Against Banks More Severe Than Most Realize," Reuters, 18 May.
36. "Two University Students in Fiji Charged for Laundering \$24,000 from Bank Accounts," Islands Business, 5 February 2014.
37. Agustin, Victor C., (2012), "Hacker Cans Up Dollar Account in Philippine Bank," 11 August.

References

- Aristotle, (350 B.C.), *Politics*, Greece.
- Basel Committee on Banking Supervision, (2012), “Core Principles for Effective Banking Supervision,” Bank for International Settlements.
- Basel Committee on Banking Supervision, (2011), “Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches,” Bank for International Settlements.
- Basel Committee on Banking Supervision, (2011), “Principles for the Sound Management of Operational Risk,” Bank for International Settlements.
- Council of Europe, (2001), Budapest Convention on Cybercrime, Strasbourg.
- Deering, S. and R. Hinden, (1998), RFC: 2460, Internet Protocol, Version 6 (IPv6) Specification, December.
- European Union, (2013), “Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity,” European Commission, Brussels, 7 February.
- Financial Stability Forum, (2009), FSF Principles for Cross-border Cooperation on Crisis Management.
- Graeber, David, (2011), *Debt: The First 5000 Years*, Melville House, New York City.
- Hasibuan, Zainal A., (2013), “Indonesia Cyber Security Strategy: Security and Sovereignty in Indonesia National Cyberspace,” National ICT Council.
- International Organisation of Securities Commissions (IOSCO), (2013), Principles for Financial Benchmarks.
- Information Sciences Institute, (1981), “RFC: 791, Internet Protocol Internet Program Protocol Specification,” University of Southern California, Marina del Rey, September.
- Juran, Joseph, (2010), *Quality Control Handbook*, 6th Edition, New York.
- Ministry of Communication and Information Technology of India, (2013), National Cyber Security Policy, Proposed 2 July 2013.
- Ministry of Information Communications and Culture of Malaysia, (2014), The National Cyber Security Policy, Available at: nitc.most.gov.my, 1 April.

- National Institute of Standards and Technology (U.S.), (2014), “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.0, February.
- OECD, (2012), Cybersecurity Policy Making at a Turning Point - Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.
- Office of the Superintendent of Financial Institutions Canada, (2013), Annex - Cyber Security Self-Assessment Guidance.
- Rapp, Ronald, J.; Franz-Stefan Gady; Sarabjeet Singh Parmar and Karl Frederick Rauscher, (2012), “India’s Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure,” *IDSA*, Volume 36, Issue 3, Commentaries: New Delhi.
- Rauscher, Karl Frederick and Yonglin ZHOU, (2011), “China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust,” *EWI and the Internet Society of China (ISC)*: New York City - Beijing.
- Rauscher, Karl Frederick and Yonglin ZHOU, (2013), “China-U.S. Track 2 Bilateral on Cybersecurity: Frank Communication and Sensible Cooperation to Stem Harmful Hacking,” *EWI and the Internet Society of China (ISC)*: New York City – Beijing.
- Rauscher, Karl. F., (2004), “Protecting Communications Infrastructure,” *Bell Labs Technical Journal Homeland Security Special Issue*, Volume 9, Number 2.
- Rauscher, Karl Frederick, (2010), “The Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report,” *IEEE*, New York City.
- Rauscher, Karl Frederick, (2010), “The Rise of the 8th Ingredient- the Imperative of Addressing the International Policy Gap in Cyberspace,” *FIRST Technical Colloquium*, Beijing.
- Rauscher, Karl Frederick and Erin Nealy Cox, (2013), *Measuring the Cybersecurity Problem*, East-West Institute.
- Spiotta, A. H., (2003), “Financial Account Aggregation: The Liability Perspective,” *Fordham Journal of Corporate and Financial Law*, Vol. 8(2), p. 557.
- The White House, (2013), U.S. President Executive Order - Improving Critical Infrastructure Cybersecurity, Washington, D.C., 12 February.