日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

"The IT Revolution and Security Challenges"

Tokyo

December 10-11, 2002

"Plugging the Floodgate"

by
Michael Yap
Chairman of the Board of Institute of Systems Science
(National University Singapore)
Chief Executive Officer, Commerce Exchange Pte Ltd.
Singapore

Plugging the Floodgate

Michael YAP

International Conference on The IT Revolution and Security Challenges

Institute for International Policy Studies, Tokyo

10-11 December ‘02

1. INTRODUCTION

The stability of the financial system is critical to the overall well being of the modern economy. The modern economy can be pushed into a corner by the failure of the financial system, a complex web of inter-dependence, cross-border and multi-interest stakeholders. The overall security of the mostly digital interactions of the global financial system is a most challenging task.

The thought of electronics attacks on "critical infrastructures" such as water and power grids is a chilling one. A study carried out in August by US Naval War College concluded that an electronic attack on America's critical infrastructure could indeed cause serious disruption, but would required tremendous amount of resources and preparation - some 5 years of preparation and US$200million of funding. There are simpler and less costly ways to attack. These traditional infrastructures tend to have control systems that are entirely separated from other systems. They tend to be obscure and not compatible with the Internet. Even authorized users require specialist knowledge to operate, and there are well-prepared "physical" contingency plans to deal with electronic failures.

However, most modern financial infrastructure and systems are essentially computer-driven. The impact of any attacks can be devastating as manual backup would not be practical.

2. FORCES DRIVING FINANCIAL STABILITY

The stability of a financial is largely dictated by its accountability and transparency, the reliability of its systems and its ability to recover from threats and failures. The financial market strives on deficiencies in reliability and timeliness of information. Exploitation of these deficiencies causes disruption to the stability of the market. A regime of strong transparency and accountability helps to counteract this behavior. A strong financial system will need to ensure transparency, relevance, reliability, comparability and understandability of information. Further, it must have an infrastructure that is trusted and able to recover from the crisis that will emerge from time to time. Proper management at time of crisis is often the hallmark of a resilient financial system.

The modern financial system is integrated into the global network. With the inter-dependence, countries face endless competition and the demand for instant and transparent information by global financial players. This competition drives the need for financial system to be computerized and to offer access to a wide range of players, both local and international. The opening up and the computerization of financial systems expose new risks. The increasing change of pace in technologies exerts further pressure. As inter-dependence of cross-border systems become more pronounced, there will be increasing requirements to comply with multiple standards and demands to further open

up the system to external participants. This put additional complexity as well as risk to the manageability and stability of the financial systems.

3. OPENING THE FLOODGATE - GREATER EXPOSURE WITH E-COMMERCE

E-commerce is often taken as the activities involved in buying and selling online. In our context, we will take it to mean doing transactions real-time via the financial system. E-commerce is about further opening up the financial system. It is about allowing players across borders to transact and exchange information. It is about opening up to new access methods, including the Internet, the wireless network, and hand-held devices. Coupled with new emerging technologies such as instant messaging, peer-to-peer exchanges, e-commerce can bring about tremendous pressure to the security of the financial system.

E-commerce is cross border transactions conducted digitally. However, to-date, it remains that most countries does not share an agreement on what constitute the basic elements of e-commerce, and are largely in exploration stage in legislating an effective set of e-commerce regulations. Cross-border harmonization of regulations remains years away. In the meantime, Government must focus on the protection of systems under its jurisdiction, as it cannot dictate the directions of its trading partners.

4. PLUGGING THE FLOODGATE

The floodgate to the interconnect world of the Internet has been opened. We will have to work with the assumptions that it is no longer viable to operate the financial system as a fortress only allowing small number of authorized people to have access. The assumption must be that there will be many classes of users of which many are outside its direct jurisdiction, much like the airports with lots of people coming and leaving. The solution will be lots more complex with the advent of e-commerce, but it is inevitable. This paper is in no position for in-depth treatment of how the new financial system might be protected. Below, at best, we offer some observations of the necessary considerations, and they are by no means exhaustive.

Firstly, we must accept that total security is impossible. With the understanding, we must put equal effort in looking at recovery and crisis management, in addition to seeking better ways to provide for greater security.

Secondly, security of a system is as strong as its weakness link, and in most systems, the element of human involvement is likely the Achilles' heel. Various studies have shown that the bulk of computer-related crimes are perpetuated by internal staff. Vista, a research consultancy company, estimated that 70% of security breaches involving more than US$100,000 are inside jobs, often by disgruntled employees. It is thus important that sufficient attention be paid to the management of human resources.

The challenge facing the financial system must be addressed in a holistic manner with a Government-Management-Technology partnership. Management here refers to the decision makers of the stakeholders, including firms and individuals transacting on the financial system.

5. ROLE OF GOVERNMENT

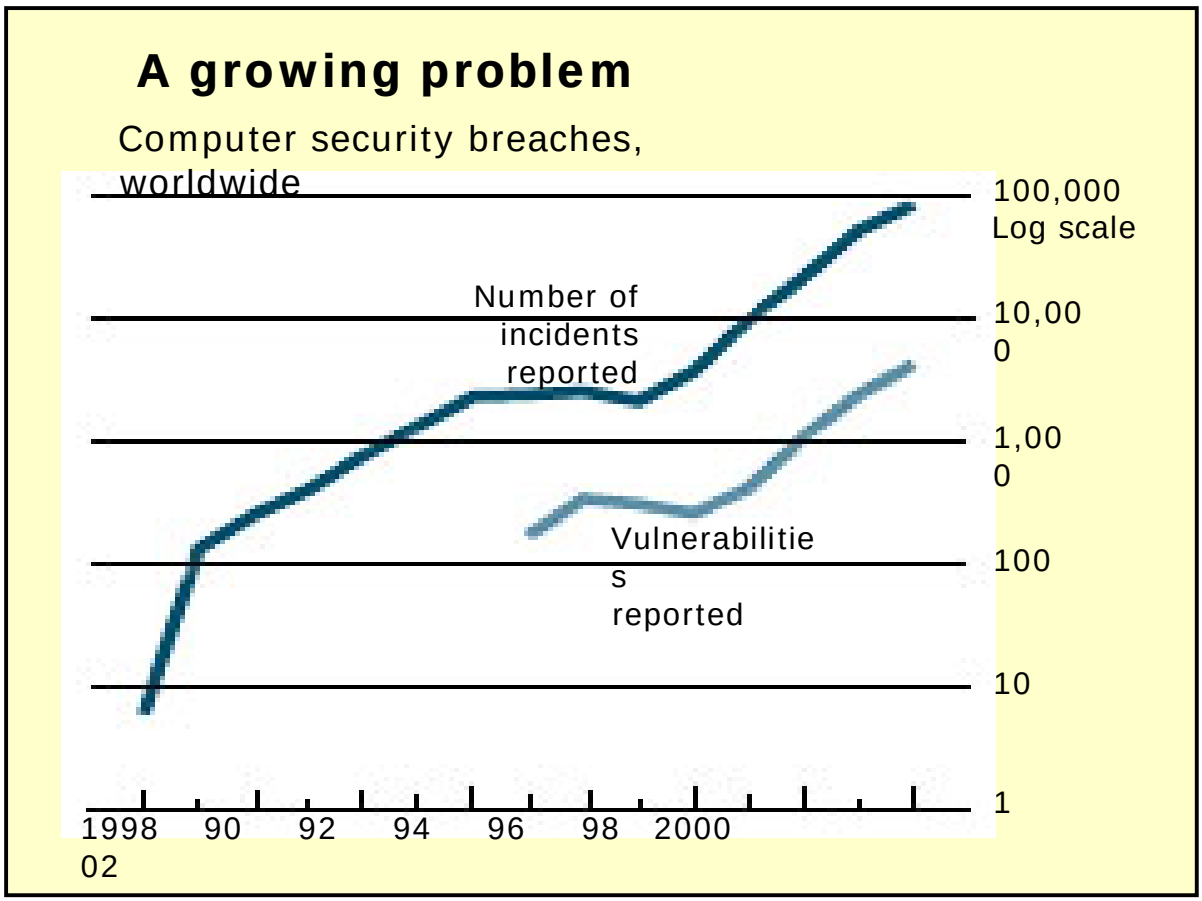
An important role of the government is to introduce and enforce appropriate regulations to make participants take more responsibility in securing the financial system. For example, changes in the audit standards in the US in 1999, requiring companies to ensure the quality of information resulted in more attention and investment made in computer security and auditing. The upcoming 2003 deadline for protecting patients' medical information under US Health Insurance Portability and Accountability Act (HIPPA) is pushing health care sector to overhaul the security of its entire network.

Another important role is for the government to establish and ensure acceptance of the equivalent legislative concepts that we have taken for granted in the physical world (e.g. signature, witness, authenticity of documents). It is also necessary that these new legislations be done with a clear appreciation that they need to find wide acceptance to ensure cross border trade. Increasingly, we are seeing nations adopting model laws to ease harmonization for cross-border trade.

Cross-border harmonization of regulations is the critical step towards a common enforceable regime for greater protection of the global financial system. Without enforceability across national boundaries, the incentives to act for financial gains will be tempting to many.

6. ROLE OF MANAGEMENT

Over the last few years, there has been growing awareness and emphasis by management on security. Nevertheless, the number of incidents reported by Carnegie Mellon's Computer Emergency Response Team (CERT) has exploded in the last few years as seen in the chart below.



Source: CERT

Though security spending is increasing, it is still a very small percentage of overall expenditure. Survey by Meta Group found that most companies spend less than 3% of their technology budget on security. This is less than 0.1% of overall spending given that technology spending is typically around 3% of revenue. Increasing spending should help improve the state of affair, however, management's involvement must go beyond it.

Management should understand that buying fancy technologies alone would not solve the problem. Improving security requires the introduction of appropriate policies, right incentives and enforcement be made in tandem.

Further, implementation of security measures cannot be left to the specialists. Implementation of security measures is a balance between risks and cost, including the inconvenience that inevitably result with the introduction of new security measures. Only management can make these trade-offs.

Management commonly perceives that threats are external, and often overlook the bigger problem associated with internal security, and the security risks internal staff pose to their trading partners. Implementing security is both a management and technical problem. Its success is as much linked to policy and human resource management, as innovative technical solutions.

7. ROLE OF TECHNOLOGISTS

The role of security technologist has been bought to the forefront with the recent spate of high-profile security breaches (in particular hackers and viruses) and the roll out of new legislations, which is speeding up as a result of 9/11. The technologist is faced with a very fast moving technological changes and one that has taken a "political" spin. He is faced with having to balance the need to protect and restrict access to its "core" system and the expanding reach of e-commerce for more users and access types.

The technologists will have to move from an "exclusion" mindset to one of "inclusion". He has to include the policy implications of his technological choices, and to include many of his trading partners as part of his "core". He has to ensure that he is able to maintain privacy/confidentiality, authenticate to ascertain source, provide integrity to detect unauthorized changes, ensure non-repudiation to prove commitment, guarantee audit ability for accountability, despite the fact that not all the computers and users are within his jurisdiction and control.

With the advent of e-commerce, he has to be particularly vigilant in monitoring physical security with both physical and electronic surveillance & monitoring methods. He has to assume the worst and ensure that full disaster recovery and crisis management are in place to bring the system back almost instantly. He has to deal with open interconnections of a multitude of access points such as Internet and wireless network that bring about virus attacks, denial-of-service attacks, and intrusions of yet unknown nature.

8. NEW CHALLENGES – A BALANCING ACT

In the wake of 9/11, the protection of financial system has taken on additional dimension, often a conflicting one, as a tool for helping to control terrorism. Before, the focus was on how to protect the system in face of bombardment of the Internet and new

technologies. The emphasis was on challenges such as fraud management, credit assessment, privacy, and non-repudiation. The new priorities are focused on preventing money laundering, ensuring disaster recovery, and to improve traceability. The US PATRIOT Act signed in the wake of 9/11, for example, imposes new anti-money laundering requirements on financial institutions.

Many of the new priorities require a calibration of priorities as they are at times at odds with existing policies. For example, the need for traceability would often conflicts with existing protections on the privacy of the users. Conversely, the introduction of new and more effective technologies (such as anonymous digital cash) can increase the difficulties of profiling and tracing.

9. CONCLUSIONS

The already complex global financial system is facing the challenges pose by e-commerce. E-Commerce exposes weaknesses of a financial system as it pushes the boundaries of its jurisdiction, and generates new demands on cross-country standards, changing technologies and varied access points. The modern financial is highly inter-related and is in the forefront of establishing the legal acceptance of various digital concepts. It is further complicated by new challenges pose by the need to balance risks, security and political considerations. The financial system has to move from an "exclusive" mode to one that is "inclusive". A holistic approach with active coordination and partnership between government, management and technologists will be necessary to tackle the challenge. This partnership need to most diligent in ensuring that it secures and protects the system under its jurisdiction, and at the same time adopt model law to ensure cross-border harmonization.