Briefing Paper

Cybersecurity

November 2013

Introduction ...........................................2
Background ............................................2
International Cybersecurity ......................4
    International Standards .......................6
    National Cybersecurity .......................7
Cyber Threats .......................................9
Enterprise Level – A Taxonomy of
Cybersecurity ......................................12
Different Risks, Same Purpose ...............13
Enterprise Calculus ...............................14
SMEs ..................................................15
Huawei’s White Paper .........................15
Closed and Private Networks ..........17
Singapore .............................................17
Conclusions .........................................18
Appendix: 1 – National Institute of
Standards and Technology (NIST) .......20
Appendix: 2 – U.S. Department of
Homeland Security ...............................21

Contact us: TRPC Pte Ltd is a boutique consulting firm which focuses on the economics of telecommunications and information technology, particularly the policy and regulatory issues associated with national information infrastructure development, with an emphasis on the Asia-Pacific region. www.trpc.biz or email us at info@trpc.biz
Cybersecurity

Introduction

Cybersecurity\(^1\) is rapidly becoming a number one issue for governments, enterprises, and increasingly so for consumers. For example, the first recorded cyber-assault on a country’s entire infrastructure was in Estonia in April 2007 when websites of Parliament, ministries, newspapers, banks, and others were brought to a standstill in distributed denial-of-service (DDoS) attacks. More recently, in early October 2013, it was reported that Adobe had discovered the credit card information of 2.9 million users of its Acrobat software had been stolen. At the end of the month the figure had been revised to 38 million and the theft involved part of Adobe’s source code which may make it far easier for criminals to break into devices using the software.\(^2\) The examples could fill a digital data centre.\(^3\)

This Briefing Paper does not attempt to cover the entire area of cybersecurity, an impossible and indeed a pointless task as each of major category of issues, ranging from cyber-warfare and cyber-spying at one end of the spectrum, through cyber-crimes great and small, to personal data protection and privacy issues, needs its own special consideration. Some of these issues call for international cooperation and criminal investigation, others call for user vigilance and cyber-education of the public.

This paper focuses on the growing range of threats to the security of public and private organisations, on the ways in which attacks can be launched, and on the best practice approaches to risk management in the field of cyberspace. As such it draws upon a selection of literature which helps to illustrate the level of the problems, and suggest a taxonomy of cybersecurity issues as a guide to risk management.

Background

Interconnectivity of everything is a dream for some, certainly for criminals. Cyber-crime has already reached industrial proportions. Not a week passes without a cyber-attack taking place somewhere. Using data from the US, in 2013 most attacks were criminal in motivation as recorded by [http://hackmageddon.com/category/security/cyber-attacks-statistics/](http://hackmageddon.com/category/security/cyber-attacks-statistics/) - see Figures 1 and 2:

---

\(^1\) Cybersecurity written as one word has been the widely accepted form since the 2013 US Federal Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity [http://www.dhs.gov/strengthening-security-and-resilience-nation%E2%80%99s-critical-infrastructure](http://www.dhs.gov/strengthening-security-and-resilience-nation%E2%80%99s-critical-infrastructure)


Of attack methods, the largest category remain unidentified (24.3%) but the most prevalent known form of attack (17.8%) is DDoS, frequently used, as a means of commercial blackmail as well as an offensive weapon. The bulk of the rest occur through Account Hijacking (16.8%), Defacement (15.9%), SQL injection attack or SQLi (9.3%) and DNS Hijacking (8.4%).

Hijacking in particular can be highly sophisticated. The insertion of malicious code into a system may remain undetected for long periods, only recognized after diagnostics reveal suspicious patterns of transactions or data flows. Registering and creating false DNS and hijacking genuine ones to redirect traffic is a blunter instrument, but can be highly effective.
for shorter periods of time. What it highlights is the importance of secondary markets for hijacked data, such as credit card numbers and personal account details. Cyber-crime creates its own black market cyber-economy.

Of the sources of attack by country, according to the 2nd Quarter Report by Akamai, Indonesia has surprisingly hit the top of the list, overtaking China. Of course the real source of the attacks could well come from anywhere globally, and servers and computers in developing economies may be seen as especially vulnerable to hijacking. One speculation is that as broadband becomes more widely adopted in these economies the easier it becomes for criminals to pirate their cyberspace.

**Figure 3: Attack Traffic, Top Originating Countries (by source IP address, not attribution)**

<table>
<thead>
<tr>
<th>Country</th>
<th>Q2 '13 % Traffic</th>
<th>Q1 '13 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Indonesia</td>
<td>36%</td>
<td>21%</td>
</tr>
<tr>
<td>2 China</td>
<td>33%</td>
<td>34%</td>
</tr>
<tr>
<td>3 United States</td>
<td>6.9%</td>
<td>8.3%</td>
</tr>
<tr>
<td>4 Taiwan</td>
<td>2.5%</td>
<td>2.5%</td>
</tr>
<tr>
<td>5 Turkey</td>
<td>2.4%</td>
<td>4.5%</td>
</tr>
<tr>
<td>6 India</td>
<td>2.0%</td>
<td>2.5%</td>
</tr>
<tr>
<td>7 Russia</td>
<td>1.7%</td>
<td>2.7%</td>
</tr>
<tr>
<td>8 Brazil</td>
<td>1.4%</td>
<td>2.2%</td>
</tr>
<tr>
<td>9 Romania</td>
<td>1.0%</td>
<td>2.9%</td>
</tr>
<tr>
<td>10 South Korea</td>
<td>0.9%</td>
<td>1.4%</td>
</tr>
<tr>
<td>– Other</td>
<td>11%</td>
<td>18%</td>
</tr>
</tbody>
</table>


**International Cybersecurity**

As reported in the 2010 report of the US Government Accountability Office (GAO)

_Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance_,

there is no internationally recognized organization responsible for coordinating an international response to a cyber-incident... The lack of an international framework for incident response has complicated efforts of US-based multinational companies to respond to international cyber incidents.

There is however an international convention. In 2004 the **Budapest Convention on Cyber-crime** (known as the Budapest Convention) came into force. It originated with the Council of Europe in 2001, and by September 2013, 40 states had ratified it, including the US in 2006, and a further 11 signed it. The objectives of the Convention are:

---


• Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime
• Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form
• Setting up a fast and effective regime of international cooperation

However legal approaches to cyber-crimes differ between nations. A document that exemplifies the differences between those who support the Convention and those who wish to retain a distance is to be found in the ITU’s Report of the Chairman of HLEG7 (High-Level Experts Group.)

The GAO report names the following organizations as being important in the international coordination of action against cyber-crimes:

<table>
<thead>
<tr>
<th>Table 1: International Coordinating Bodies Against Cyber-Crimes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>Association of Southeast Asian Nations</td>
</tr>
<tr>
<td>Council of Europe</td>
</tr>
<tr>
<td>European Union</td>
</tr>
<tr>
<td>Forum of Incident Response and Security Teams</td>
</tr>
<tr>
<td>Group of Eight</td>
</tr>
</tbody>
</table>


It would seem logical that these agencies would collaborate closely with each other, none claiming exclusivity in a fast-moving world of cyberspace. On the contrary, some reports begin their Introduction with: “In response to its mandate *as sole Facilitator* of WSIS Action Line C5, the ITU General Secretary...” [emphasis added].8 The ITU’s Global Cybersecurity Agenda (GCA) is very ambitious,9 but there is a real dilemma here because there are just so many different aspects and meanings to the word ‘security.’ Line C5 relates to “The WSIS Declaration of Principles10, which state that strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.”11 By trying to address issues as diverse as network security, and, for example, personal data protection, and online safety for minors, there is an immediate danger for any organization to lose focus and impact.12

---

9 [http://www.itu.int/osg/csd/cybersecurity/gca/hleg/membersbio.html](http://www.itu.int/osg/csd/cybersecurity/gca/hleg/membersbio.html)
11 [http://www.itu.int/osg/csd/cybersecurity/WSIS/index.phtml](http://www.itu.int/osg/csd/cybersecurity/WSIS/index.phtml)
12 See the range of activities if the ITU Cybersecurity-Gateway website [http://groups.itu.int/cybersecurity-gateway/ITUInitiatives.aspx](http://groups.itu.int/cybersecurity-gateway/ITUInitiatives.aspx)
The ITU itself recognizes the problems. For example, under *Key Cybersecurity Challenges*, one ITU presentation lists “lack of adequate and interoperable national and regional legal frameworks’ and “lack of international cooperation between industry experts, law enforcements, regulators, academia and international organizations, etc. to address a global challenge.”¹³

**International Standards**

Among the many standards-setting bodies the following are identified by the ITU’s ICT Security Standards Roadmap.¹⁴

<table>
<thead>
<tr>
<th>Table 2: ITU’s ICT Security Standards Roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global</strong></td>
</tr>
<tr>
<td>IETF</td>
</tr>
<tr>
<td>ISO/IEC</td>
</tr>
<tr>
<td>ITU-T</td>
</tr>
<tr>
<td>3GPP</td>
</tr>
<tr>
<td>3GPP2</td>
</tr>
<tr>
<td><strong>Regional</strong></td>
</tr>
<tr>
<td>ATIS</td>
</tr>
<tr>
<td>ETSI</td>
</tr>
<tr>
<td>IEEE</td>
</tr>
<tr>
<td>RAISS</td>
</tr>
</tbody>
</table>


However

In the past 20 years the ICT industry has had phenomenal growth by agreeing global technical standards and disciplines – from hypertext to WiFi – but when it comes to Cybersecurity many standards are just not followed. (John Suffolk, Global Head of Cybersecurity,¹⁷ Huawei ‘We should learn from the cold war to strengthen cyberspace’ *Financial Times*, 21 October, 2013)

In the US the Department of Commerce’s National Institute of Standards and Technology (NIST) has been commissioned along with the Department of Homeland Security to produce a Cybersecurity Framework as a “living document” that is a “standards-based approach” to the Framework with the emphasis upon interoperability, scalability and reliability¹⁸ but on a purely voluntary basis for industry. A paper released by Microsoft (2013) *Developing a*

---


¹⁵ Unites six telecom standard development organizations: ARIB (Japan), ATIS (US), CCSA (China), ETSI, TTA (Korea), TTC (Japan) [http://www.3gpp.org/About-3GPP](http://www.3gpp.org/About-3GPP)

¹⁶ Develops global specifications for ANSI/TIA/EIA-41 Cellular Radio telecoms, mostly for North American and Asian markets [http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm](http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm)

¹⁷ Previously UK Government CIO

National Strategy for Cybersecurity, notes that “some governments have adopted well-known security approaches to help manage risk, such as the ISO/IEC 27000 family of standards or the U.S. NIST Special Publication series while others have adopted a ‘Top 20’ approach to prioritize mitigations.”

A risk-management approach is now standard practice among national cybersecurity strategy plans. See, for example, the EU’s National Cyber Security Strategies: Practical Guide on Development and Execution published in December 2012 by the European Network and Information Security Agency (ENISA).

National Cybersecurity

National cybersecurity is generally focused on three levels: safeguarding critical infrastructure from attacks as may arise in cyber-warfare, combatting cyber-spying including industrial espionage, and enhancing the capacity of the public and private sectors and citizens against cyber-crimes.

The common approach to cybersecurity for critical infrastructure is the creation of a National Emergency Response Team or CERT. For example, at the APECTEL in 2010, Australia reported the results of its survey of seven responding APEC economies showing that all had established CERTs. Specifically for the telecom sector the ITU has promoted a Cybersecurity Information Exchange Framework or CTBEX. It consists of a set of protocols and standards and a general framework which integrates different security domains, such as measures for protection, detection, remedies and legal as illustrated in Figure 4 below.

Combatting cyber-spying is a more diffuse exercise. It ranges from the methods employed by national intelligence agencies worldwide, constrained only by the limits of the cyber technologies available to them and public oversight to variable degrees, to industry efforts to closedown loopholes in their information security systems and to detect breaches and loss of assets as quickly as they can by following recommended procedures.

References:
The crucial element of any national strategy, according to the Microsoft (2013) paper is that it should be “regularly updated as an ongoing process…” and “continuous monitoring of systems involves using automation to collect and analyse data from a variety of sources in order to maintain an accurate description of an organization’s security posture to support organizational risk-management decisions.” This in turn requires trained “cybersecurity and forensic experts to manage and defend networks…” and it is “essential that the relevant agencies have the right resources and skills to meet the operational security needs set forth in the national strategy.” One of the important roles CERTs could play is to provide such training for government agencies and to support and partner with the private sector in training. (See also ‘Singapore’ below). Special attention could also be given to SMEs within such a national framework.

According to the report “Microsoft has observed dozens of national approaches aimed at addressing cyber risk, and has developed views about what makes for an effective national cybersecurity strategy.” The three most important characteristics of a successful strategy are seen to be (1) it must be a ‘living’ document developed in partnership with public and private stakeholders; (2) is must be based upon “clearly articulated principles that reflect societal values, traditions and legal principles”; (3) they are based upon a risk-management...

---

approach, including those risks that must be accepted. Microsoft lays out six foundational principles:

**Table 3: Foundational Principles of Cybersecurity Strategy**

<table>
<thead>
<tr>
<th>Principles</th>
<th>Cybersecurity Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk-based</td>
<td>Identify and assess risks, then use mitigation measures</td>
</tr>
<tr>
<td>Outcome-focused</td>
<td>Focus on ends rather than means, and monitor progress</td>
</tr>
<tr>
<td>Prioritized</td>
<td>Adopt a graduated approach according to level of risk</td>
</tr>
<tr>
<td>Practicable</td>
<td>Optimize to apply for largest group of critical assets</td>
</tr>
<tr>
<td>Respectful of privacy and civil liberties</td>
<td>Include privacy protection based upon Fair Information Practice Principles</td>
</tr>
<tr>
<td>Globally relevant</td>
<td>Integrate international standards and keep harmonization in mind</td>
</tr>
</tbody>
</table>

Source: adapted from Microsoft (2013) *Developing a National Strategy for Cybersecurity*

Co-ordinating between national agencies seems to be just as fundamental a problem as co-ordinating between international agencies. The GAO report, for example, states that “unless the Cybersecurity Coordinator provides top-level leadership, there is an increased risk that US agencies will not formulate and coordinate U.S. international cybersecurity-related positions as envisioned in the President’s Cyberspace Policy Review...” but notes that the “Cybersecurity Coordinator and staff stated that our report does not fully portray their leadership efforts...”

**Cyber Threats**

The Microsoft paper identified four broad categories of cyber-crimes: conventional, military and political espionage, economic espionage and cyber-conflict cyber-warfare. This Briefing Paper is principally concerned with the first and third of these categories.

The GAO report identified the following sources of threats:

**Table 4: List of Cyber Threats by US Government Accountability Office (GAO)**

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bot-network operators</td>
<td>Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial of service attack or servers to relay spam or phishing attacks).</td>
</tr>
<tr>
<td>Criminal groups</td>
<td>Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.</td>
</tr>
<tr>
<td>Hackers</td>
<td>Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking others, and monetary gain, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks.</td>
</tr>
</tbody>
</table>

Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.

**Insiders**
The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization, as well as employees who accidentally introduce malware into systems.

**Nations**
Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.

**Phishers**
Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.

**Spammers**
Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).

**Spyware/malware authors**
Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

**Terrorists**
Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: US GAO

Any list of threats, even by general categories, will require regular updating, but often it is not just the new threats that are seriously damaging but the old threats which are so easily replicated. Spear phishing, for example, works because while regular uses of email may become wise to suspicious anonymous invitations to visit fraudulent websites or to open malicious attachments, an email that appears to come from a friend or a colleague is more difficult to ignore or resist.

Another example is the stealing of passwords and identify theft. These are widespread techniques of cyber-criminals. A more sophisticated method is to install a keyboard video mouse (KVM) device that reveals every keystroke entered. The installation is the tricky part and often has to rely upon an insider or an outsider who has managed to breach security. For example, eight men were arrested in the UK in September 2013 for stealing £1.3 million from a leading bank. A gang member posed as an engineer and installed a KVM on the bank's computers. Perhaps the most important part of the story is that the transactions were quickly identified as ‘unusual’ and the fraud was detected and the money recovered.24 Security breaches will take place, but are the systems robust enough to spot the malfeasance in time?

---

Responses Requiring R&D

A report in 2009 by the US Department of Homeland Security, *A Roadmap for Cybersecurity Research*,\(^2^5\) identifies eleven “hard problems” that require attention:

Table 5: Eleven Hard Problems for Cybersecurity Research

<table>
<thead>
<tr>
<th>Hard Problems</th>
<th>Research Requirements</th>
</tr>
</thead>
</table>
| 1             | Scalable trustworthy systems  
“the security of a system may be drastically less than that of most of its components.. The perceived order of importance for R&D in this topic areas is as follows: (1) trustworthiness, (2) composability, and (3) scalability.” |
| 2             | Enterprise-level metrics (ELMs)  
“Lack of effective ELMs leaves one in the dark about cyber threats in general... This lack seriously impedes the ability to make enterprise-wide informed decisions of how to effectively avoid and control innumerable known and unknown threats and risks at every stage of development and operation.” |
| 3             | System evaluation life cycle  
“The security field lacks methods to systematically and cost-effectively evaluate its products in a timely fashion... Systematic, realistic, easy-to-use and standardized evaluation methods are needed to objectively quantify performance of any security artefact [i.e. protocol, device, architecture or system].” |
| 4             | Combating insider threats  
“The insider threat today is addressed mostly with procedures such as awareness training, background checks, good labor practices, identity management and user authentication, limited audits and network monitoring, two-person controls, application-level profiling and monitoring, and general access controls. However, these procedures are not consistently and stringently applied because of high cost, low motivation and limited effectiveness.” |
| 5             | Combating malware and botnets  
“Present classes of malware include viruses, worms, Trojan horses, spyware and bot executables... Current detection and remediation approaches are losing ground... Emerging approaches such as behaviour-based detection and semantic malware descriptions have shown promise.” |
| 6             | Global-scale identity management  
“Our concern here is mainly IT-oriented aspects of broad problems of identity and credential management, including authentication, authorization and accountability. However, we recognize there will be many trade-offs and privacy implications...” |
| 7             | Survivability of time-critical systems  
“At present, IT systems attempt to maximize survivability through replication of components, redundancy of information (e.g., error-correcting coding), smart load sharing, journaling and transaction replay, automated recovery to a stable state, deferred committing for configuration changes, and manually maintained filters to block repeated bad requests... The current metrics for survivability, availability and reliability of time-critical systems are based on the probabilities of natural and random failures (e.g., MTBF\(^2^6\)). These metrics typically ignore intentional attacks, cascading failures, and other correlated causes and effects... Future research should be divided into three categories: understanding the mission and risks; survivability architectures, methods and tools; and test and evaluation.” |
| 8             | Situational understanding and attack attribution  
“The challenges lie in the path from massive data to information understanding if a system is under attack, who is the attacker, what is the attacker’s intent, how do we defend against the attack and how can we prevent or deter the attack in the future... Accurate attribution (‘defined as determining the identity or location of an attacker or an attacker’s intermediary’) supports improved situational understanding and is therefore a key element of research in this area... Attribution should also encompass shell companies, such as rogue domain resellers...” |
| 9             | Provenance (related to information, systems and hardware)  
“Provenance refers to the chain of successive custody... includes pedigree, which relates to the total directed graph of historical dependencies... The granularity of provenance ranges from whole systems through multi-level security, file, paragraph, and line, and even to bit. For certain applications (such as access control) the provenance of a single bit may be very important.” |

\(^2^5\) For a synopsis see [http://cyber.law.harvard.edu/cybersecurity/A_Roadmap_for_Cybersecurity_Research](http://cyber.law.harvard.edu/cybersecurity/A_Roadmap_for_Cybersecurity_Research)

\(^2^6\) Mean time between failures
Privacy-aware security encompasses several distinct but closely related topics, including anonymity, pseudo-anonymity, confidentiality, protection of queries, monitoring, and appropriate accessibility... The central problem of privacy-aware security is the tension between competing goals in the disclosure and use of private information...”

“Typically, as the security of systems increases, the usability of those systems tends to decrease... Security issues must be as transparent as possible... In the short-term, the current situation can be significantly improved by R&D that focuses on making security technology work sensibly ‘out-of-the-box’ – ideally with no direct user intervention.”

**Source:** US Department of Homeland Security, 2009

### Enterprise Level – A Taxonomy of Cybersecurity

Advanced Persistent Threat (APT) is the term used by the cyber-security community to describe the growing dangers of malware that exploit DNS or SQLi for malicious communications and data transfer. APT is seen as a growing threat to enterprise because legacy security measures that are targeted against traditional cyber-threats such as worms, Trojans, viruses, etc., are often ineffective against the insertion of malware into systems.

Systematic threats call for systematic responses, and although there is an important debate as to whether or not there is yet sufficient breadth as well as depth of understanding of cyber-space to produce a comprehensive taxonomy of threats and how to deal with them,27 several have emerged. The CERT Program, part of the Carnegie Mellon University’s Software Engineering institute (SEI), has produced one of them named a Resilience Management Model “which draws upon the definition of operational risk adopted by the banking sector in the Basel II framework.”28 The model, reproduced below in outline in Figure 5, identifies four classes of risk: (i) actions of people, (ii) systems and technology failures, (iii) failed internal processes, and (iv) external events.29 The model contains sub-classes under each heading and their elements. It should be noted that failure in one category of risk can cascade as it impacts upon other categories.

As a benchmarking and reference tool such a taxonomy is undoubtedly strategically important. The model offers a series of ‘decision trees’ to follow through from problem arising to solution achieved.

---

27 For example, Doug DePeppe (January 2013) expressed the following concern for ‘A taxonomy for the National Cybersecurity Doctrine’: “We can also look at lexicon shifts: network security, information security, data protection, cyber security, ... This uncertain landscape reminds me of my partner’s reference to cybersecurity as a ‘five-year old soccer game, with everyone chasing the ball in a cluster and without a game plan.’ We remain in an immature state with respect to cybersecurity... Academic study and shaping of a cybersecurity discipline would therefore seem more helpful than a new doctrine.” [http://www.csoonline.com/article/727099/a-taxonomy-for-the-national-cybersecurity-doctrine?page=1](http://www.csoonline.com/article/727099/a-taxonomy-for-the-national-cybersecurity-doctrine?page=1)


29 For a blog discussion of the strengths and weaknesses of this taxonomy, see Bruce Schneier [https://www.schneier.com/blog/archives/2011/08/taxonomy_of_ope.html](https://www.schneier.com/blog/archives/2011/08/taxonomy_of_ope.html)
Different Risks, Same Purpose

While no two enterprise networks are the same, either in architecture or in modes of operation, they do share many common aspects. For example, they are usually multi-component and multi-sub-systems and at weak links along the chain it is possible to insert malware, by internal means or by online means. The remedies are easier to state than to implement: identify the attack, quarantine the components or sub-systems, isolate the effects, recover as many assets as possible, and restore security. After that, try to anticipate the next areas of vulnerability and upgrade the security measures.

Historically, telecom networks have been examples of these procedures. Whenever new software is to be introduced into their systems, they do it in sectioned-off parts of the network. This has not always been successful. In 1990, for example, the AT&T network in the US temporarily went down coast to coast due to a software glitch in just one of its exchanges. Because networking is the product a telecom company sells, awareness of the problem was immediate even if it took time to identify the cause. In AT&T’s case it was not
a cyber-attack, but initially no-one knew whether it was or wasn’t: asked whether it could be, the spokesman said “we’re not going down that road yet.”

Identification of the attack is the critical issue. For example, if the attack is super surreptitious the data leakage might go on for months before it is discovered. Indeed, that is the objective of cyber-spying. Diagnostics that can identify suspicious patterns in the data is a vital tool and widely used, especially in the banking and financial sectors. The tools are there for large enterprises because the value of the assets at risk is high and the attacks can be very sophisticated, so the diagnostic software has to be equally sophisticated. This is high value business for IT professionals. High-risk, high-value markets are well served by top-end IT companies. For smaller companies the issues are not so simple. For example, how carefully and how regularly do people check their bank statements and credit card balances? Just like consumers, SMEs often depend upon human alertness which is not very safe or reliable, and they lack the tools to substitute for it. Here there is a market for easy-to-use and out-of-the-box tools. In Singapore, for example, this could become part of the IDA’s Call-for-Collaboration (CFC) projects which often target IT adoption by SMEs.

Another common feature of many networks is they are connected, directly or indirectly, to third party networks, such as suppliers, logistics companies and customers. The trend since the 1990s has been to open some internal company databases to collaborating partners and that trend is now extending to state agencies in the form of Open Government projects. The implication is that network vulnerabilities beyond the control of enterprises may exist in these other networks. Firewalls help, but traditionally these work by allowing or blocking (as one vendor puts it) “entire network channels (ports) as opposed to individual applications.” Of course, these weaknesses represent an opportunity for vendors to offer improved security tools.

**Enterprise Calculus**

There is no shortage of vendor advice on how to approach security at the enterprise level, and each enterprise will have its own priorities in terms of assets to protect, and its own set of vulnerabilities and levels of risk. Trends such as the use of cloud computing for document storage and retrieval and for collaborative work on an international scale also shift the parameters, so legacy approaches to security may not be sufficient and new learning curves have to be climbed. These shifts raise the level of both the costs and benefits involved so the calculus for each enterprise will be different. Company A may be planning on manufacturing a new version of its product and its primary asset lies in its trade secrets; naturally it will focus security on reducing the risk of theft. The opportunity cost for

---


11 Identification here includes (a) realization an attack is underway or has taken place, (b) identifying the location and method of the attack, and if possible, (c) identifying the source of the attack.

12 In September 2013, for example, IDA issued a CFC worth SGD42 million (USD 33 million) to boost SME productivity through IT adoption: [http://www.ida.gov.sg/Collaboration-and-Initiatives/Collaboration-Opportunities](http://www.ida.gov.sg/Collaboration-and-Initiatives/Collaboration-Opportunities)

13 Paloalto [2013] [https://www.paloaltonetworks.com/resources/whitepapers/cybersecurity-imperatives.html](https://www.paloaltonetworks.com/resources/whitepapers/cybersecurity-imperatives.html)
company A is what it would mean to lose its trade secrets on which its entire future may depend. Company B may be a bank and of necessity its security will focus upon transactions and privacy of its customers’ data. Losing funds and customer data may be no be fatal for the bank but very costly in terms of embarrassing reputational damage, and inevitably the bank’s security systems will be complex.

**SMEs**

At the other end of the spectrum are the SMEs, often family businesses that traditionally are reluctant to store records, company accounts and trade secrets in documents of any kind. In all countries SMEs are slow to adopt IT, partly for these reasons; but as the digital economy starts to impact upon all forms of business this is likely to become a major sector of growth for low-cost and easily implemented security tools, as discussed above.

Although in terms of risk priorities, no two industrial and commercial sectors are the same, and rarely are two enterprises within each sector the same, there is nevertheless a common procedural issue that they need to share. Whether it’s a single firewall or a whole blanket of security tools, each enterprise needs to audit and monitor its level of security on a regular basis. Failure to do so shifts the problem from known risks to unknown risks and therefore increased insurance premiums. There are some companies that need that level of quality control throughout their entire product and production cycle, from customer input and the R&D and design process, through the procurement process for components and parts, to manufacturing and assembly and testing, to final customer delivery and installation and post-sales maintenance. The telecom equipment manufacturer Huawei is one such company and has recently issued a cyber-security white paper outlining its own production process security model.\(^{34}\)

**Huawei’s White Paper**

Huawei’s white paper also serves to combat suspicions expressed by politicians in the US, Australia, and the UK among others, that this Chinese company may be embedding bugging devices into its carrier products. Irrespective of whether it does or does not come under pressure from China’s state security apparatus – and the same sets of issues surely apply to all equipment manufacturers from all nation states \(^{35}\) – Huawei’s white paper has some interesting lessons for any enterprise wishing to ensure absolute end-to-end surveillance whether it applies to cyber-security or any other quality control issue.

---


\(^{35}\) This issue is a classic case of what economists call moral hazard. The PR of any company will deny wrong-doing in cyber-space and probably will be among the last to know of any wrong-doing into the bargain, which adds a touch of authenticity to any denials. At the same time no national intelligence agency in the world would easily pass up the opportunity, subject to two principles: as far as possible keep it legal, and never get caught. Doing it too often and too regularly is one way to get caught out. Outsourcing it to a whistle-blower is, of course, another way.
Figure 6 is from the white paper showing Huawei’s overall process architecture which starts from the customer’s input in terms of immediate past experience and future requirements, then proceeds through a series of audited and monitored steps which include parts bought in from suppliers, and concludes with delivery to the customer and a renewal of the whole cycle. This is an exceptionally controlled and secure set of procedures that can only make sense in cost-benefit terms due to the fact that the product itself is a security product. The production of refrigerators or TV sets, for example, would hardly warrant such an exhaustive process.\(^{36}\)

**Figure 6: Huawei’s Production Process Architecture**

As supply chains stretch globally, security and quality control risks are bound to rise. The Microsoft (2013) paper includes the following core elements for reducing supply chain risk. The paper is directed towards government agencies, but can apply equally to enterprise:

- An overall threat model for supply chain risk developed by the government and shared with its ICT vendors and suppliers.
- Policies and controls to ensure that the government is buying genuine products from trusted sources, as well as capabilities that can identify and remove counterfeit or

---

\(^{36}\) From a business economics perspective, there will always be a trade-off between quality control, which is expensive, and post-sales repairs, maintenance, replacement and redemption. Where security is the key issue, the trade-off can be expected to favour quality control. In some cases the trade-off is highly questionable, as in the legal case surrounding deaths in the 1970s claimed to be due to a safety fault in the Ford Pinto car, a case that remains controversial to this day, see [http://www.corporatenarc.com/fordpintoscandal.php](http://www.corporatenarc.com/fordpintoscandal.php). Whatever the merits of the arguments in that case, the issue remains that there are opportunity costs (monetary and reputational) associated with cost cutting on security or safety or quality.
gray-market systems that can create risks to the integrity of government information, services, and assets.

- A lifecycle approach to government systems that extends beyond the procurement phase and addresses the controls needed to ensure that the process for updating systems and retiring systems does not introduce risk into organizations.
- Mechanisms to ensure that suppliers have demonstrable processes for: (1) managing employee identity, including tying identity to role-based access for system development and production; (2) a secure development process, such as the Microsoft Security Development Lifecycle and ISO 27034:1; (3) code integrity practices that prevent or remediate potential risks associated with intentional or unintentional insertion of malware; (4) digitally signing code; and (5) swift recognition of counterfeit products.

**Closed and Private Networks**

Even closed networks are vulnerable. In most cases the means of attack requires an initial offline point of entry, for example, an internal staff or an outside maintenance contractor inserting illegal bugging devices. But even this may not be true if parts of the network are wireless and can be intercepted by outside persons. At the very highest level of cyber-spying is the interception of data over the fibre cable connections and data management systems. For example, an IPVN or a managed data network over international leased circuits at some stage leaves the physical premises of the user organization and enters the domain of a carrier. The revelations of Edward Snowden are sufficient to confirm that ‘stuff happens’.

**Singapore**

The cost to Singapore of its interconnectivity is that it “is internationally ranked fourth highest in cyber-crime rate and this is expected to increase” according to Hee Jhee Jiow (NUS) in the Jan-July 2013 edition of the International Journal of Cyber Criminology.\(^ {37}\) Over the past year, cyber-crime has cost each victim in Singapore on average SGD 1,448 (USD 1,158), much higher than the global average of SDG 370 (USD298) according to a newly released Norton report.\(^ {38}\) This represents a jump of 75% from the previous year, but the percentage of victims actually fell, suggesting perhaps a more sophisticated focus by criminals on higher value heists.

Singapore’s approach has been two consecutive 2005-2012 multi-agency IT and Cybersecurity Masterplans led by the IDA, and the most recent 5-Year National Cyber Security Masterplan 2018. The latest plan places focus on three areas: the security and resilience of the Critical Information Infrastructure (CII) to include a number of cross-sector exercises; the promotion of security adoption by business and end-users including

---


situational awareness; growing the pool of cybersecurity experts through working with Institutes of Higher Learning (IHL) and industry. Situational awareness and risk mitigation are to be handled through a Cyber Watch Centre and a Threat Analysis Centre. At the highest level is the National Security Coordination Secretariat (NSCS) based in the Prime Minister’s Office.

In 2012 the Computer Misuse and Cybersecurity Act was strengthened to give the Ministry of Home Affairs (MHA) powers to take direct measures upon receipt of credible information that an attack on CII was being planned rather than having to wait until such an attack is underway. Awareness is also being promoted through campaigns orchestrated by the Cyber Security Awareness Alliance between the IDA and the Singapore Infocomm Technology Federation (SiTF). Training has been enhanced with the setting up of a Cyber Security Lab (CSL) at the Nanyang Technological University to serve the Home Team Academy, where the Home Team includes the Singapore Police Force, the Department of Internal Security, the Civil Defence Force, the Prison Service, Immigration and Checkpoints Authority, the Central Narcotics Bureau and the Casino Regulatory Authority.

At the enterprise level, the IDA is taking steps to foster the development of local security software through the Call-for-Collaboration (CFC) process. For example, in August 2013 IDA issued a CFC calling for proposals for a DDoS Mitigation Service:

As DDoS attack patterns change, it is no longer sufficient just to augment a target’s perimeter defences, e.g. firewalls, IPS, WAF, as such defences are usually constrained by bandwidth and capacity limitations and are easily overwhelmed during a large scale DDoS attack. What is needed is to push the mitigation upstream into the Internet, to provide automated access to sufficient resources to quickly scale to mitigate DDoS attacks, and to do so in a cost effective manner.

This nicely captures the changing nature of the threats and therefore the changes needed in security response strategies.

Conclusions

Cyber-attacks are clearly a growing problem, although as research from Freshfields seems to show share prices rarely reflect the extent of the damage done.

41 http://sce.ntu.edu.sg/Research/cyber/Pages/index.aspx
Freshfields research suggests that only one-in-ten of the listed companies in its global sample saw share prices drop by over 2 per cent, although that accounted for US$53 billion. The average time for share prices to climb back to their pre-attack levels was 24 days. Their analysis “also reveals that industrial espionage the biggest immediate impact and ‘hactivism’ has the longest-term effect in share prices.” See chart above.

This suggests that companies, and their shareholders, have still not fully appreciated the potential costs, financial but also existential, at risk from breaches in cybersecurity. Within a public agency or private enterprise this is most likely reflected in the persistence of legacy approaches to security, in particular dealing with each type of cyber threat as a separate and discrete issue with its own solution. In a large enterprise the role of security will most likely come under the CIO, but how, for example, does the enterprise co-ordinate the role of the CIO with the HR department’s recruitment policies and vetting potential employees, or with the CEO’s enterprise strategy of outsourcing some business processes to third parties? If any evidence of the latter was necessary, see the Wall Street Journal’s account of how vetting of US Government security personnel was outsourced leading to their headline ‘Former Officials Say Firm Rushed Background Checks’. The rest, as they say, is history.

---

44 http://online.wsj.com/news/articles/SB30001424052702304330904579137443326694158
Appendix: 1 – National Institute of Standards and Technology (NIST)

“The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation’s measurement and standards infrastructure... The United States Office of Management and Budget (OMB) issued a memo in April 2010 requesting that the Department of State, Department of Justice, and Department of the Treasury coordinate with the Department of Homeland Security (DHS) to evaluate their continuous monitoring (CM) best practices and scale them across the Government. As a result of this evaluation, DHS released the Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESARS) Reference Architecture Report version 1.8. The CAESARS report provides a reference architecture, based on security automation standards, that guides organizations in deploying enterprise CM implementations.”

Figure 8: Enterprise Architecture View for Continuous Monitoring

---

### Table 6: Categories of Cyber Exploits

<table>
<thead>
<tr>
<th>Cyber exploits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of service</td>
<td>A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.</td>
</tr>
<tr>
<td>Distributed denial of</td>
<td>A variant of the denial of service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.</td>
</tr>
<tr>
<td>service</td>
<td></td>
</tr>
<tr>
<td>Exploit tools</td>
<td>Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.</td>
</tr>
<tr>
<td>Logic bombs</td>
<td>A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer’s employment.</td>
</tr>
<tr>
<td>Phishing</td>
<td>The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.</td>
</tr>
<tr>
<td>Sniffer</td>
<td>Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.</td>
</tr>
<tr>
<td>Virus</td>
<td>A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.</td>
</tr>
<tr>
<td>Vishing</td>
<td>A method of phishing based on voice-over-Internet-Protocol technology and open-source call centre software that have made it inexpensive for scammers to set up phony call centres and criminals to send e-mail or text messages to potential victims, saying there has been a security problem, and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.</td>
</tr>
<tr>
<td>War driving</td>
<td>A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adapter that involves patrolling locations to gain unauthorized access.</td>
</tr>
<tr>
<td>Worm</td>
<td>An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.</td>
</tr>
<tr>
<td>Zero-day exploit</td>
<td>A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.</td>
</tr>
</tbody>
</table>


[^46]: For a synopsis see http://cyber.law.harvard.edu/cybersecurity/A_Roadmap_for_Cybersecurity_Research