Explorations in Cyber International Relations (ECIR) – Data Dashboard Report #1: CERT Data Sources and Prototype Dashboard System

Stuart Madnick, Nazli Choucri,
Steven Camina, Erik Fogg, Xitong Li, Fan Wei

Composite Information Systems Laboratory (CISL)
Sloan School of Management, Room E53-320
Massachusetts Institute of Technology
Cambridge, MA 02142

Explorations in Cyber International Relations (ECIR)

Data Dashboard Report #1:

CERT Data Sources and Prototype Dashboard System

Prof. Stuart Madnick
Prof. Nazli Choucri
Steven Camina
Erik Fogg
Xitong Li
Fan Wei

10 August 2009

ABSTRACT

Growing global interconnection and interdependency of computer networks, in combination with increased sophistication of cyber attacks over time, demonstrate the need for better understanding of the collective and cooperative security measures needed to prevent and respond to cybersecurity emergencies. The Exploring Cyber International Relations (ECIR) Data Dashboard project is an initial effort to gather and analyze such data within and between countries. This report describes the prototype ECIR Data Dashboard and the initial data sources used.

In 1988, the United States Department of Defense and Carnegie Mellon University formed the Computer Emergency Response Team (CERT) to lead and coordinate national and international efforts to combat cybsersecurity threats. Since then, the number of CERTs worldwide has grown dramatically, leading to the potential for a sophisticated and coordinated global cybersecurity response network. This report focuses primarily on the current state of the worldwide CERTs, including the data publicly available, the extent of coordination, and the maturity of data management and responses. The report summarizes, analyses, and critiques the worldwide CERT network.

Additionally, the report describes the ECIR team's Data Dashboard project, designed to provide scholars, policymakers, IT professionals, and other stakeholders with a comprehensive set of data on national-level cybersecurity, information technology, and demographic data. The Dashboard allows these stakeholders to observe chronological trends and multivariate correlations that can lead to insight into the current state, potential future trends, and approximate causes of global cybersecurity issues. This report summarizes the purpose, state, progress, and challenges of developing the Data Dashboard project.

Disclaimer: This report relies on publicly available information, especially from the CERTs' pubic web sites. They have not yet been contacted to confirm our understanding of their data. That will be done in subsequent phases of this effort. This work was funded, in part, by the Office of Naval Research under award number N00014091059. Any opinions, findings, and conclusions or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

1. Introduction

The development of the modern economy, and of sophisticated information technology in particular, has led to an increasing global interconnectivity and interdependence. Such interconnectivity deeply benefits commerce and communication, but collectivizes vulnerabilities and security problems to a state the international community has not before had to address. The development of collective and collaborative cybersecurity has been formally underway for more than twenty years, and much progress has been made. Nonetheless, there remain many opportunities to further develop collaborative and decentralized collective cybersecurity networks and procedures.

The purpose of this report is twofold: first, the report explores and summarizes the state of collaboration and information availability from the oldest and most-developed formal institutions of collaborative cybersecurity: the Computer Emergency Response Teams (CERTs), and identifies potential shortcomings and areas for development. Second, we introduce the reader to the Data Dashboard project, conducted under the auspices of the Exploring Cyber International Relations (ECIR) team at MIT and Harvard. The Dashboard will function as a simple, easy-to-use source on global and nation-level data, with specific emphasis on cybersecurity and threat data, as well as on related current events. The Dashboard is designed to help researchers, policymakers, IT professionals, and other stakeholders to track potentially critical trends in relevant cybersecurity data, including attacks, threats, vulnerabilities, and defenses, etc. Increasing stakeholder access to summary and analytical data should significantly increase the efficacy of cybersecurity efforts at all levels, including individual and institutional defense, corporate and national policymaking, and high-level coordination and cooperation.

Well-known collectors of relevant nation-level cybersecurity data are the Computer Emergency Response Teams, or CERTs. The largest CERTs typically operate at a national level as quasi-governmental entities (that is, a country has its own CERT), but have a mandate to coordinate extensively with other CERTs within the country and in other countries, often under the auspices of the CERT Coordination Center (CERT/CC) operated by Carnegie Mellon University (CMU). While highly diverse, and often in infancy, these CERTs have the potential to not only provide critical cybersecurity data to all stakeholders, but also to coordinate responses to cyber attacks or to other cyber emergencies. A brief history, summary, and analysis of national-level CERT activities and their publicly available data are discussed below.

2. Computer Emergency Response Teams (CERTs)

2.1 History and Purpose of CERTs

The first CERT, at Carnegie Mellon University (CMU), was launched in 1988 with funding from DARPA, as a response to the Morris Worm attack (which took down perhaps 10% of the Internet during November, 1988). The CERT mandate is now to develop and promote best management practices and technology applications to "resist attacks on networked systems, to limit damage, and to

ensure continuity of critical services."[1]

The CMU CERT, during the 1990s, began to help other countries develop their own CERTs and maintains to this day a formal Computer Security Incident Response Team (CSIRT) development program[2], including for the United States. The CERT at CMU is now officially known as the CERT Coordination Center (CERT/CC), as many other response teams have chosen the name CERT (where others have chosen CSIRT). The Coordination Center works closely with US-CERT, the latter of which is an indirect branch of the Department of Homeland Security. It uses a largely decentralized approach to prevention of security failures (in education and training, helping create local CERTS, publishing information, etc), but is ready to lead a coordinated response with US-CERT and other local CERTs in order to stamp out major security failures or major threats.

CERT/CC works in the following fields; these fields provide a guideline for the work of other national CERTs and CSIRTs around the world:

> ● Software Awareness: Searches for, receives, analyzes, and reports major software security vulnerabilities and malicious code. Publishes advice on responses to vulnerabilities and threats, helping to create software more secure to attack.

> ● Secure Systems: Engineering of networks that have high situational awareness and high response speed to deal with coordinated attacks. Goal is to create networks that can survive attack and continue functioning.

> ● Organizational Security: Encourages and helps develop implementation of proper security management and software in individual organizations. Advocates government policy that increases security of national, corporate, and private systems.

> ● Coordinated Response: Helps create and train response teams for different organizations, governments, and companies, including the Department of Homeland Security (US-CERT), and the National Computer Security Incident Response Team (CSIRT) of Qatar. Thanks largely to this training, the United States has dozens of smaller CSIRTs (that belong to enterprises or industry organizations) that work together to deal with high-risk threats, and to perform forensics on past security breaches.

> ● Education and Training: Provides public training seminars, certification training/testing, as well as collegiate degrees at CMU.

The interconnected nature of modern computer networking assures that major failures in the security of a single institution have the potential to create larger damage to other institutions, or even large portions of the Internet. To solve the collective action problem, CERTs were designed with decentralization and coordination in mind. Ideally, the national CERTs would overlook an array of CERTs at various levels below. CERTs within a single company or institution, in a sector, etc, would work with each other under the auspices of the national CERT in order to offer both robust prevention and monitoring capability and a decentralized, distributed response to emergencies and attacks that may arise. This ideal configuration would lead to an efficient coordination between organizations

---

1 http://www.cert.org
2 http://www.cert.org/csirts/

ranging from semi-government to non-profit to private/corporate to ensure both collective and individual security. Figure 1.1 (below) provides an abstract diagram of the potential hierarchies and responsibilities of a distributed CERT system.
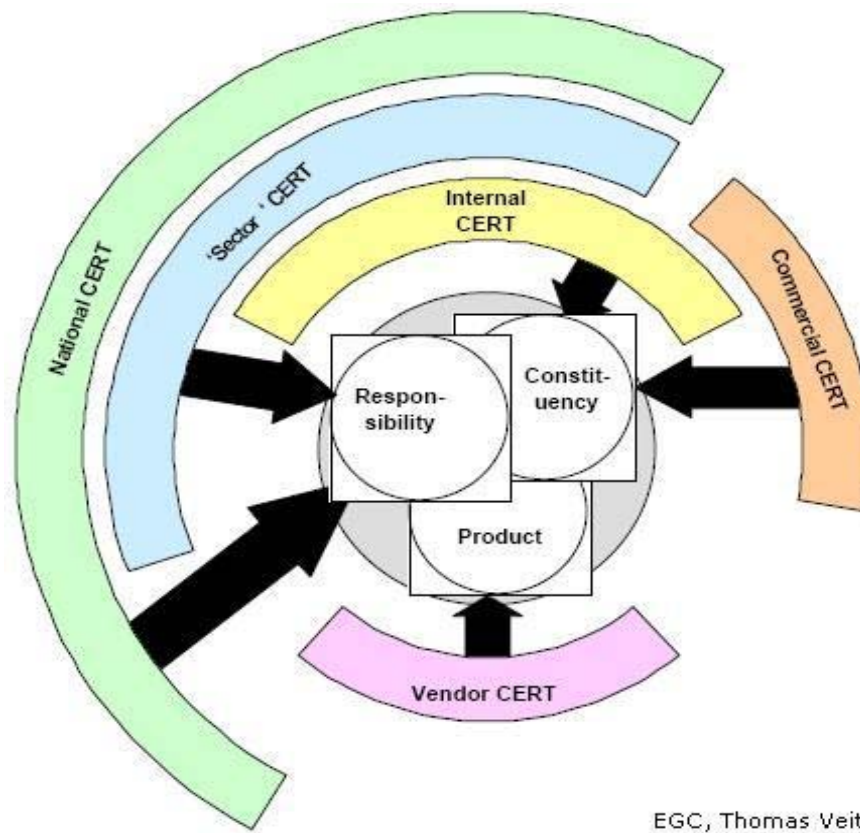

Figure 1.1: Ideal CERT Hierarchy and Relationship[3]

As can be seen from Figure 1.1, the national CERT is intended to coordinate the activities of the other internal CERTS, such as those of individual enterprises, of industry organizations, and NGO/semi-governmental organizational CERTs for different sectors of the economy. Vendor CERTs would be responsible for ensuring that state-of-the-art security is embedded in software, to prevent the spread of vulnerabilities. Commercial and internal CERTs would work together to disseminate best security practices to large enterprises. National and sector CERTs would collect and organize cybersecurity information, and coordinate active responses to major cyberseucrity threats or breaches.

2.2 Current Status and Breadth

In reality, the CERT security structure remains in its infancy in most countries that do have national CERTs, and the ideal CERT network (as explained above) is not even fully developed in the CERT's origin nation, the United States. Many countries do not have CERTs, but significant progress has been made over the past two decades in increasing the population of national CERTs and other CERT

---

3   http://www.first.org/resources/guides/cert-in-a-box/images/6.jpg

institutions in many countries with a large Internet user population or Internet-centric economy. While there is no authoritative centralized list of national CERT programs, the following list of 54 countries provides those that the authors have found. There are certainly other countries with some sort of cybersecurity teams, but these CERTs are more specifically national-level, cooperative, educating, and responsive organizations.

<u>Countries with National CERTs[4]</u>

- Argentina
- Bangladesh
- Canada
- Croatia
- Estonia
- Germany
- Hungary
- Indonesia
- Italy
- Lithuania
- Myanmar
- Philippines
- Qatar
- Singapore
- Sri Lanka
- Taiwan (ROC)
- Turkey
- United States

- Australia
- Brazil
- Chile
- Czech Republic
- Finland
- Greece
- Iceland
- Ireland
- Japan
- Malaysia
- Norway
- Poland
- Republic of Korea
- Slovenia
- Sweden
- Thailand
- UAE
- Uraguay

- Austria
- Brunei
- China (PRC)
- Denmark
- France
- Hong Kong
- India
- Israel
- Latvia
- Mexico
- Pakistan
- Portugal
- Russia
- Spain
- Switzerland
- Tunisia
- UK
- Vietnam

Table 2.1: Countries with National CERTs

Most large enterprises have dedicated IT security teams, some of which are called CSIRTs or even CERTs (but many of which are not).[5] These cybersecurity teams are often the targets of solicited surveys for collecting incident information and are the points of contact for dissemination of best practices and threat alerts.

2.3 General Data Availability from CERTs

---

4   From http://www.first.org/about/organization/teams/ and http://www.apcert.org/about/structure/members.html
5   Some examples can be seen here: http://www.first.org/about/organization/teams/

Many of the national CERTs collect information on a number of cybersecurity issues in their countries by year, quarter, or month. Information collection, in general, is conducted by surveys: organizations voluntarily (although often by solicitation) disclose attack types (placed on the organization) and defenses and shortcomings within the organization, etc. In addition, some CERTs have performed data collection through passive probes in their national networks. CERTs often aggregate these data to present nationwide reports on the state of cybersecurity during the reporting period, and trends over time. Some CERTs also ask institutions about their defenses and security technology, as well as request self-criticisms by institutions of their security readiness for different kinds of attacks, and policies, standards, etc, used by different institutions. The aggregated survey method has some interesting methodological artifacts that are worth noting. They are best described by two examples: if a single virus hits 1000 institutions (and they all report), then the virus is counted 1000 times. If 100 viruses hit a single enterprise, an "incident" reporting method will lead to 100 hits, where a "respondents" method will report only one hit (as a "respondents" method simply asks whether the respondent has experienced that specific problem in the reporting period.)

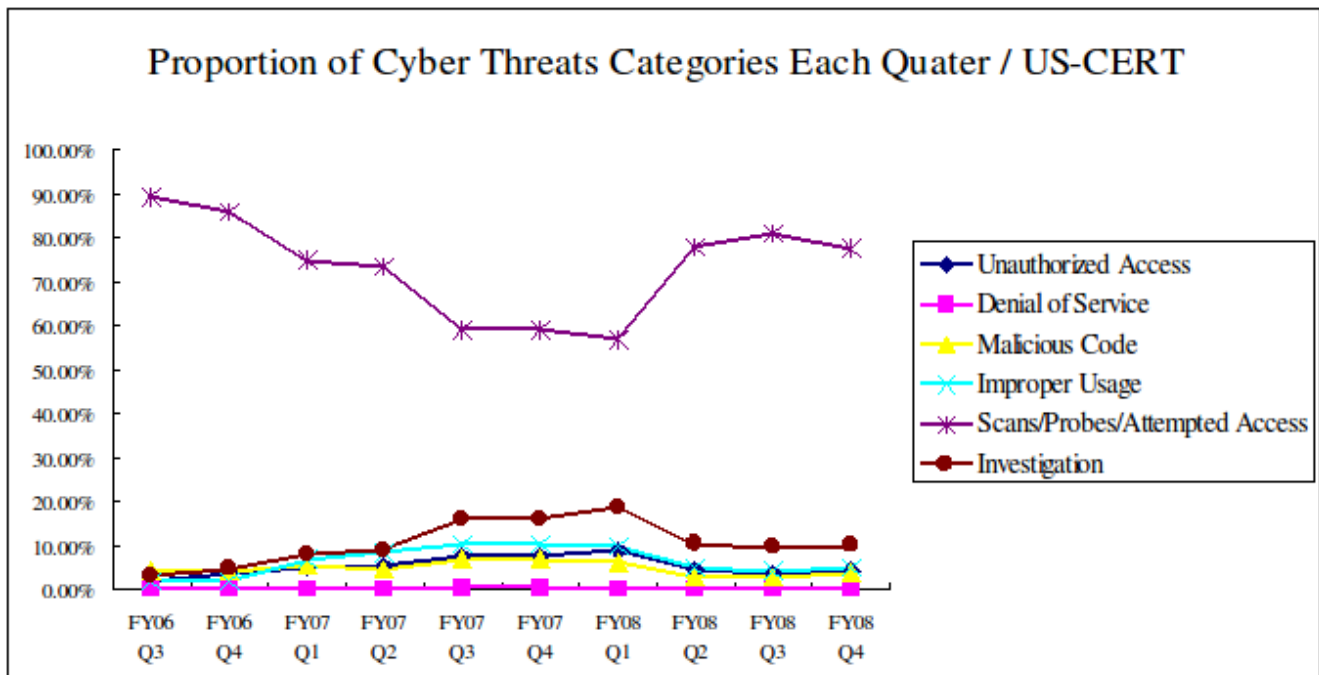An example graph from US-CERT is provided below and then briefly explained.

Figure 2.1: Proportional Threat Reports by Quarter to US-CERT[6]

While each CERT is usually consistent between reporting periods, data consistency between CERTs is limited. CERTs do not have a standardized typology of data: their surveys ask different questions and create different categories of attacks and vulnerabilities. CERTs lack a consistent data presentation method: some present data in absolute numbers of reports, others in percentages only. Term definition across CERTs is also sometimes inconsistent or unclear. Comparison and international aggregation are therefore often difficult, but there are a number of types of data that are commonly reported, in some

---

6 These types of attacks are the official US-CERT "Incident Category" designations, including "investigation," which designates an attack whose nature and source are still under investigation.

form or another:

US-CERT provides the most comprehensive and detailed definition of terms, as explained: "A *computer incident* within US-CERT is, as defined by NIST Special Publication 800-61, a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices."

There are six categories regarding computer incidents used by US-CERT.

CAT 1 -- *Unauthorized Access*: In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resources.

Other reports by US-CERT further elaborate on this definition:

"Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner…The specifics are different for each individual event but it could happen in any number of ways. Usually access is gained via unpatched software or other known vulnerabilities." ("Unauthorized Access")

"Unauthorized access" entails approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent. These laws relate to either or both, or any other actions that interfere with computers, systems, programs or networks." ("Computer Hacking and Unauthorized Access Laws.")

CAT 2 -- *Denial of Service (DoS)*: For example: Downloading files causes a significant amount of traffic over the network. This activity may reduce the availability of certain programs on your computer or may limit your access to the internet. ("Cyber Security Tip ST05-007")

"A 'denial-of-service' attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service , attempts to disrupt service to a specific system or person (…) Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack. Illegitimate use of resources may also result in denial of service. For example, an intruder may use your anonymous ftp area as a place to store illegal copies of commercial software, consuming disk space and generating network traffic.

There are three basic types of DoS attack:
- 1) consumption of scarce, limited, or non-renewable resources
- 2) destruction or alteration of configuration information
- 3) physical destruction or alteration of network components"

CAT 3 -- *Malicious Code*: *Successful* installation of malicious software (e.g., virus, worm, spyware, bot, Trojan horse, or other code-based malicious entity that infects or affects an operating system or application). The intent of such malicious code is often to take control of the computer or destroy or change information stored on the computer. Agencies are *not* required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.

CAT 4 -- *Improper Usage*: Violation of acceptable usage policies (as established by the enterprise).

CAT 5 -- *Scans, Probes, or Attempted Access*: any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.

CAT 6 -- *Investigation*: *Unconfirmed* incidents of potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

These definitions are not shared universally by other CERTs, but certainly provide a relatively authoritative guide to what statistical data represents.

There are a few methodological concerns beyond incompatibilities that are worth noting. The survey style of information reporting on the part of CERTs means comparisons between nations with otherwise compatible data definitions and typology is difficult. Numerical comparisons can be misleading if the breadth of a survey is not explicitly clear—if both countries survey very different proportions of the population, then their absolute numerical data will be incomparable (though percentages may remain comparable). Additionally, even if survey respondents are relatively accurate, most respond on behalf of institutions—there may be disproportionate weights placed upon different institutions if response rates are significantly different. It is further unclear whether an incident at a large institution should be counted the same way as an incident at a smaller one.

3 Examples of Specific Data Provided by Some CERTs

Here we explore data available at select CERTs, including type of vulnerability/threat, frequency of publication, and other relevant information. A table below concisely displays relevant information about the data available at each CERT. Note that not all reports by national CERTs have quantitative data available.

Country / Region	Reporting Period	Data Presentation	Data Categories	Formation Date
Asia-Pacific (Regional)	Annual			?
Australia	Annual	Percentage	Many	?
Brunei	None	N/A	N/A	05/01/04
Bangladesh	None	N/A	N/A	07/01/07
China	Semi-Annual	Numerical	Website Malicious Code, Spam, Virus/Worm/Trojan, Phishing, Vulnerabilities, Botnet, DoS Attack	10/01/00
Hong Kong	Annual	Numerical	Website Alerts, Virus Alerts, Virus Incidents	?
Indonesia	Occasional	Numerical?	?	?

India	Monthly	Numerical	Scanning, Malicious Code, Spamming, Phishing, SQL Injection, Website Compromise / Malware Injection	?
Japan	Quarterly	None	N/A	?
Korea	Monthly	?	<Data Corrupted>	07/01/96
Malaysia	Occasional	Numerical	DoS Attacks, Viruses/Malicious Code, others	01/13/97
Pakistan	Occasional	?	Defacement, others?	?
Myanmar	Unknown	N/A	(No Website)	?
Philippines	Unknown	N/A	(No Website)	?
Qatar	None	None	None	?
Russia	Yearly	Numerical	Malware, Phishing, DoS, Unauthorized Access, Scan/Password Bruteforcing, Others	?
Sri Lanka	None	None	None	06/01/06
Singapore	None	None	None	10/01/99
Taiwan	None	None	None	09/01/87
Thailand	None	None	None	2000
Vietnam	None	None	(No English Version)	12/01/05
Canada	None	None	(No Website)	?
USA	Quarterly	Percentage	Unauthorized Access, DoS, Malicious Code, Improper Usage, Scans/Probes/Attempted Access, Under Investigation	11/01/88
Mexico	Unknown	N/A	(No English)	?
Argentina	None	None	None	05/01/99
Brazil	Quarterly	Numerical	Worm, Spam, Scanning, DoS, others	?
Austria	None	None	(No English)	?
Belgium	None	None	None	?
Croatia	None	None	None	?
Czech Republic	None	None	None	1996
Denmark	None	None	(No English)	?
Estonia	Yearly	Percentage	Computer Viruses, Personal Data Abuse, Spam, others	2005
Finland	None	None	None	?
France	None	None	None	?
Germany	Occasional	None	None	?
Greece	None	None	(No English)	?
Hungary	None	None	None	?

Iceland	None	None	(No Website)	?
Ireland	None	None	None	?
Israel	None	None	None	?
Italy	N/A	N/A	(Must be registered for statistics)	1994
Latvia	Occasional	Numeric	?	?
Lithuania	Yearly	?	?	?
Netherlands	None	None	None	?
Norway	Monthly	None	None	?
Poland	None	None	(No Website)	1993
Portugal	Monthly	None	(No English)	?
Slovenia	None	None	None	?
Spain	Yearly	Numeric	"Vulnerabilities"	?
Sweden	None	None	None	?
Switzerland	?	?	Internet Background Noise	1987
Turkey	None	None	None	?
UK	None	None	None	?

Table 3.1: Selected National CERT PubliclyAvailable Data

To illustrate the types of CERT data available, examples are provided below. These examples are provided largely to emphasize the diversity of data available at CERTs across the world (and, similarly, inter-CERT data inconsistency). The five national CERTs chosen below are the United States, China, India, Russia, and Estonia.

3.1 US-CERT

The United States national CERT is affiliated with the Department of Homeland Security, and is a distinctly different entity from CERT/CC at Carnegie Mellon University (which is an independent and academic entity). These two largest US CERTs share information and, in the case of a large-scale attack, will often coordinate extensively in leading a response.
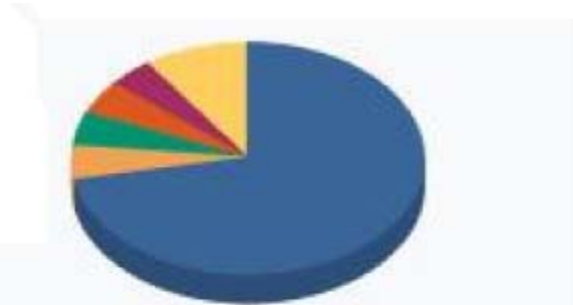
Examples of information provided is shown in Figures 3.2, 3.3, and 3.4.

2008 Q4

■ Unauthorized Access	4.1%
■ Malicious Code	3.6%
■ Improper Usage	5.0%
■ Scans, Probes & Attempted Access	77.3%
■ Under Investigation / Other	10.0%
Total:	100.0%

Figure 3.2: US-CERT - Incidents by Category, 2008 Q4[7]

■ Phishing	71.8%
■ Malicious Web Site	4.8%
■ Non Cyber	4.8%
■ Policy Violation	4.7%
■ Suspicious Network Activity	4.1%
■ Others	9.8%
Total:	100.0%

Figure 3.3: US-CERT - Top 5 Incidents vs. Others, 2008 Q4[8]

7   US-CERT Quarterly Trends and Analysis Report Nov 7th, 2008 (http://www.us-cert.gov/press_room/trendsanalysisQ408.pdf)

8   US-CERT Quarterly Trends and Analysis Report Nov 7th, 2008 (http://www.us-cert.gov/press_room/trendsanalysisQ408.pdf)
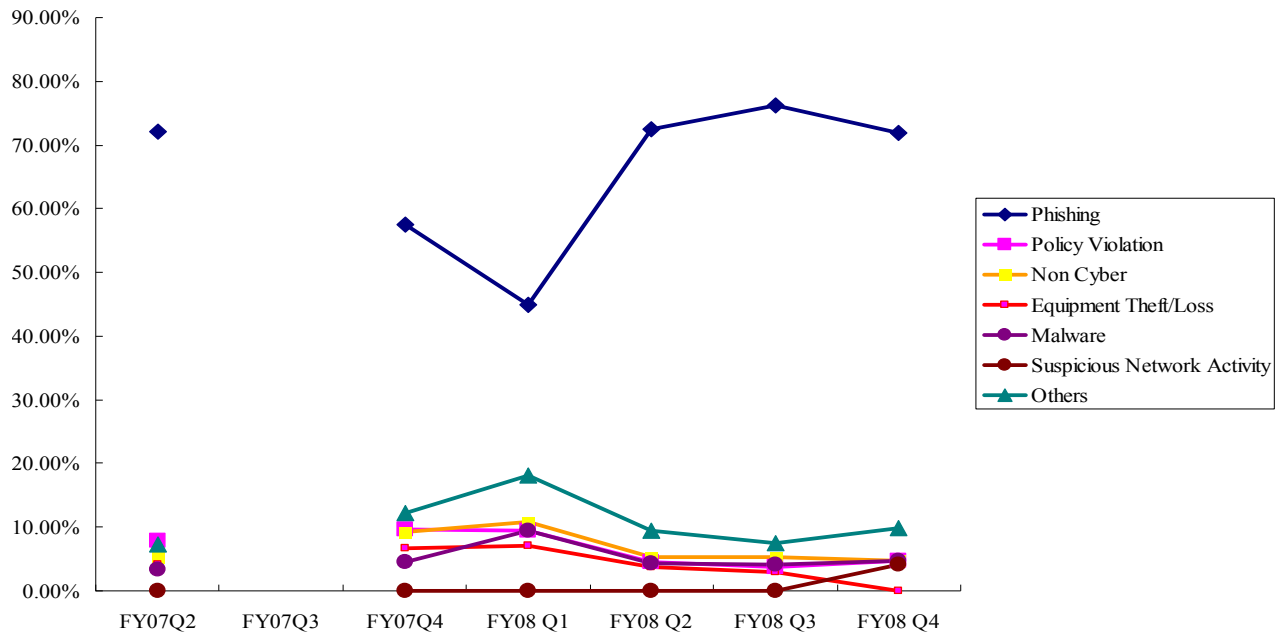
Figure 3.4: US-CERT - Percentages of Top 5 Incidents vs. Others, 2007 Q2 – 2008 Q4[9]

The charts and graph above suggest that the greatest threat by frequency to US institutions and users is some form of attempted information access, namely phishing. The vast majority of threats reported to US-CERT are related to attempts to deceive the user (phishing, malicious website, non-cyber) rather than direct attacks against the defenses of the computer or the network. Figure 3.2 breaks down reported incidents by official US-CERT category; Figures 3.3 and 3.4 describe more specific attacks (each attack falling into one of the official categories). As can be seen, most "Scans, probes, and attempted access" attacks are phishing. Comparing the two graphs, we see that phishing (at 72% of all incidents) makes up the vast majority of attempted access attacks (at 77% of all incidents), suggesting that by far, most access attempts attack the user rather than the software or hardware directly.
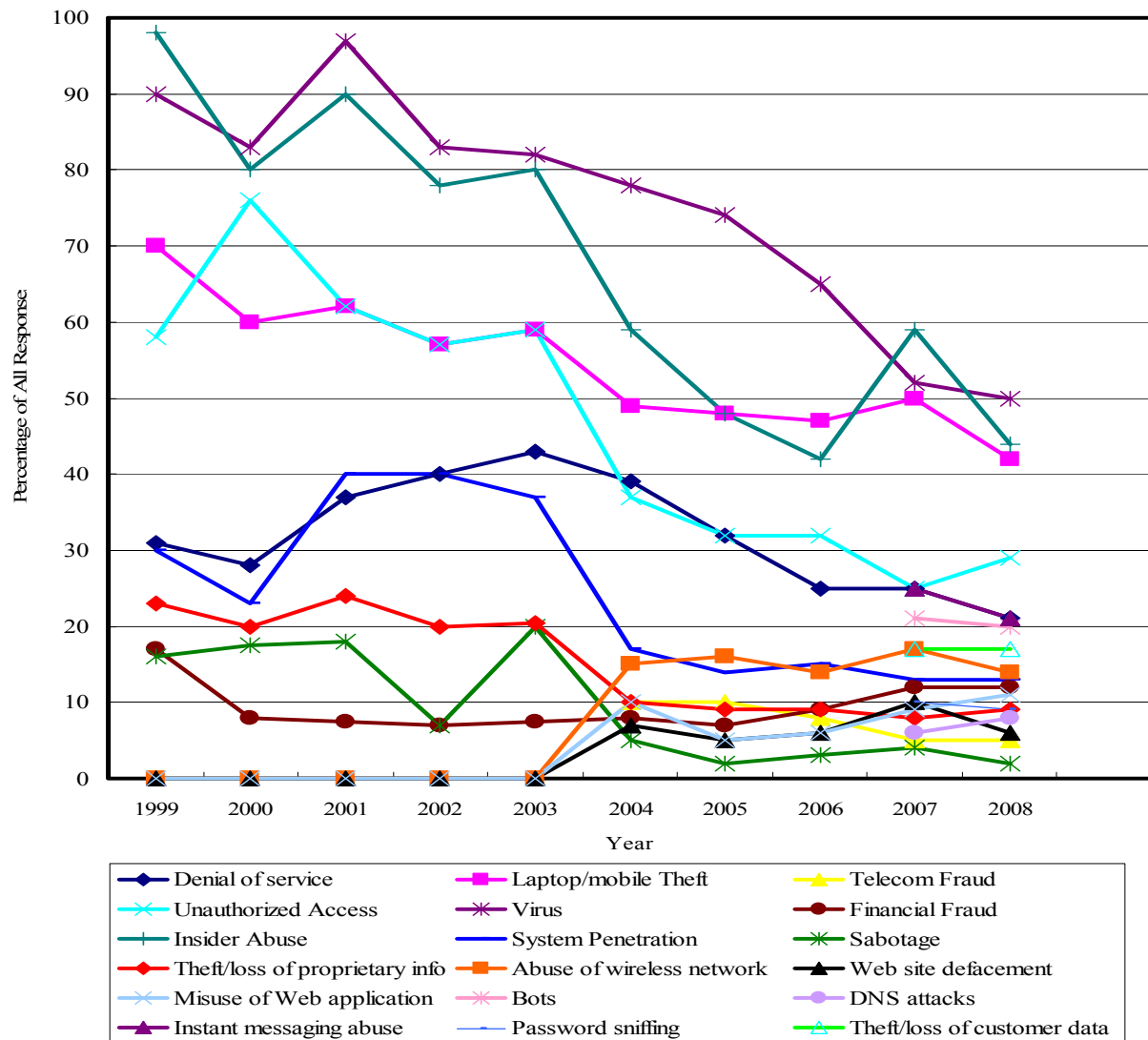

Figure 3.5: US-CERT - Types of Detected Misuse, by Year[10]

Figure 3.5 describes different sub-categories of misuse of enterprise computing equipment, which can lead to any of the US-CERT categories of attacks. Above we observe a general decline in the most pervasive of misuses over the past 5 years, including viruses, insider abuse, mobile theft, unauthorized access, and denial of service attacks. Proportional increases are seen in a number of "misuses" occur in 2004, which suggests (although we have no confirmation of) their addition to the reporting and collecting mechanisms by US-CERT, rather than sudden onset of their use. Because the above statistics represent a percentage of all respondents (rather than a percentage of all incidents reported), the decline in largest misuses (including viruses, insider abuse, mobile theft, unauthorized access, etc) may be due to an actual reduction in the incident as a problem, suggesting that IT professionals and companies in the US may be responding well to the most prevalent security threats.

---

10   2008 CSI Computer Crime & Security Survey (http://i.zdnet.com/blogs/csisurvey2008.pdf) and 2005 CSI/FBI Computer Crime and Security Survey (http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf)

3.2 CN-CERT (China)

Examples of the China CERT (CN-CERT) national-level data is shown below.
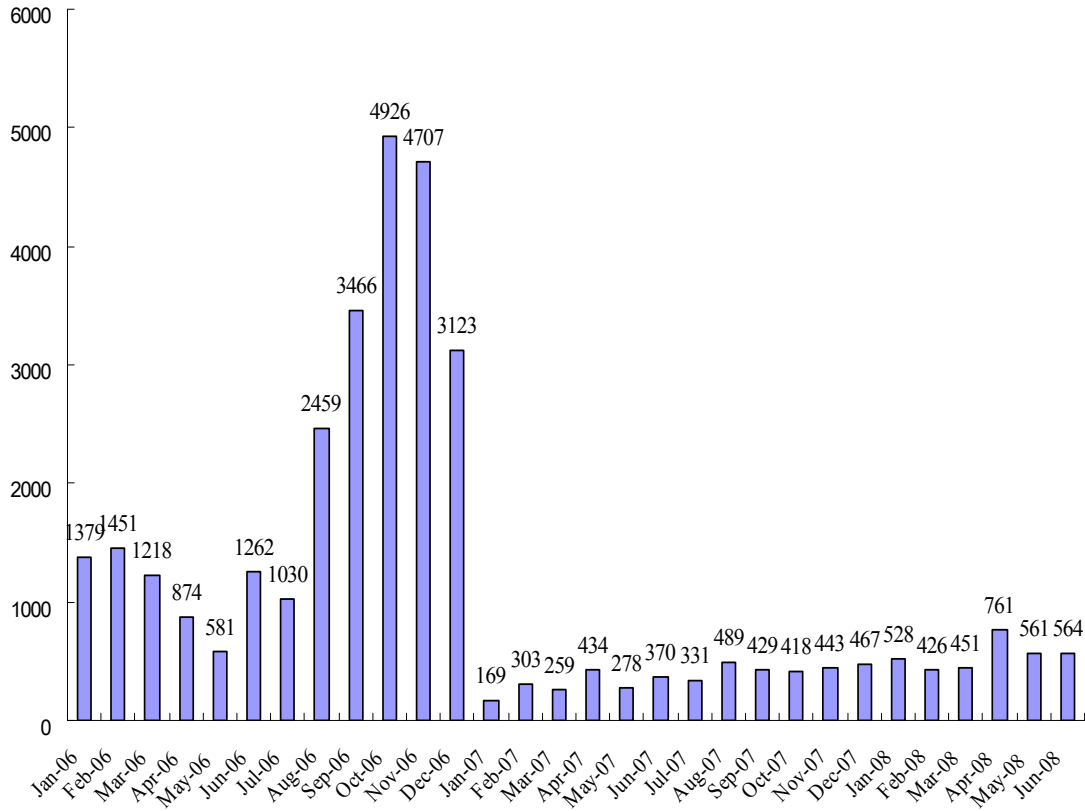

Figure 3.6: Total Incidents Reported to CN-CERT (not including Scanning), Jan 2006 – June 2008[11]
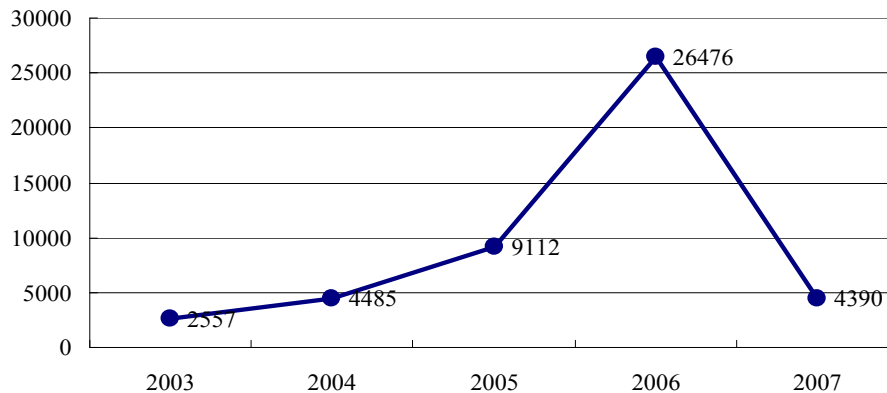

Figure 3.7: Total Incidents Reported to CN-CERT (not including scanning) by Year, 2003-2007[12]

---

11   China-CERT Report   (http://www.cert.org.cn/articles/docs/index.shtml)
   Note: Incident reporting changed in January 2007 to no longer include CN-CERT detection, only voluntary reporting,
   leading to the significant drop in reports.
12 China-CERT Report   (http://www.cert.org.cn/articles/docs/index.shtml
   Note: Incident reporting changed in January 2007 to no longer include CN-CERT detection, only voluntary reporting,

At least until 2006, we observe a dramatic (and perhaps exponential) growth in incidents. After 2006, due to the change in reporting structure of CN-CERT, the trend is difficult to follow. This growth in absolute number of incidents is likely at least as much due to an explosion in Internet users in China as it is due to an increase in vulnerabilities.
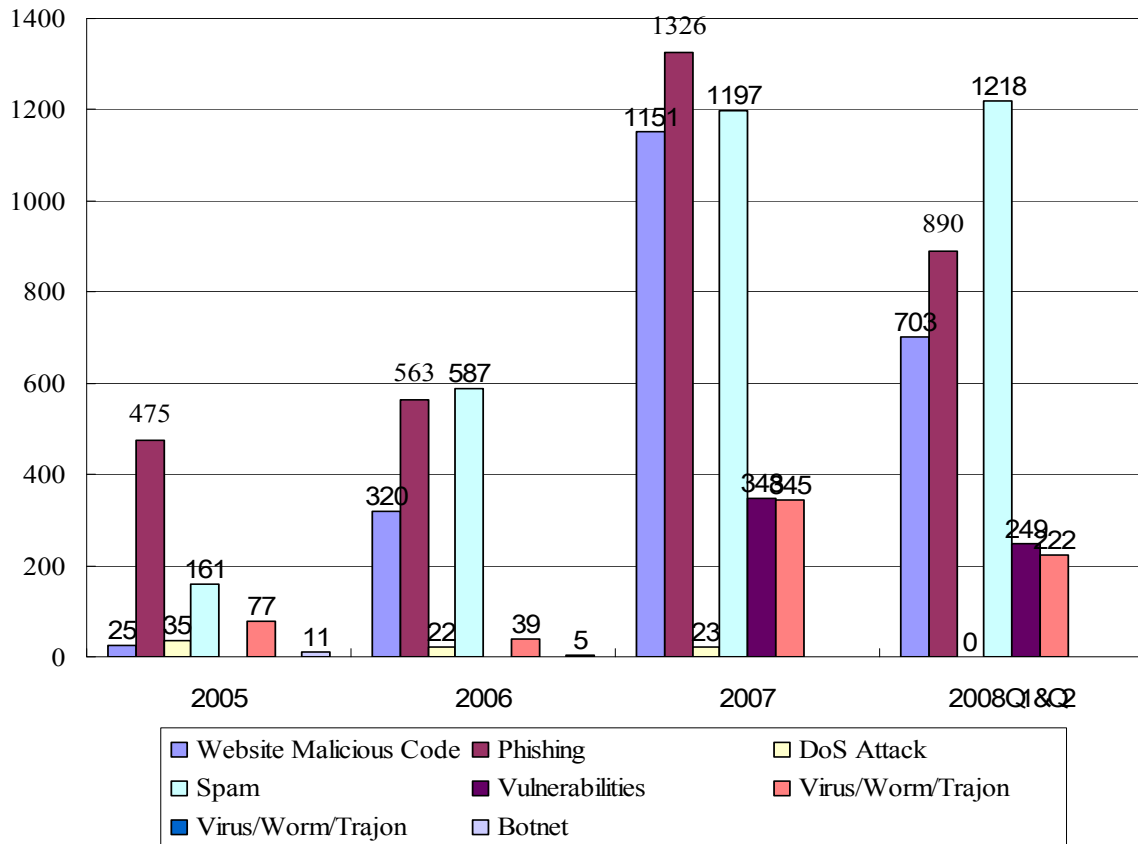

Figure 3.8: CN-CERT – Selected Events per Year, 2005 – 2007[13]

Here we observe a dramatic proportional increase in botnets and spam as reported by CN-CERT. Such attacks typically represent organized for-profit ventures rather than purely destructive attacks, and usually target users, rather than technical defensive network capabilities. Denial of Service attacks actually decline from few to literally none in the first half of 2008, suggesting either a reporting bias or an increase in (already extensive) government cybersecurity defensive effectiveness.

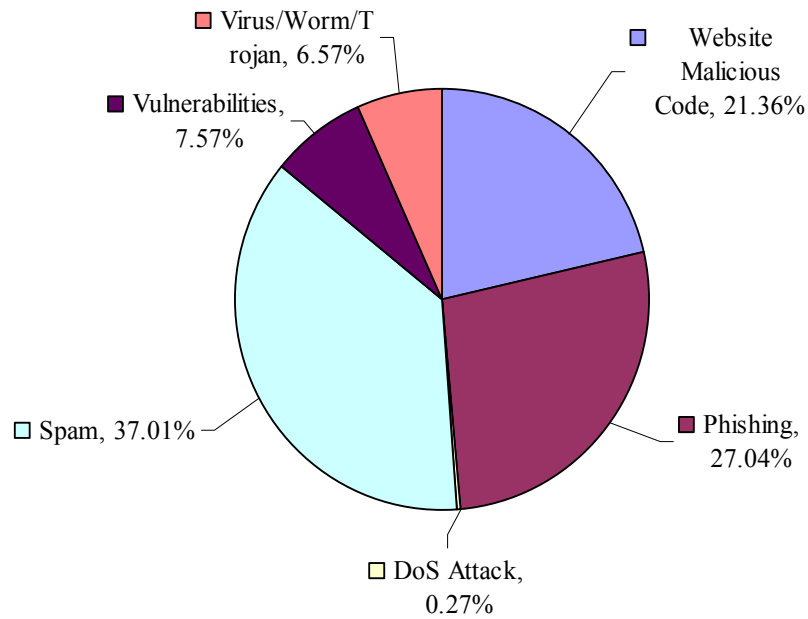---

leading to the significant drop in reports.

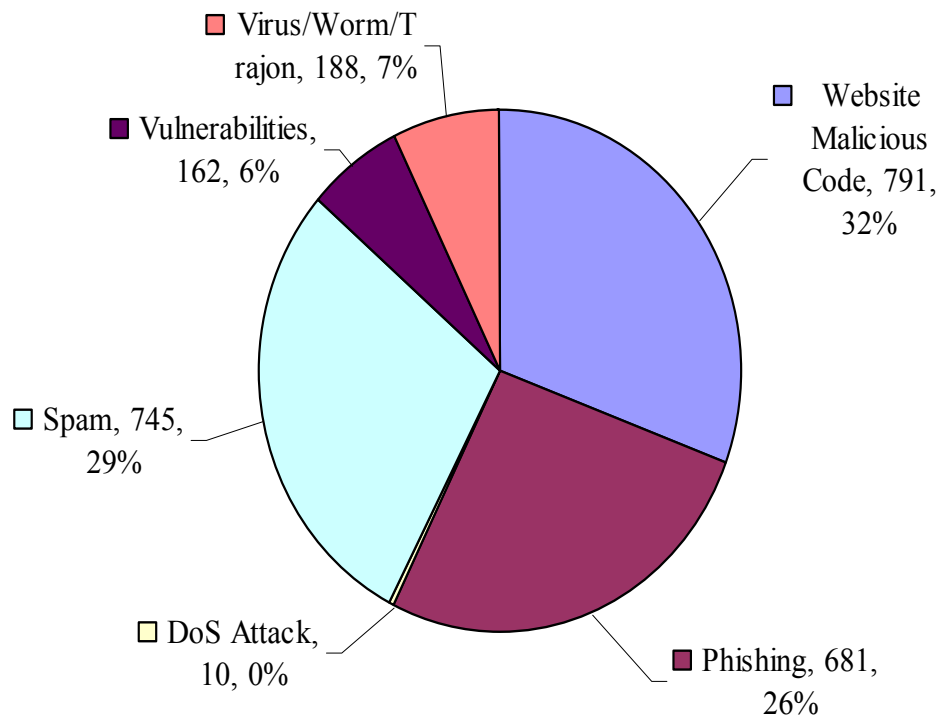Figure 3.9: CN-CERT Distribution of Incidents by Category, 2008 Q1 & Q2[14]

Figure 3.10: CN-CERT Distribution of Incidents by Category, 2007 Q3 & Q4[15]

---

14 China-CERT Report 2008 Q1 and
    Q2   (http://www.cert.org.cn/UserFiles/File/CISR2008fh.pdf1.pdf)
15 China-CERT Report 2007 and 2007 Q1 & Q2 (http://www.cert.org.cn/servlet/Articles?channel=docs&for=0&page=2)
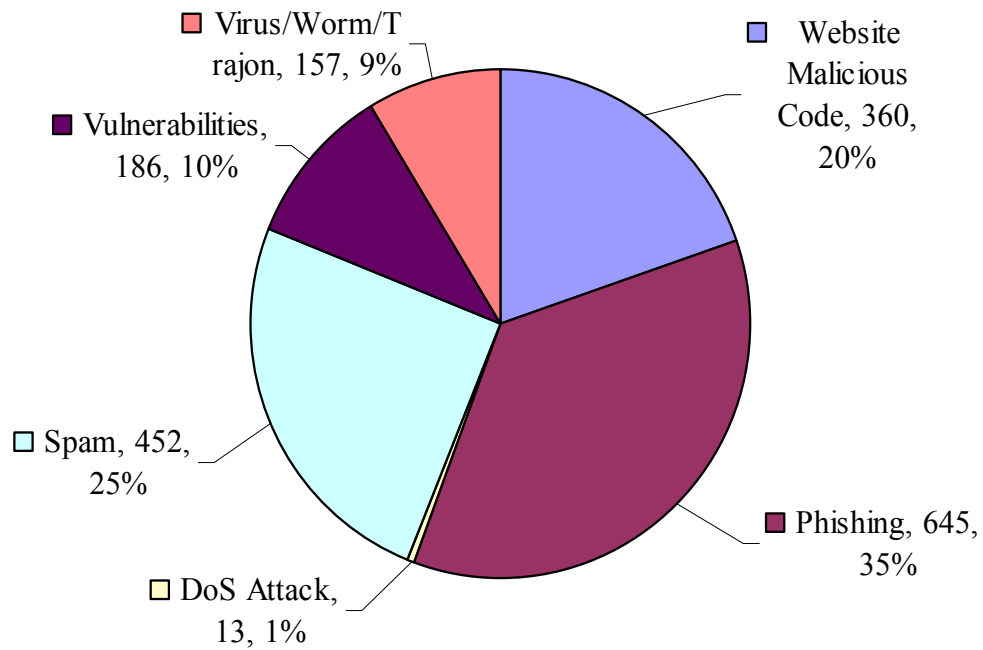
Figure 3.11: CN-CERT Distribution of Incidents by Category, 2007 Q1 & Q2

Throughout 2007 and into 2008, the primary trend observed is a relative increase in spamming; phishing decreases proportionally to some extent, and malicious website code increases briefly and drops again.
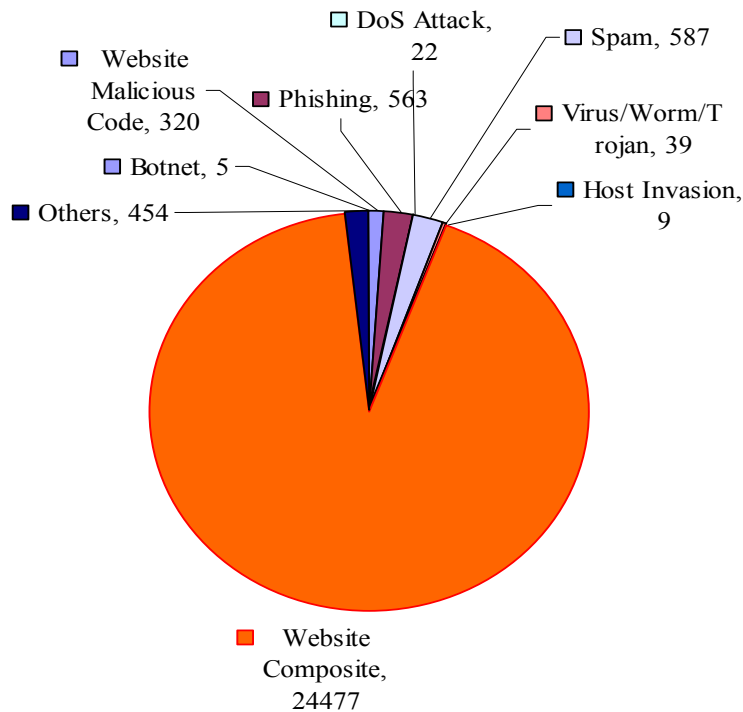
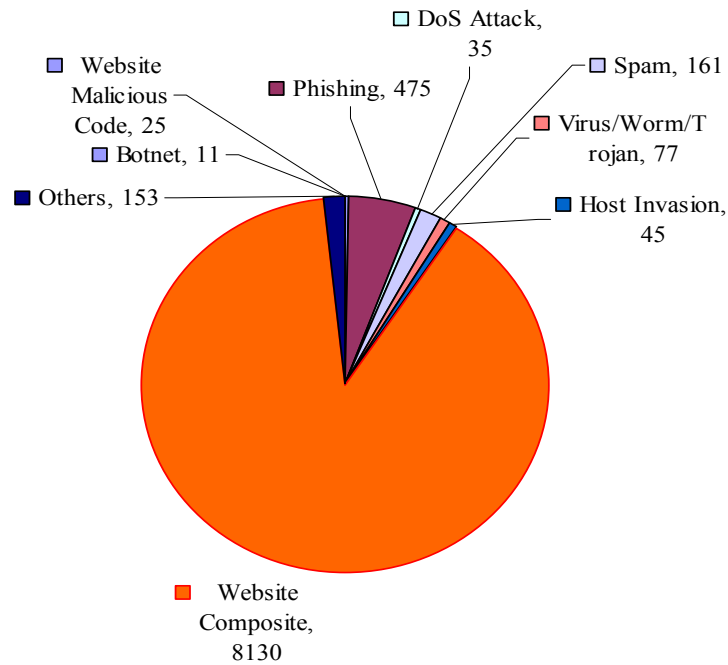Figure 3.12: CN-CERT Distribution of Incidents by Category, 2006[16]

Figure 3.13: CN-CERT Distribution of Incidents by Category, 2005[17]

Between 2006 and 2007, CN-CERT changed its reporting methodology, removing "Website Composite" from the list of reported incidents on distribution charts. This removal allows the reader to more easily observe trends after 2006, though a significant proportional increase in spam and a proportional decrease in phishing through the 2005-2007 period.
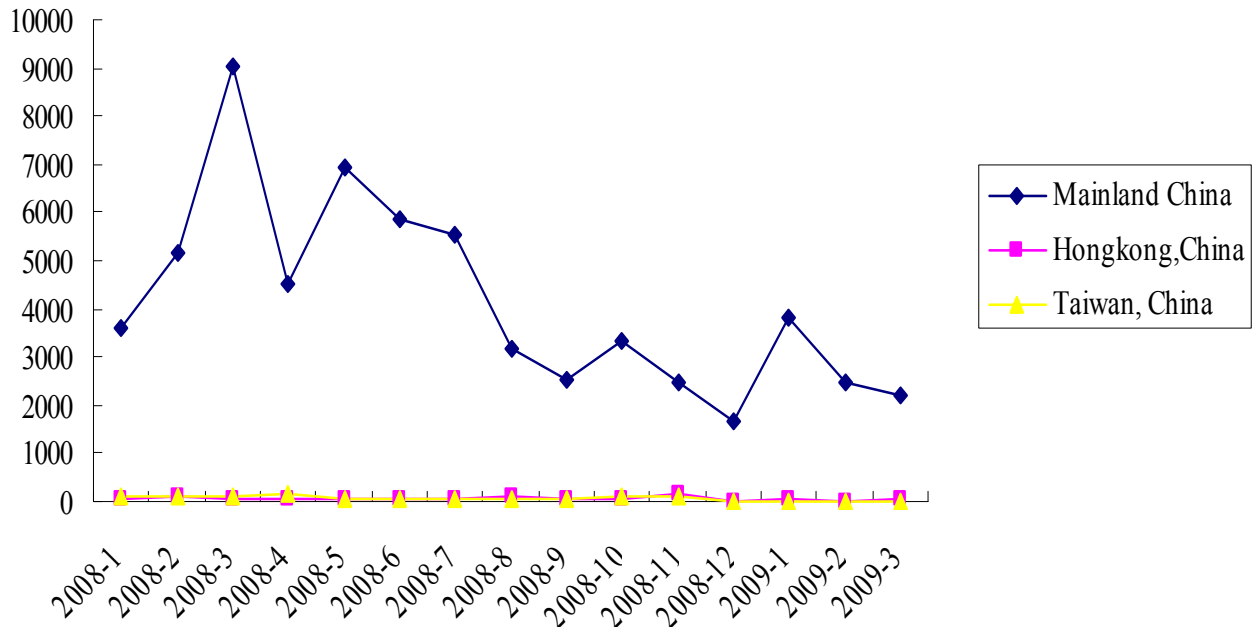
16   China-CERT Report 2007 Q1 and Q2
    (http://www.cert.org.cn/UserFiles/File/2006CNCERTCCAnnualReport_Chinese.pdf)
17   China-CERT Report 2005 (http://www.cert.org.cn/upload/2005CNCERTCCAnnualReport_Chinese.pdf)

Figure 3.14: CN-CERT – Websites Attacked in China by Quarter, 2008 Q1 – 2009 Q3[18]
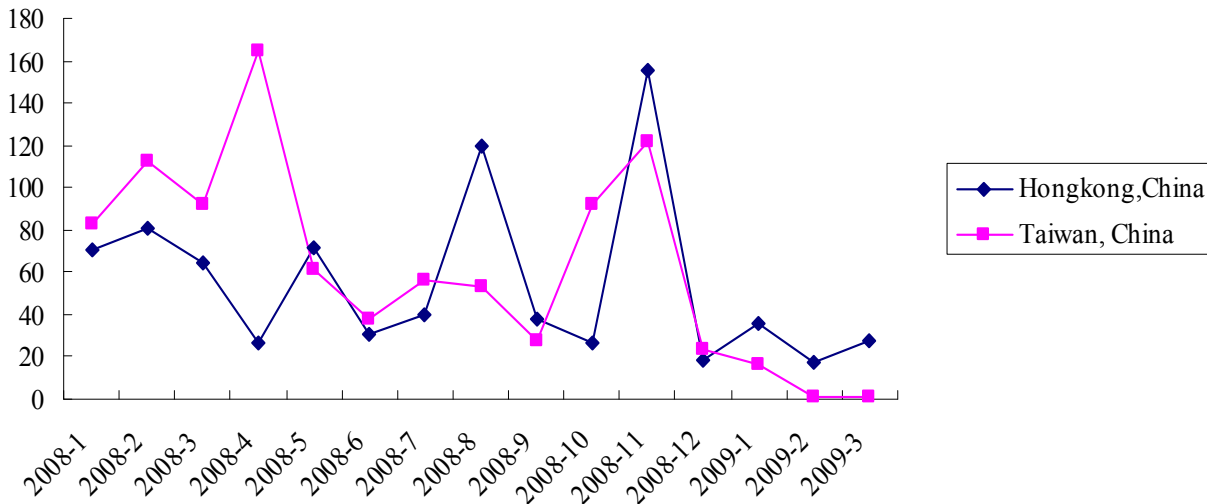
Figure 3.15: CN-CERT – Websites Attacked in Hong Kong and Taiwan by Quarter, 2008 Q1 – 2009 Q3

Over the relatively short period in the above graphs, we observe a downward trend in website attacks in Mainland China, which may be due to increased sophistication in government control. Hong Kong and Taiwan also seem to show a gradual downward trend in attacks, though the trend is not as sharp as in the mainland.

3.3 CERT-IN (India)

Examples from CERT-IN are presented below:
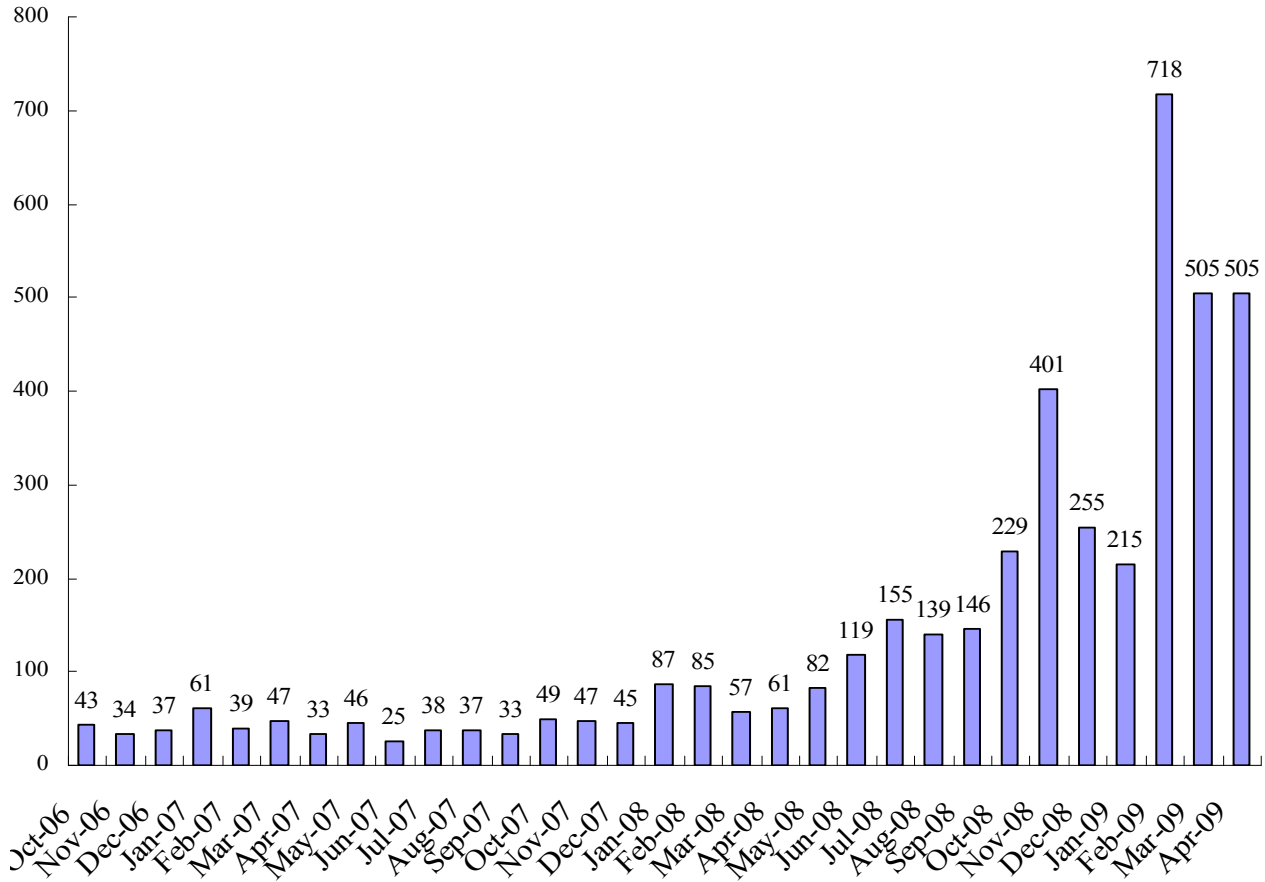
Figure 3.16: CERT-IN – Total Reported Incidents by Month, October 2006 – April 2009[19]

Here we observe a marked and rapid increase in total reported incidents, starting in 2008, with spikes in December 2008 and March 2009. The long-term increase may be due to increases in reporting, vast increases in Internet usage, increases in attacks, or any combination of the three.

---

19   CERT-In Monthly Security Bulletin: (http://www.cert-in.org.in/knowledgebase/SecurityBulletin/)
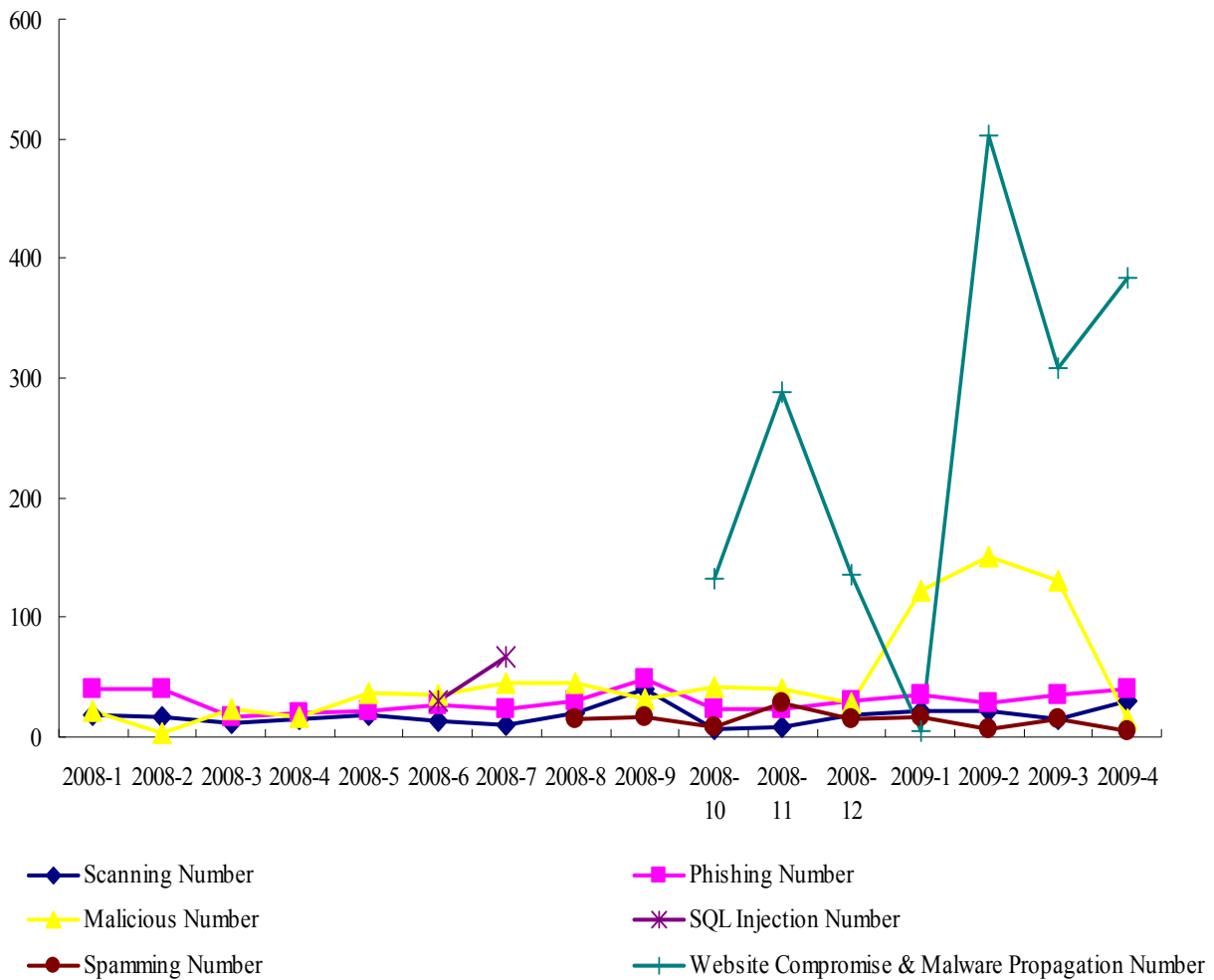
Figure 3.17: CERT-IN – Incidents by Category by Month, January 2008 – April 2009[20]

This graph suggests that most incidents reports are on the rise (which is to be expected), except for spamming, which appears to be slowly decreasing over time, suggesting potentially increased spamming defenses (like spamscreens) in deployment. It also suggests that malicious code and website compromise / malware propagation are the major forms of attack in India. It should be noted that this is quite different from the United States, where Phishing is the major reported attack.

---

20   CERT-In Monthly Security Bulletin: (http://www.cert-in.org.in/knowledgebase/SecurityBulletin/)
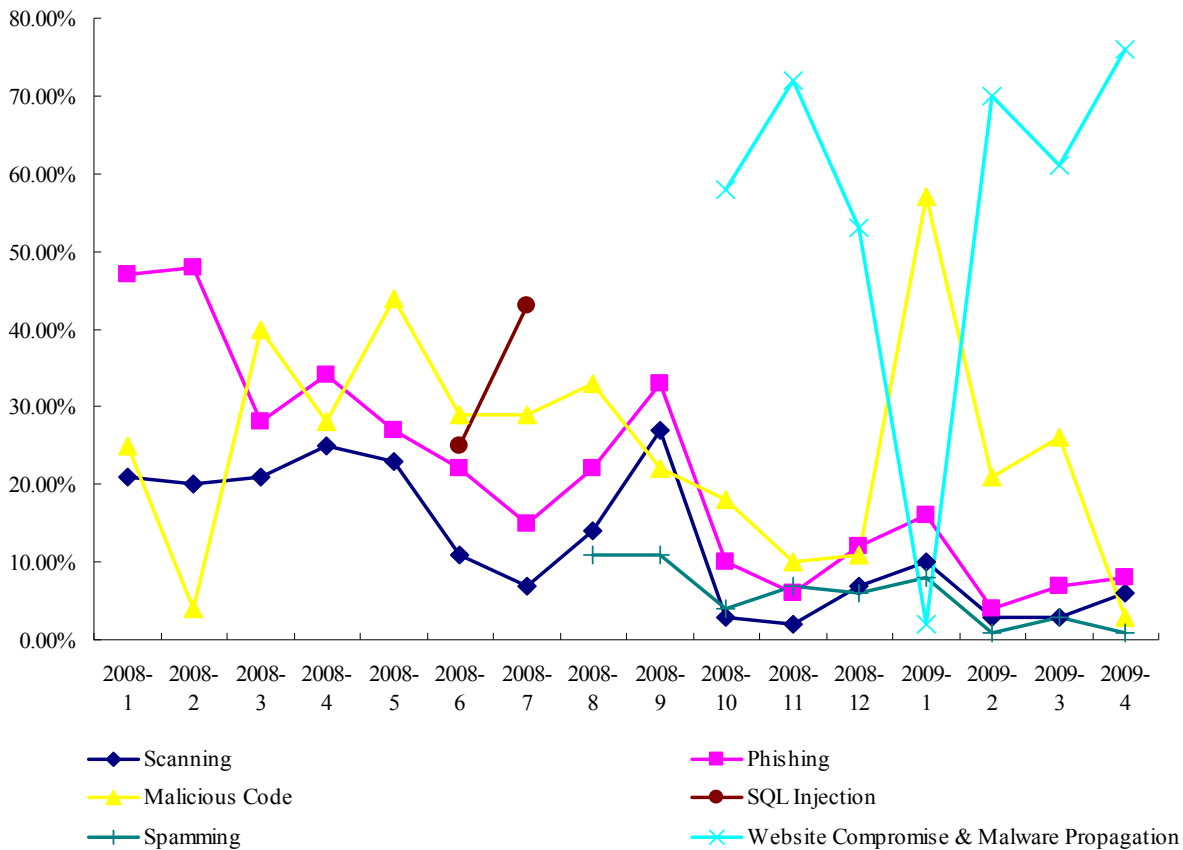
Figure 3.18: CERT-IN - Proportional Incidents by Category by Month, January 2008 – April 2009[21]

In the Figure 3.18 we observe a more marked reduction in the percentage of Phishing, Scanning, and Spamming over time, suggesting that user-oriented attacks have decreased in general. A significant spike (both in "Malicious Code" and "Website Compromise & Malware Propogation") in January 2009 suggests an anomaly in reporting or recording, leading to the two (admittedly similar) concepts to be switched, though a simple coincidence is possible. Either way, by 2009, attacks on software infrastructure, rather than direct attacks on users, appear to dominate cybersecurity issues in India.

3.4 Russia CERT

We provide a few examples of data from Russia CERT below:
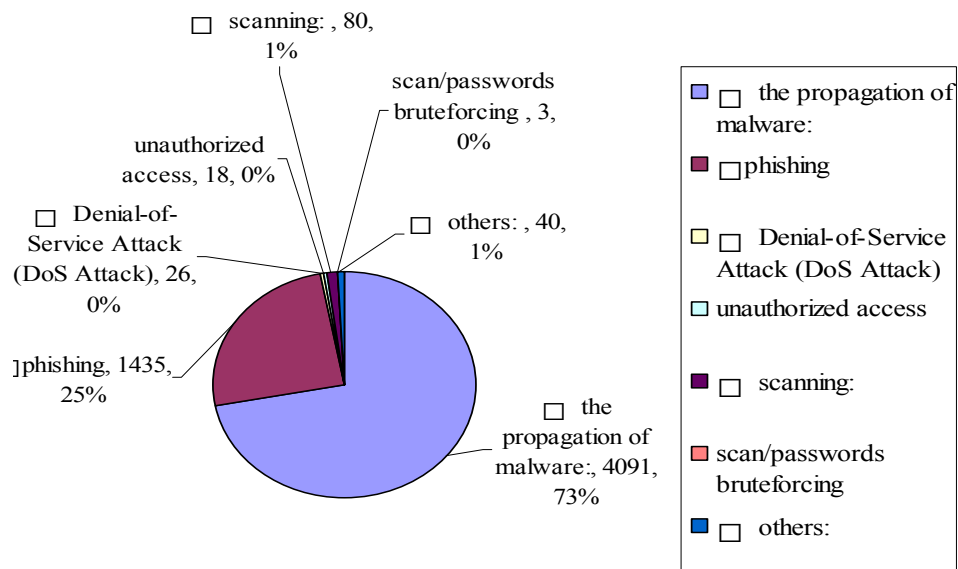
Figure 3.25: Russia CERT – Proportion of Incidents by Type, 2007[22]
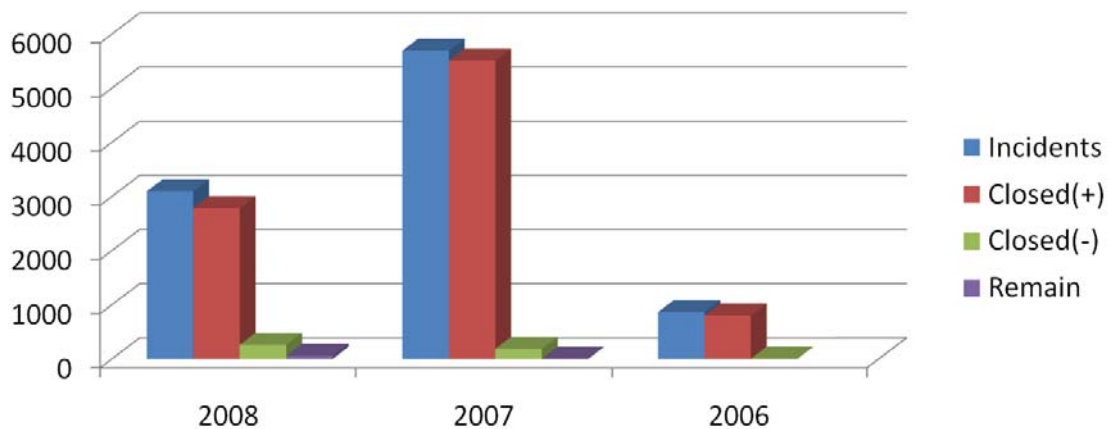
Figure 3.26: Russia CERT – Incidents Reported by Status, 2006-2008[23]

The above graphs indicate that in Russia, user-centered attacks like malware and phishing are high proportions of reported incidents, much like the United States (and unlike India).

---

22 http://www.cert.ru/stat.html (originally in Russian)
23 http://www.cert.ru/conference2008.html
   Note: Best interpretation suggests that "Closed(+)" indicates an incident that was resolved to satisfaction; "Closed(-)" indicates an incident that was resolved unsatisfactorily; "Remain" indicates incidents that remain unresolved.

3.5 CERT Estonia

CERT Estonia, established in 2006, is young, particularly interesting, due to its involvement in constant low-level (and occasionally high-level) cyberwar presumably with Russia. The data examples below are from the Estonian RISO State Information Office[24]:
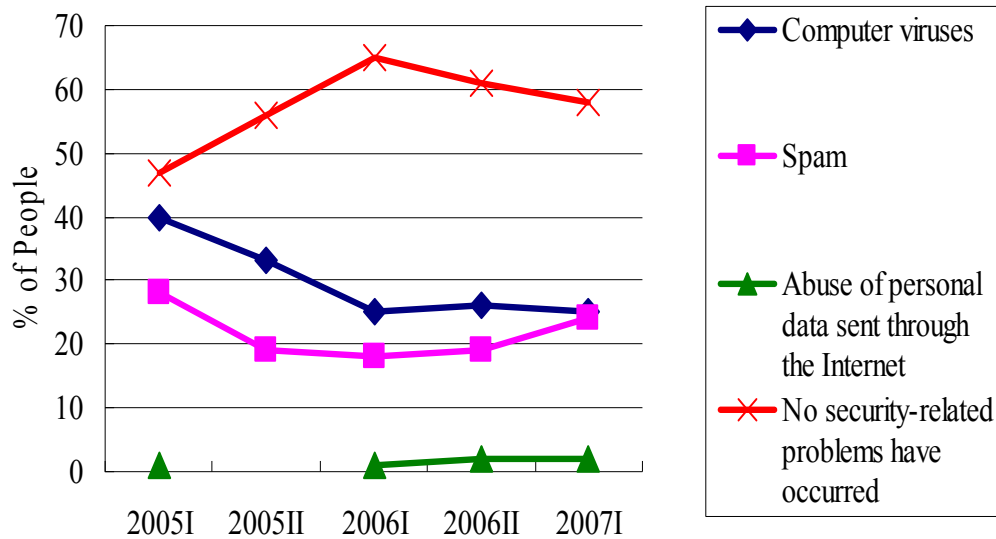
Figure 3.27: CERT Estonia – Security Problems by Type, as a Percentage of Internet Users, 2005-2007[25]

The above graph shows a slightly different story in Estonia than the US or China. Computer viruses take up a much larger proportion of cybersecurity incidents—a larger proportion than even spamming. Reporting methodology may be to blame for this discrepancy: specifically, the survey refers to "security problems" for a particular user—many may not consider spamming a serious "security problem" even if they are spammed. Most users report having had no problems, which may suggest that most indeed had no major problems, or that standards for security in personal users are more lax.

---

24 For more information on RISO, see http://www.riso.ee/en

25 TNS Emor e-Track survey, http://www.riso.ee/en/files/eSeire_uuringu_internet_security_2007_I_ENG_2005-2007.pdf
   Note: "I" indicates the first half of the year; "II" indicates the second.
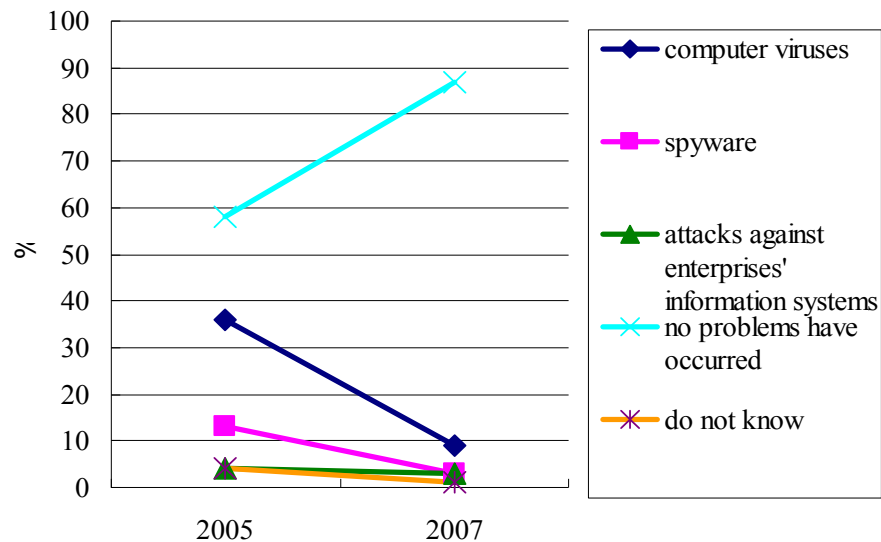
Figure 3.28: CERT Estonia – Security Problems by Type, as a Percentage of
Corporate Enterprises, 2005 – 2007[26]

The above graphs reveal that the majority of enterprises in Estonia report that no serious problems have occurred, and that the trend seems to be relatively positive. This is somewhat surprising, given the widely reported spree of denial-of-service (DOS) attacks against websites in Estonia during April and May of 2007[27], possibly this reporting does not capture all such events, especially against government web sites.

Furthermore, corporate enterprises seem to report an even lower proportion of security incidents than personal users, though it should be noted that the categories reported are significantly different, making the two results difficult to compare. Furthermore, the lack of differentiation between number of attacks on corporate enterprises leaves open the distinct possibility that certain enterprises are attacked often and deliberately, where others are not high-priority targets to attackers. We do not know if the 10-40% of attacked enterprises were attacked once or a hundred times.

---

26   TNS Emori uuring "Info - ja kommunikatsioonitehnoloogia kasutamine Eesti ettevõtetes
      http://www.riso.ee/en/files/Emor_Computer_Security_2007_I_2005-2007.pdf
27   BBC NEWS, "Estonia fines man for 'cyber war'" Jan 25, 2008 ... A 20-year-old Russian man is the first person to
      be convicted for taking part in cyber attacks against Estonia, reported by news.bbc.co.uk/2/hi/technology/7208511.stm

3.6 Summary

These examples illustrate a number of interesting key points, some of which will be discussed in more detail later. First, the nature of cybersecurity issues varies widely between different countries, in sometimes surprising ways. Estonia seems to have a surprisingly low number of incidents per enterprise capita, particularly given its history with Russia. The predominant type of threat in China and the United States is against the user directly—phishing, spamming, improper usage, and other attempts to trick the user into compromising his own security; in Russia and India, malware and malicious code attacks are more common, and there is no clear explanation as to why.

Second, reporting methods vary significantly between different CERTs. No two CERTs above reported information in the same way; variations in incident or threat definitions, in typology, in frequency and chronological scale, and in reporting methodology (some CERTs report by total number of reports, some by proportion of total incidents, some by proportion of respondents). These inconsistencies make cross-country comparisons (and, presumably, information coordination) challenging – though trends over time might be identifiable.

4. The ECIR Data Dashboard

4.1 Purpose

The ECIR Data Dashboard is developed to provide historical trend data as well as current statistics and news to policymakers, academics, IT professionals, and other stakeholders. By consulting the Dashboard, the user can compare trends in national-level Cybersecurity threats/vulnerabilities among several countries and/or regions, as well as compare these trends against other relevant national-level statistics to find patterns and correlations. To this extent, the Dashboard provides data in three categories:

- Demographic Data: Basic data about a country's population, economy, education level, and other attributes that may affect the development of the country's Internet services or IT security sectors. (Source: World Development Indicators Database)

- IT Data: Data outlining the state of the country's IT infrastructure, usage, and security, including Internet bandwidth, users, servers, etc. (Sources: ITU, World Development Indicators, CIA World Factbook)

- Cybersecurity Data: Data provided largely by national CERTs that reflect chronological trends threat/vulnerability statistics.

The Dashboard allows the user to select any number of countries and/or regions with which to compare data. While the default x-axis measurement is year (future versions will consider other time scales such as quarter, month), any data can be selected for the y-axis, allowing the user to compare correlations in multiple strands of data. Additionally, the Dashboard allows the user to divide any strand of data into another. This allows the user to compare the data in new ways. For example: dividing population into any measurement creates a "per capita" measurement. Also, the user can compare the viruses reported per number of Internet users. Future versions will further allow the user to compare the viruses reported per number of Internet users per capita, requiring two division functions. Additionally, the user can select to graph the data on a linear or logarithmic scale. The Dashboard thus provides the user with a great amount of flexibility and power in finding exactly what data to compare, how to compare it, and how to illustrate it, so that international cybersecurity can be deeply and robustly investigated.

4.2 Development

The Dashboard was developed in three primary parts: web user interface, database generation, and newsfeed. A regulated interface between the user interface front-end and the database back-end allow information flow from the back-end to the front to operate seamlessly and robustly though changes in code.

Web User Interface

The user interface is a Web application designed to query a database and create graphs of information on-the-fly. The user interface provides a number of fields from which the user can select the countries/regions of interest, the x-axis variable (i.e., start year and end year for the observation) and the y-axis variable (i.e., measurement data to observe) as well as graphing type (linear or logarithmic).

The "submit" button sends the request, after which the web application reads the requested data from the back-end database and draws the graph, automatically scaling the axes to reflect a "best fit" view of the data.

Figure 4.1: Web User Interface of the Cybersecurity Dashboard

Figure 4.1 is a screenshot of the Dashboard configuration. As shown in Figure 4.1, a number of countries are listed in the left side. In the selection list, the countries are grouped into corresponding regions. From the list, the user can select several countries and/or regions of interest[28]. By selecting the start year and the end year, the user can set the observation period. The Dashboard currently incorporates a chronological range of 2000 to 2008. In the right side of the page, the user can select one or two attributes (i.e., measurement data). In case of two attributes, the user should also select an operator by which the data of interest can be calculated from them. The current Dashboard provides only the Division operator by which Attribute 1 is divided by Attribute 2 can be observed. The user can also set the y-axis to a linear or logarithmic scale – which is particularly helpful when comparing data strands that different considerably in values, such as comparing large and small countries, as illustrated later.

---

[28] Multiple countries can be selected by holding down the "Ctrl" key.

Figure 4.2: Example Request to Generate Graph of # Personal Computers per Capita

Country/Region	Data	2000	2001	2002	2003	2004
China	# Personal Computers / Population	0.0163	0.0196	0.0276	0.0392	0.0408
Croatia	# Personal Computers / Population	0.0	0.1431	0.1731	0.1809	0.1872
Estonia	# Personal Computers / Population	0.1537	0.1756	0.2013	0.4224	0.4621
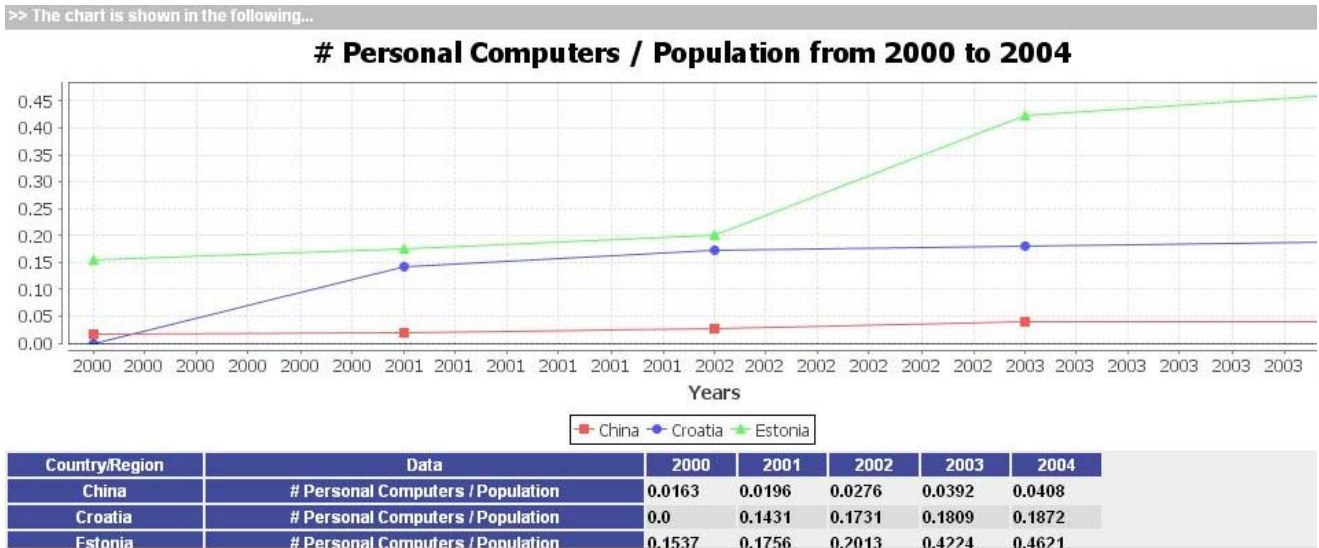
Figure 4.3: Generated Graph of # Personal Computers per Capita

Figure 4.2 is a request to display the number of PC per capita of three countries (in this example, China, Croatia, and Estonia) from 2000 to 2004. Figure 4.3 is the resulting screenshot from the Dashboard. For convenience, the actual data from the database is listed in the table below the graph.

Database

The back-end database of the Dashboard is the Palo MOLAP database[29]. MOLAP stands for

---

29 http://www.jedox.com/

"Multidimensional On-Line Analytical Processing," which is an approach to quickly answer multidimensional analytical queries. The Palo database uses a multidimensional data model, allowing multidimensional structures to organize data and express the relationships between the data. These structures are broken into cubes; the cubes are able to store and access data within the confines of each cube. Each cell within a multidimensional structure contains aggregated data related to elements along each of its dimensions. The output of a MOLAP query is displayed in a matrix format in which the dimensions form the rows and columns, and the relevant measurements form the data values. By using MOLAP database, the Dashboard can quickly answer queries of any aggregated data, such as regional data. Palo consists of a mature MOLAP database server and an Excel add-in. Furthermore, JPalo provides a set of Java API to manipulate the Palo database[30]. These features make it an excellent choice as the back-end database of the Dashboard.

In the current stage, there exists one cube with three dimensions in the Palo MOLAP database. The three dimensions are "Countries", "Years" and "Attributes". When the country, year and attribute are determined, the corresponding measurement data can be accessed.

Recent Headlines

The Dashboard uses Chameleon to create a list of top-relevance recent news headlines. Cameleon is a web extraction engine developed by MIT to automatically extract any piece of data of interest from semi-structured documents (e.g., web pages). In the current stage, the Dashboard lists recent news articles using the search terms "cyber security OR computer spam OR cyber" in Google News[31]. The Dashboard displays the up-to-date news story snippets at the bottom of the user interface page, with hyperlinks that allow the user to open the full story in a new window or tab on their browser.

Figure 4.4: Dashboard Recent Headlines (on July 17, 2009)

---

30 http://www.jpalo.com/
31 http://news.google.com/

4.3 Interesting Demonstrations

Country/Region	Data	2003	2004	2005	2006	2007	2008
China	Total CERT Reported Incidents	2557.0	4485.0	9112.0	26476.0	4390.0	3291.0
Malaysia	Total CERT Reported Incidents	4295.0	15286.0	10147.0	24252.0	39639.0	82649.0
Brazil	Total CERT Reported Incidents	4126941.0	4232104.0	2482200.0	3601322.0	404695.0	3520501.0
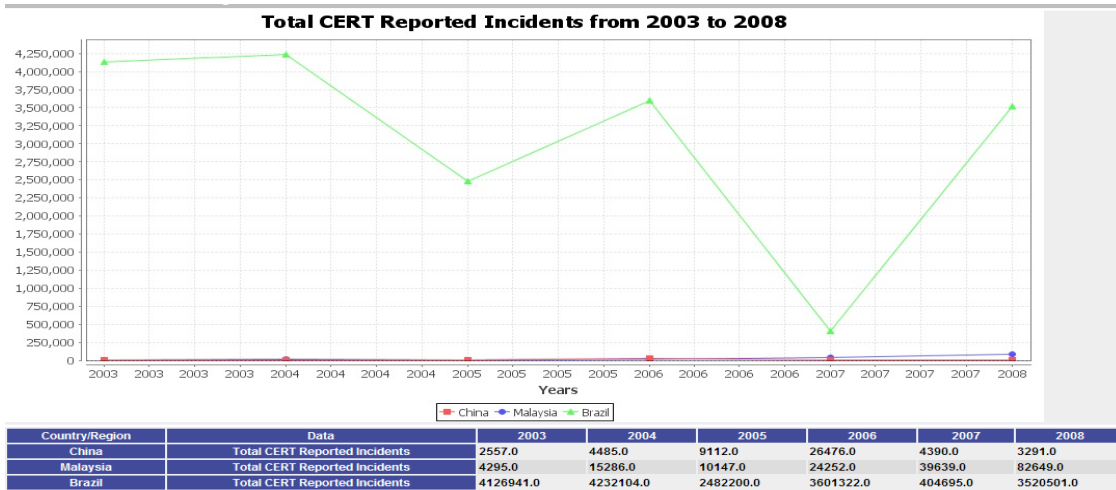
Figure 4.5: Total CERT Reported Incidents from 2003 to 2008 (Linear)

Figure 4.5 is a screenshot of the total CERT reported incidents of three countries (China, Malaysia and Brazil) from 2003 to 2008. It shows that the total CERT reported incidents of Brazil are much greater than that of China and Malaysia in almost of all years – the actual amount data is gathered in the table below the chart. Because of the huge differences, the data strands of China and Malaysia are pushed to the bottom of the chart in the linear Y-axis style.

Country/Region	Data	2003	2004	2005	2006	2007	2008
China	Total CERT Reported Incidents	2557.0	4485.0	9112.0	26476.0	4390.0	3291.0
Malaysia	Total CERT Reported Incidents	4295.0	15286.0	10147.0	24252.0	39639.0	82649.0
Brazil	Total CERT Reported Incidents	4126941.0	4232104.0	2482200.0	3601322.0	404695.0	3520501.0

Figure 4.6: Total CERT Reported Incidents from 2003 to 2008 (Logarithmic)

Figure 4.6 is also a screenshot of the total CERT reported incidents of three countries from figure 4.4 (China, Malaysia and Brazil) from 2003 to 2008. Unlike Figure 4.5, the user uses the logarithmic Y-axis style for the chart, so that the data strands of the three countries are more clearly shown in Figure 4.6.
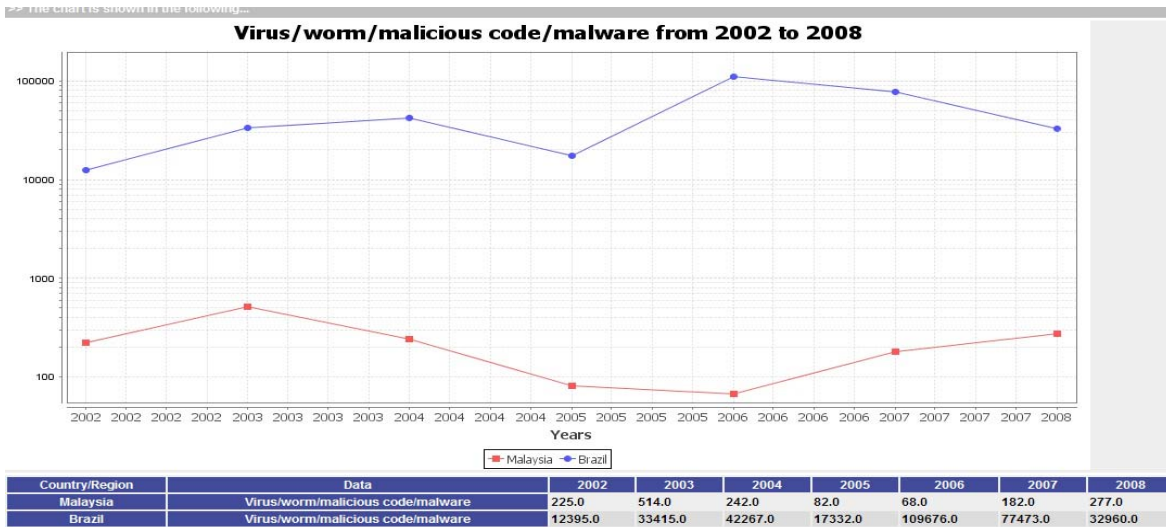
Figure 4.7: Virus/worm/malicious code/malware from 2002 to 2008 (Logarithmic)

Figure 4.7 is a screenshot of "Virus/worm/malicious code/malware", a category of the reported CERT incidents, of two countries (Malaysia and Brazil) from 2002 to 2008 with logarithmic Y-axis style in the chart.
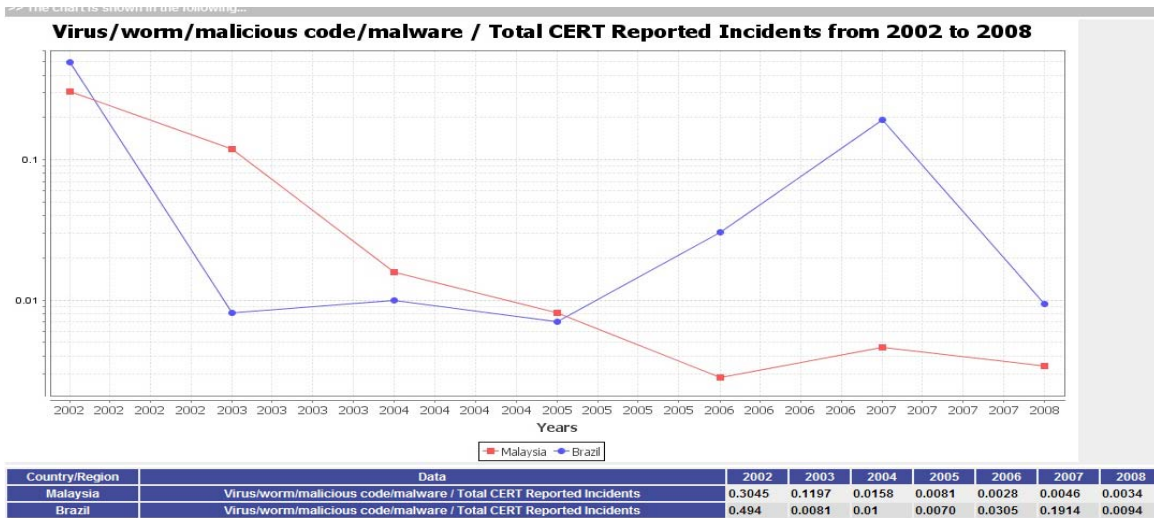
Figure 4.8: Percentage of Virus/worm/malicious code/malware from 2002 to 2008 (Logarithmic)

Figure 4.8 is a screenshot of "Virus/worm/malicious code/malware" divided by "Total CERT Reported Incidents" of two countries (Malaysia and Brazil) from 2002 to 2008 with logarithmic Y-axis style in the chart. In other words, Figure 4.8 shows the data strands of the percentage of a category of the total reported CERT incidents, in this case, "Virus/worm/malicious code/malware".
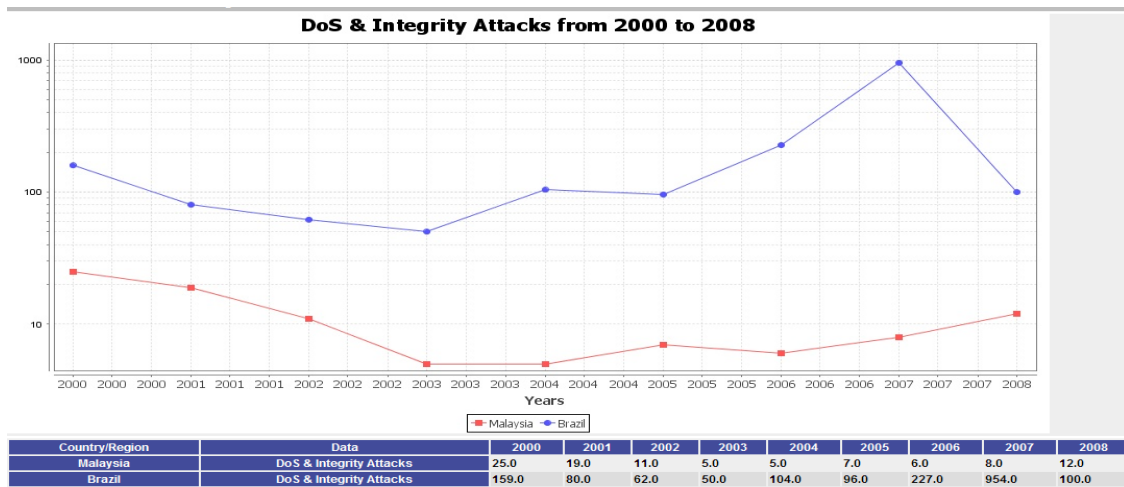
Figure 4.9: Dos & Integrity Attacks from 2000 to 2008 (Logarithmic)

Figure 4.9 is a screenshot of "Dos & Integrity Attacks", a category of the reported CERT incidents, of two countries (i.e., Malaysia and Brazil) from 2000 to 2008 with a logarithmic Y-axis style in the chart.
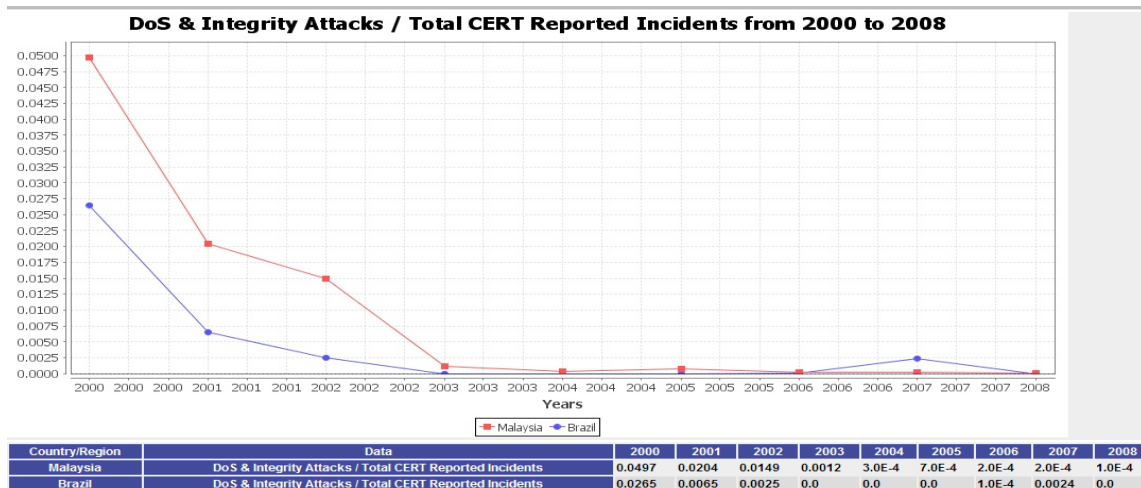
Figure 4.10: Percentage of Dos & Integrity Attacks from 2000 to 2008 (Linear)

Figure 4.10 is a screenshot of "Dos & Integrity Attacks" divided by "Total CERT Reported Incidents" of two countries (Malaysia and Brazil) from 2000 to 2008 with a linear Y-axis style in the chart. In other words, Figure 4.10 shows the data strands of the percentage of a category of the total reported CERT incidents, in this case, "Dos & Integrity Attacks".
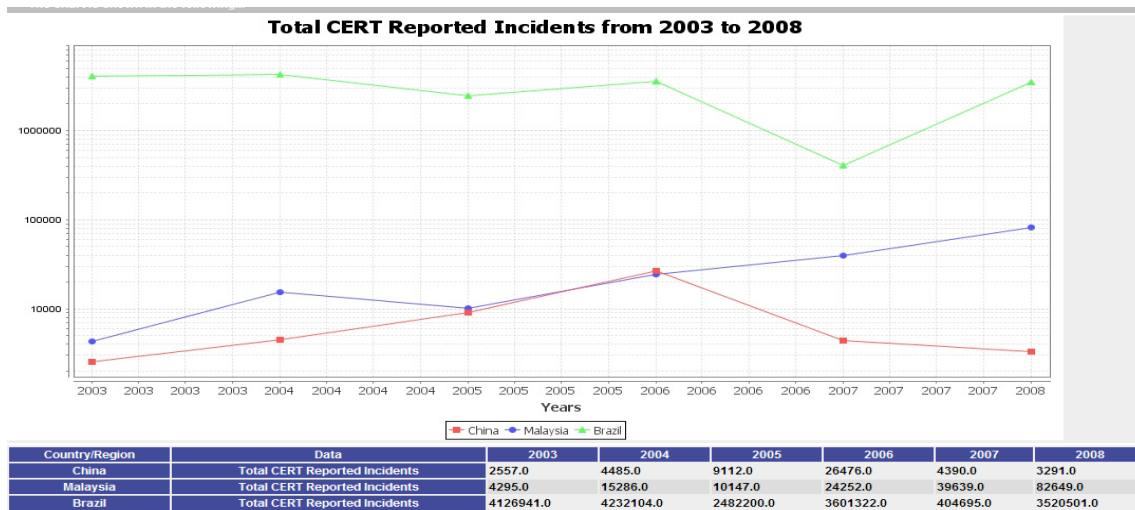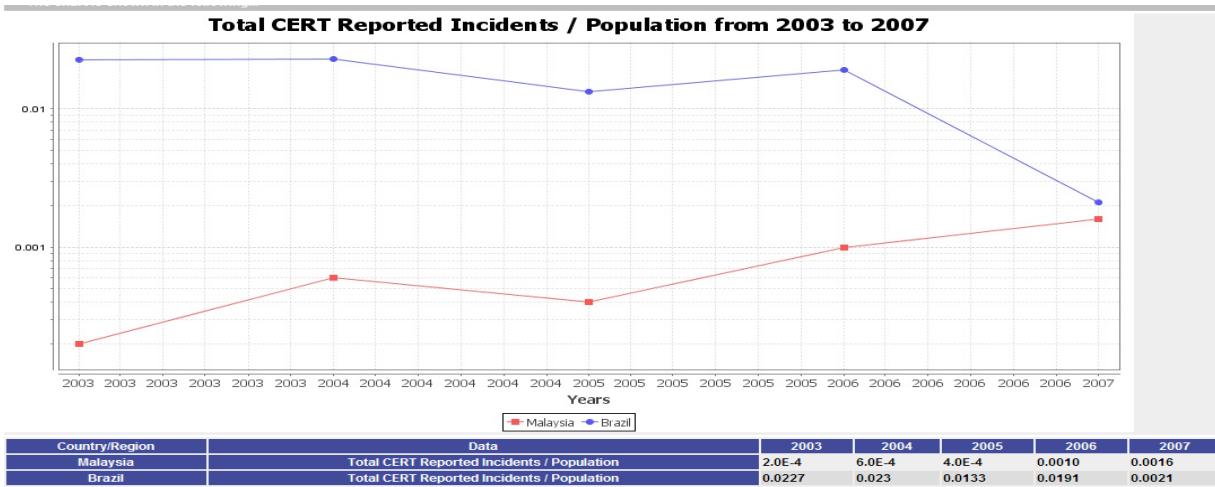
Figure 4.11: Total CERT Reported Incidents per Capita from 2003 to 2007 (Logarithmic)

Figure 4.11 is a screenshot of "Total CERT Reported Incidents" divided by "Population" (thus creating a per capita measurement) of two countries, Malaysia and Brazil, from 2003 to 2007 with a logarithmic Y-axis style in the chart. It is interesting that the per capita number of reported incidents started at very different levels (in 2003), but the rate has dropped sharply in Brazil while rising sharply in Malaysia such that they are about equal rates by 2007.
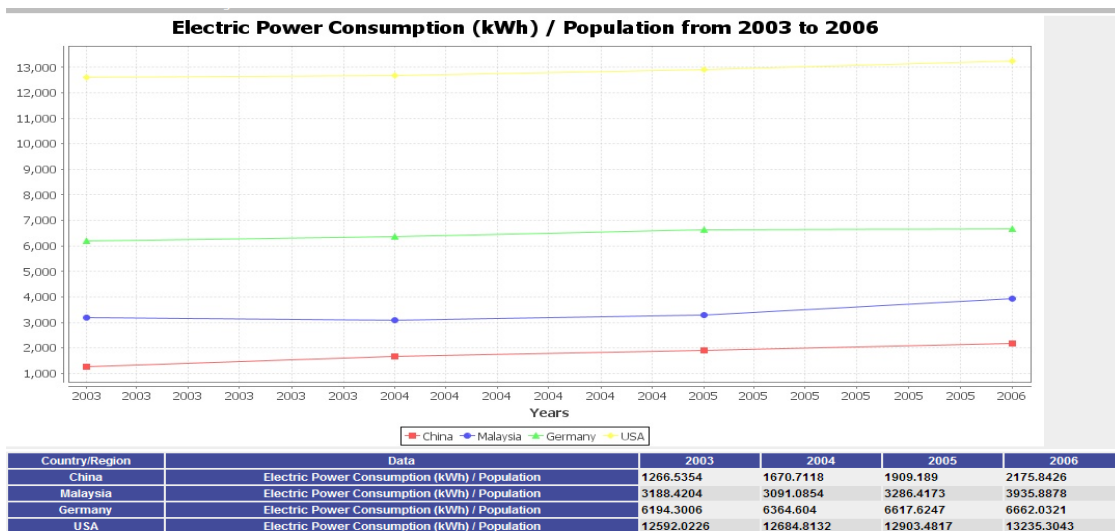
Figure 4.12: Electric Power Consumption (kWh) per Capita from 2003 to 2006 (Linear)

Figure 4.12 illustrates other types of analyses that can be done, such as "Electric Power Consumption (kWh)" divided by "Population" (creating a per capita measurement) of four countries (China, Malaysia, Germany and USA) from 2003 to 2006 with a linear Y-axis style in the chart.
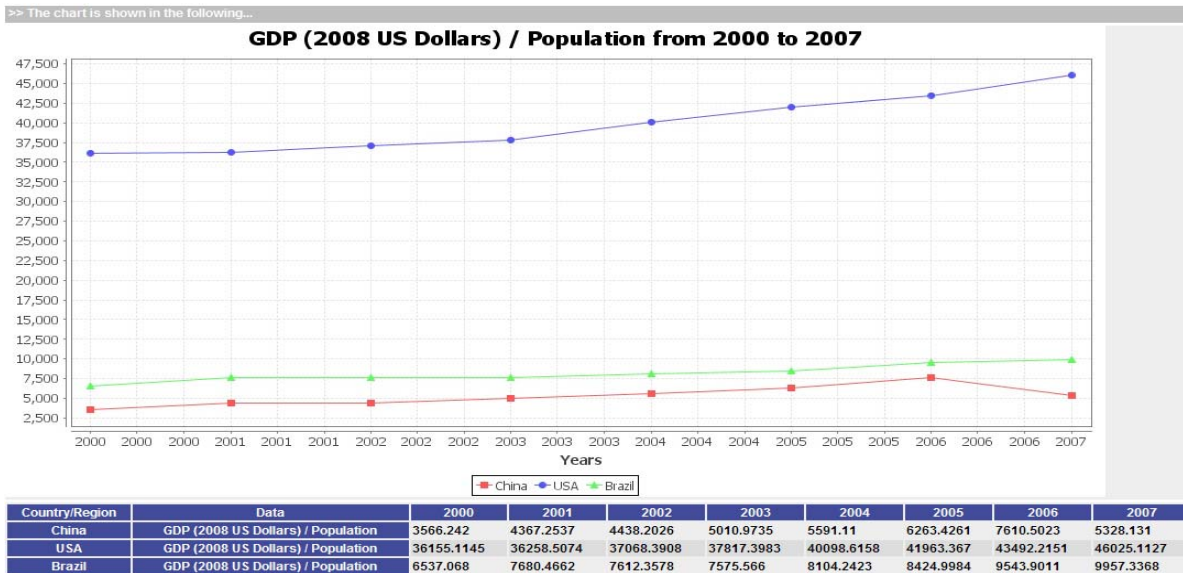
Figure 4.13: GDP (2008 US Dollars) per Capita from 2000 to 2007 (Linear)

Figure 4.13 is the screenshot of "GDP (2008 US Dollars)" divided by "Population" (creating a per capita measurement) of three countries (China, USA and Brazil) from 2000 to 2007 with a linear Y-axis style in the chart.

4.4 Current Status of Data Dashboard Prototype

The current status as of August 7, 2009, includes a working prototype of the Dashboard. The database has some gaps in cross-time or cross-national CERT coverage. In the next phase, more extensive types of data and better sources of data are being sought.

The current variables expressed in the prototype Dashboard include:

Demographic Data	IT Data	Cybersecurity Data
Population (#)	Internet Users (#)	Total incidents (#)
Gross Domestic Product (USD)	International Bandwidth (MBps)	Phishing (#)
Software Piracy Losses (USD)	Personal Computers (#)	Trojan/worm/malware (#)
Energy Consumption (KWh/yr)	Hosts (#)	(D)DoS (#)
Total Education Enrollment (%)	Secure Servers[32] (#)	Spam (#)

Table 4.1: Variables in the Data Dashboard

The current list of countries in the Dashboard are: United States, China, India, Germany, Japan, Republic of Korea, Brazil, Estonia, Latvia, Croatia, Malaysia, Australia.

---

32 "Secure Servers" are those that use fully cryptographed communication.

Both the number of countries and the types of data will be significantly expanded in future versions.

The particular cybersecurity data availability of each category, by country, is presented below:

Type	USA	China	India	Korea	Malaysia	Brazil	Germany	Japan	Estonia	Croatia	Latvia
Malicious Code	Prop.	Abs.	Abs.	Abs.	Abs.	Abs.	None	None	Prop.	None	None
Phishing	Prop.	Abs.	Abs.	None	None	None	None	Abs.	Prop.	None	Prop.
Scanning	Prop.	Abs.	None	None	None	Abs.	None	Abs.	None	None	None
Spam	None	Abs.	Abs.	None	Abs.	Abs.	None	None	Prop.	None	None
DoS	None	Abs.	None	None	Abs.	Abs.	None	None	None	None	Prop.

Table 4.2: CERT-based Cybersecurity Data by Country[33]

4.5 Challenges

A number of challenges and opportunities for discovery and improvement remain for the Cybersecurity Dashboard project.

Data Availability

The availability of data varies by category, but is often limited or nonexistent. In particular, the cybersecurity category of data is particularly difficult to find. CERTs are the primary source of such data, but many countries do not have national CERTs, and many national CERTs do not provide much data, if any at all. The lack of data availability will continue to be a pressing challenge for the ECIR Dashboard project.

Data Consistency & Reliability

Among CERTs that have data available for nation-level threats and vulnerabilities, consistency is a serious problem. Many of the CERTs that have such data have only begun recording data within the past three or four years; this makes historical trend analysis limited in utility. Furthermore, a lack of consistency between CERTs makes the deployment of a single framework for comparison of cybersecurity data difficult. CERTs often do not share similar reporting styles (some report in absolute numbers; some report in percentages only); they often do not share categorization methods for threats/vulnerabilities (identifying different groups into which threats/vulnerabilities fall differs between almost every CERT). There are some very general categories that can be constructed successfully, but they are uncommon. Data consistency and reliability issues will continue to pose a challenge for the ECIR Dashboard project and will be a major focus of our future activities.

---

33 In this table, "Prop." represents a source hosting proportional data; "Abs." represents absolute numerical data; "None" represents no data. Most data threads are not available for all years of the dashboard (2000-2008); most CERTs that publish quantitative data have only published in the past few years; many have not yet released a publication with 2008 data.

References

"2008 Cyber Security Summary and 2009 Projection." Security China. 31 Dec 2008. 8 Jun 2009
    <http://www.anqn.com/news/a/2008-12-31/a09104963-1.shtml>.
The CERT Coordination Center (CERT/CC). Pittsburgh: Carnegie Mellon University. <http://www.cert.org>
CERT Estonia." RISO State Information System. 28 Aug 2008. RISO State Information System. 11 Jun 2009
    <http://www.cert.ru/conference2008.html>.
"China Cyber Security Report 2008 Q1 and Q2." 2008. CN CERT/CC. 8 Jun 2009
    <http://metc.zzuli.edu.cn/upload/Files/20081216185349.pdf>.
"CNCERT/CC Half-yearly Report 2008Q1 & Q2," CNCERT/CC. 11 Jun 2009
    <http://www.cert.org.cn/UserFiles/File/CISR2008fh.pdf1.pdf>.
"Computer Hacking and Unauthorized Access Laws." National Conference of State Legislatures. 2009. National
    Conference of State Legislatures. 8 Jun 2009
    <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ComputerHackingandUna
    uthorizedAccessLaws/tabid/13494/Default.aspx>.
"Cyber Security Tip ST04-012, Browsing Safely: Understanding Active Content and Cookies." National Cyber
    Alert System. 2009. United States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-
    cert.gov/cas/tips/ST04-012.html>.
"Cyber Security Tip ST04-014, Avoiding Social Engineering and Phishing Attacks." National Cyber Alert
    System. 2009. United States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-
    cert.gov/cas/tips/ST04-014.html>.
"Cyber Security Tip ST04-015, Understanding Denial-of-Service Attacks." National Cyber Alert System. 2009.
    United States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-cert.gov/cas/tips/ST04-
    015.html>.
"Cyber Security Tip ST05-007, Risks of File-Sharing Technology." National Cyber Alert System. 2009. United
    States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-cert.gov/cas/tips/ST05-007.html>.
"Cyber Security Tip ST05-007, Risks of File-Sharing Technology." National Cyber Alert System. 2009. United
    States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-cert.gov/cas/tips/ST05-007.html>.
"Cyber Security Tip ST05-008, How Anonymous Are You?" National Cyber Alert System. 2009. United States
    Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-cert.gov/cas/tips/ST05-008.html>.
"Cyber Security Tip ST05-011, Effectively Erasing Files." National Cyber Alert System. 2009. United States
    Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-cert.gov/cas/tips/ST05-011.html>.
"Cyber Security Tip ST06-001, Understanding Hidden Threats: Rootkits and Botnets." National Cyber Alert
    System. 2009. United States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-
    cert.gov/cas/tips/ST06-001.html>.
"Cyber Security Tip ST06-006, Understanding Hidden Threats: Corrupted Software Files." National Cyber Alert
    System. 2009. United States Computer Emergency Readiness Team. 8 Jun 2009 <http://www.us-
    cert.gov/cas/tips/ST06-006.html>.
"Denial of Service Attacks." CERT. 2009. Software Engineering Institute, Carnegie Mellon University. 8 Jun
    2009 <http://www.cert.org/tech_tips/denial_of_service.html>.
"Emerging Cyber Threats Report for 2009." Goergia Tech Information Security Center. 8 Jun 2009
    <http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>.
Forum for Incident Response and Security Teams. <http://www.first.org>.

Appendix A: Sources of Data Currently Used in the Prototype ECIR Dashboard

The years covered by the current data used in the prototype ECIR Dashboard is summarized in the table below:

	# Hosts	# Personal Computers	# Secure Internet Servers	# Users w/ Internet Access	DoS & Integrity Attacks	Electric Power Consumption (kWh)	GDP (2000 US Dollars)	International Bandwidth (MB/s)	Phishing/personal data abuse	Population	Scanning	School enrollment, tertiary (% gross)	Software Piracy Losses ($M)
Australia	2000-2004, 2006-2008	2000-2004	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2006	2003-2008
Brazil	2000-2004, 2006-2008	2000-2005	2001, 2003-2008	2000-2007	all	2000-2006	2000-2007	2000-2005	none	2000-2007	all	2000-2005	2003-2008
China	2000-2004, 2006-2008	2000-2006	2001, 2003-2008	2000-2007	2005-2008	2000-2006	2000-2007	2000-2005	2005-2008	2000-2007	2003-2005	2000-2003, 2006	2001, 2003-2008
Croatia	2000-2004, 2006-2008	2000-2004	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2003, 2005-2006	2003-2008
Estonia	2000-2004, 2006-2008	2000-2007	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2006	2003-2008
Germany	2000-2004, 2006-2008	2000-2006	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	none	2003-2008
India	2000-2004, 2006-2008	2000-2007	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	2007-2008	2000-2007	2007-2008	2000-2006	2001, 2003-2004, 2007-
Japan	all	2000-2004	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2006	2003-2008
Latvia	2000-2004, 2006-2008	2000-2006	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2006	2003-2008
Malaysia	2000-2004, 2006-2008	2000-2006	2001, 2003-2008	2000-2007	all	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2005	2003-2008
ROK	2000-2004, 2007-2008	2000-2008	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2006	2003-2008
USA	all	2000-2006	2001, 2003-2008	2000-2007	none	2000-2006	2000-2007	2000-2005	none	2000-2007	none	2000-2006	2003-2008

The sources of each of these data fields is listed below:
 # Hosts: 2000-2004: ITU Data, all other: CIA World Factbook
 # Personal Computers: 2000-2004: ITU Data, all other: World Development Indicators Database
 # Secure Internet Servers: World Development Indicators Database
 # Users w/ Internet Access: World Development Indicators Database
DoS & Integrity Attacks: Country-Specific CERT where available
Electric Power Consumption (kWh): World Development Indicators
GDP (2000 US Dollars): World Development Indicators
International Bandwidth (MB/s): World Development Indicators Database
Phishing/personal data abuse: Country-Specific CERT where available
Population: World Development Indicators
Scanning: Country-Specific CERT where available
School enrollment, tertiary (% gross): World Development Indicators Database
Software Piracy Losses ($M): BSA & IDC Global Software Piracy Study
Total CERT Reported Incidents: Country-Specific CERT where available
Virus/worm/malicious code/malware: Country-Specific CERT where available

The specific resources referred to above are described below:
The World Development Indicators Database (WDI) describes itself as "the statistical benchmark that helps measure the progress of development. The WDI provides a comprehensive overview of development drawing on data from the World Bank and more than 30 partners. It includes more than 800 indicators in over 90 tables organized in 6 sections: World View, People, Environment, Economy, States and Markets, and Global Links." We believe that the World Bank has less reason

to mis-represent data than other sources might. Because of this trustworthiness, the WDI is our primary statistical source.
For further information, see:
http://web.worldbank.org/WBSITE/EXTERNAL/DATASTATISTICS/0,,contentMDK:21725423~pagePK:64133150~piPK:64133175~theSitePK:239419,00.html

The Annual BSA and IDC Global Software Piracy Study tracks global losses due to piracy, mainly as a tool for business strategists. To do this they "Determine how much PC packaged software was deployed in [a given year;] Determine how much PC packaged software was paid for/legally acquired in [this given year; and] Subtract one from the other to get the amount of pirated software." As the data was intended for strategic use, we believe it to be highly trustworthy. Unfortunately, the BSA & IDC Global Software Piracy Study was only begun in 2003 – and do not provide data from previous years.
For more information, please see: http://global.bsa.org/globalpiracy2008/index.html

The International Telecommunications Union publishes a "The World Telecommunication/ICT Indicators Database [which] contains time series data… for around 100 sets of telecommunication statistics (updated) covering telephone network size and dimension, mobile services, quality of service, traffic, staff, tariffs, revenue and investment… Selected demographic, macro-economic and broadcasting statistics are also included." Because countries self-report certain series in the ITU database, we believe there is a small risk of inflation. To avoid this, we have only relied on ITU data where the WDI data is notably less complete.
For further information, please see: http://www.itu.int/ITU-D/ict/publications/world/world.html

An additional resource, **The CIA World Factbook** "provides information on the history, people, government, economy, geography, communications, transportation, military, and transnational issues for 266 world entities." The CIA World Factbook receives their data from other groups and databases, including those groups otherwise mentioned here. In the interest of continuity, we have only referenced the CIA World Factbook for data that we could not find in a first-level database.
For further information, please see: https://www.cia.gov/library/publications/the-world-factbook/

Appendix B: Summary of Reporting By Selected National CERTs

Appendix B is a full summary of the reporting habits of selected National CERTs, and their founding year (if known). Many of these reports do not contain quantitative data or charts; the following appendix should thus not be used as a guide to quantitative data for aggregation projects.

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
Asia						
Asia Pacific Computer Emergency Response Team **(contains 15 countries' CERT, including China)**	N/A	2003-2008	N/A	N/A	N/A	N/A
Australia CERT	N/A	N/A	N/A	N/A	1. Yearly Australian Computer Crime and Security Survey: 2002-2006 (http://www.auscert.org.au/render.html?it=2001) 2. AusCERT Newsletter but only access to authorized member, updated until July 2004	N/A
Brunei CERT	N/A	N/A	N/A	N/A	N/A	May 2004
Bangladesh CERT	N/A	N/A	N/A	N/A	N/A	July 2007, right now the publication tag is not available
China	Half-yearly Report:	2005 - 2007	N/A	Composite Website Monthly	N/A	Oct 2000

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
	2005 -- 2008 Q1&Q2			Report: 2006 - - March 2009		
Hong Kong CERT	N/A	N/A	N/A	N/A	Only available: Alerts received from websites from 2001-2009; Virus alerts from websites from 2001-2009; Number of incidents reported from 2001-2009; Virus incidents reported from 2001 -2009;	N/A
Indonesian CSIRT	N/A	N/A	N/A	N/A	Almost no tags is available. Events only updated until 2005	N/A
India	N/A	N/A	July 2006 - April 2009	Phishing Incidents Trend Report: Jan 2009 -- March 2009		N/A
Japan CERT-CC	Quarterly : 2008Q2 – 2009 Q1 (in Japanese); 2000Q1 – 2009Q1 , 1996Q4				Vulnerabilities Quarterly Report: 2004Q3 – 2008Q4 ; Weekly Bulletin: Sep 6th 2006 - June 10th, 2009	N/A
Korea CERT	N/A	N/A	Jan 2006 – Jan 2009	Phishing Activity Trends Report: Feb 2005 – Jan 2009	N/A	JUL. 1996
Korea National	N/A	Only 2004	1)Monthly	N/A	N/A	N/A

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
Computer Emergency Response Team			Cyber Security: June 2004 – April 2009 (contains events distribution, number of events per month) 2) Cyber threat trends and countermeasures: Jan 2005 – May 2008 (contains detailed data)			
Malaysia CERT	Situational report on major worms outbreaks up to 2003 in Malaysia.	N/A	N/A	N/A	Having statistics about number of incidents and distribution of different events from 1997 to 2009 (annually) (http://www.mycert.org.my/en/services/statistic/mycert/2009/main/detail/625/index.html)	January 13, 1997
Myanmar CERT					Link is not available	
Pakistan CERT	N/A	N/A	N/A	N/A	Defacement statistics from 1999 – 2008.	N/A
Philippine CERT						Not available
Qatar CERT	N/A	N/A	N/A	N/A	No statistics is found	
Russia CERT	N/A	N/A	N/A	N/A	Only2007 events distribution is available only in Russian: http://www.cert.ru/stat.html	N/A

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
Sri Lanka CERT	N/A	N/A	N/A	N/A	Not about statistics: Cyber Security Term Glossary: http://www.slcert.gov.lk/index.php?q=8&id=27	June 2006
Singapore CERT	N/A	N/A	N/A	N/A	N/A	October 1997
Taiwan Computer Emergency Response Team/Coordination Center	N/A	N/A	N/A	N/A	N/A No statistics is found	Sep 1987
Taiwan National Computer Emergency Response Team	N/A	N/A	N/A	N/A	No statistics is found	N/A
Thai CERT	N/A	N/A	N/A	N/A	(English version only has "about Thai CERT). The Thai version needs double check. I could not find any statistics from it.	2000
Vietnam	N/A	N/A	N/A	N/A	(English version is being established)	Dec 2005
North America						
Canadian Cert					Link is not available	N/A
Computer Emergency Response Team -Coordinating Centre	N/A	N/A	N/A	N/A	Only vulnerabilities statistics from 1988-2008, and they are no longer publish or collect those data.	N/A
Forum of Incident					Its focus is not on publishing the statistics data	1990

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
Response and Security Teams						
US-CERT	N/A	Quarterly Reports: 2006Q3 -- 2008 Q4	N/A	Nov 2007 -- May 2009	N/A	N/A
Mexico (MX)	N/A	N/A	N/A	N/A	Only in Mexican	N/A
South America						
Argentinian CERT	N/A	N/A	N/A	N/A	No published statistics was found	May 1999
CAIS- Brazilian Research Network CSIRT	N/A	N/A	N/A	N/A	Number of Incidents reported. 1997-2009 (yearly and monthly) http://www.rnp.br/en/cais/statistics/	N/A
Computer Emergency Response Team Brazil	2000Q1, 2003Q1-2009Q1 ((http://www.cert.br/stats/) Half-year: 1999, 2000,	1999-2008 (http://www.cert.br/stats/)	N/A	Spam: Jan 2009- April 2009; Number of spam (yearly): 2003 - 2009	1) Daily statistics for the network flow data directed to honeypots from the Brazilian Honeypots Alliance (http://www.honeypots-alliance.org.br/stats/) 2) Total number of incidents reported 1999 - 2009	
NIC BR Security Office Brazilian CERT	The same as above	The same as above	The same as above	The same as above	The same as above	
European						
Austrian CERT	N/A	N/A	N/A	N/A	N/A Did not find English version	N/A
Belgian CERT	N/A	N/A	N/A	N/A	N/A	N/A
Crotian CERT	N/A	N/A	N/A	N/A	The English version is only partly translated.	N/A
Czech Republic	N/A	N/A	N/A	N/A	N/A	1996?

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
CERT						
Danish CERT					*English version covers almost nothing and online translation is not working for this website. Cannot write any summry here because of language.*	
Estonian CERT	N/A	N/A	N/A	N/A	http://www.riso.ee/en/node/22 has the only available data: 2005 - 2007	
Finland CERT	N/A	N/A	N/A	N/A	No statistics was found	N/A
France Industry,services and Tertiary CERT	N/A	N/A	N/A	N/A	No statistics was found	N/A
French CERT	N/A	N/A	N/A	N/A	No statistics was found. No English version.	N/A
German CERT	N/A	N/A	N/A	N/A	http://www.cert.dfn.de/index.php ?id=aw-typen contains examples of reports for some events, such as defacement, Phishing; only in German.	N/A
Greek Research and Technology Network CERT	N/A	N/A	N/A	N/A	No English version is available. No statistics was found.	N/A
Hungarian CERT	N/A	N/A	N/A	N/A	No statistics was found	N/A
Iceland					Link is not available	
Ireland	N/A	N/A	N/A	N/A	No statistics was found	N/A
Israeli CERT	N/A	N/A	N/A	N/A	No Israeli-oriented data was found. Only contains document links for other reports.	N/A
Israeli Government CERT						
Italian CERT	N/A	N/A	N/A	N/A	No statistics can be access unless register	1994

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
Latvian CERT	N/A	N/A	N/A	N/A	Only the current 3 months' event distribution is available (in one graph and in Latvian) http://www.ddirv.lv/?cat=3	N/A
Lithuanian CERT	N/A	Yearly statistic: 2001-2008	N/A	N/A	N/A	N/A
Netherlands CERT	N/A	N/A	N/A	N/A	N/A	N/A
Norwegian Computer Emergency Response Team		N/A	Jan 2009 – April 2009, do not contain data such as number of incidents, distribution of different events:	N/A	N/A	Jan 2006
Norwegian Network for Research Education CERT	N/A	N/A	N/A	N/A	No statistics was found	N/A
Poland CERT Research and Academic Network	N/A	N/A	N/A	N/A	The link to CERT Polska (www.cert.pl) is not available.	(1993)
Portuguese CERT	N/A	N/A	Jan 2005 – March 2009, only available in Portuguese.	N/A		N/A
Slovenian CERT	N/A	N/A	N/A	N/A	No statistics was found	N/A
Spanish CERT	N/A	N/A	N/A	N/A	Only number of vulnerabilities from 2005-2009, vulnerabilities	N/A

Country / Region	Quarterly Report / Half-year Report	Yearly Report	Not-specified Monthly Report	Specified Monthly Report	Others	Date Formed
					data in 2008 and 2009.	
Sweden	N/A	N/A	N/A	N/A	No statistics was found	N/A
Swiss Academic and Research Network CERT					Internet Background Noise (IBN) 2003 – 2009 (**http://www.switch.ch/security/services/IBN/**)	1987
Turkish CSIRT	N/A	N/A	N/A	N/A	The statistics page has nothing about number of incidents or distribution of events: http://www.ulakbim.gov.tr/ulaknet/istatistik/	N/A
United Kingdom	N/A	N/A	N/A	N/A	No statistics about cyber events was found	