

TeleContinuity®

The Survivable Cyber Solution

Presentation For



Presenter:
October 14, 2009
Mr. Takanobu Ito
Managing Director,
Asia Pacific & Middle East Operations

Cybersecurity and Business Continuity for Commercial Business and Government Agencies

General Background

- ➔ **Information and Communications networks are under constant attack from terrorists, criminal groups, virus and malware developers and have made network continuity the focus of a recovery strategy.**
- ➔ **As organizations move towards using Software as a Service (SaaS) and Cloud Computing, the mitigation of any cyber attack must be taken into consideration.**
- ➔ **Under a wide variety of Emergencies includes Earthquake, Fire, Flood, Typhoon, Hurricane, Pandemic, Utility Outage, Terrorism, fiber Cut, and even building evacuation, it is highly probable that organizations will suffer huge loss by Cyber-Attack.**

Cyberspace Policy Review Obama's a 60 days report

- ➔ **President Obama has declared cybersecurity to be “one of the most serious economic and national security challenges we face as a nation.” May 29th , 2009**

Securing Our Nation's Cyber Infrastructure, Speech by President Obama, May 29, 2009.

http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

- ➔ **Foreign powers have infiltrated the e-mail of Defense Secretary Robert Gates, stolen data from the Pentagon's most technologically advanced fighter aircraft, and hacked State Department computers and the electrical grid. July 2009**
- ➔ **The Government Accountability Office (GAO) reported weaknesses in the ability of 23 of 24 major agencies to detect or prevent cyber attacks, and investigators said that unless those flaws are corrected a “broad array of federal assets and operations will remain at unnecessary risk of fraud, misuse, and disruption. January 2009**

Clean Slate Review and Addressed Obama's a 60 days report

1) Cybersecurity again with a Clean Slate

Work together with academia, industry, government and international partners.

2) White House and Cybersecurity Coordinator

Responsible for integrating all Cybersecurity policies for the government.

3) Public-Private partnership with International Cooperation

Cyber space are owned and operated by the private sector, both nationally and internationally, so the issues require to be collaborated.

4) Failure of Critical Infrastructures

Disruption of electric power capabilities in multiple regions.

5) Exploiting global financial services

Financial business is global and depend on cyberspace.

6) Systemic Loss of U.S. Economic Value

Industry estimates losses in 2008 range as High as \$1 trillion.

Five Key Action Plan by Obama's 60days Report

1) Leading from the Top

Information and Communication Infrastructure Interagency Policy Committee (ICI-IPC), chaired by the National Security Council (NSC) and Homeland Security Council (HSC) for the primary policy coordination.

2) Building Capacity for a Digital Nation

Promote Public Awareness and increase Cybersecurity Education, which expand Federal information Technology Workforce.

3) Sharing responsibilities for Cybersecurity

Improve Partnership between Private Sector and Government with evaluating potential barriers in-between as well as develop partners effectively with International community.

4) Improving Information Sharing and Incident Response

The ICI-IPC process define roles, responsibilities, and resources for different departments and agencies with respect to incident response.

5) Encouraging Innovation

Link R&D Frameworks to infrastructure Development and integrate Globalization Policy with Supply Chain Security.

Overview IC3 for Private Sector 2008 Internet Crime Report

1) The Internet Crime Complaint Center (IC3)

- Start operation on May 8, 2000, as the Internet Fraud Complaint Center.
- Established as a partnership between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI).
- Receive, process, and refer criminal complaints to serve the law enforcement.

2) Wide Variety of Cyber Crime

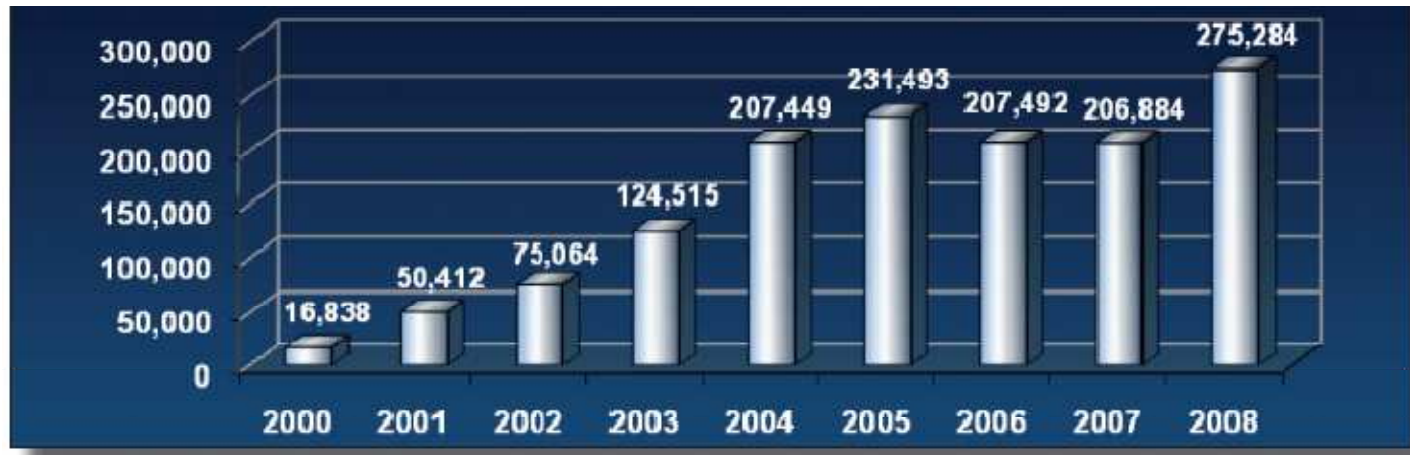
- Online Fraud (in many forms)
- Intellectual Property Rights Matters
- Computer Intrusions (hacking)
- Economic Espionage (theft of trade secrets)
- Child Pornography
- International Money Laundering
- Identity Theft

3) Internet Complaint Search and Investigation System

- “Internet Complaint Search and Investigation System (ICSIS)”
- Available to any NW3C approved agencies.
- https://members.nw3c.org/services_databases.cfm
- A public website, <http://www.lookstoogoodtobetrue.com> for various consumer alerts, tips, and fraud trends.
- Recommend periodically checking the IC3, FBI, and the FTC websites for the latest updates

IC3 Report for Internet Crimes & Complaints

Yearly Comparison Complaints Received via IC3 Website

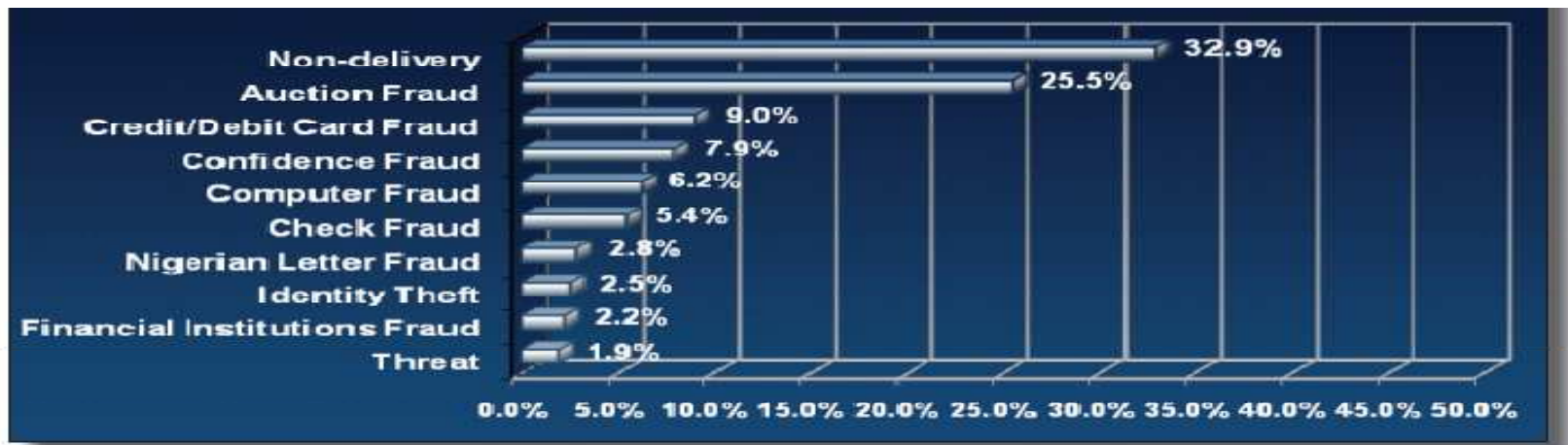


2008 Yearly Dollar Loss (in million) Referred Complaints

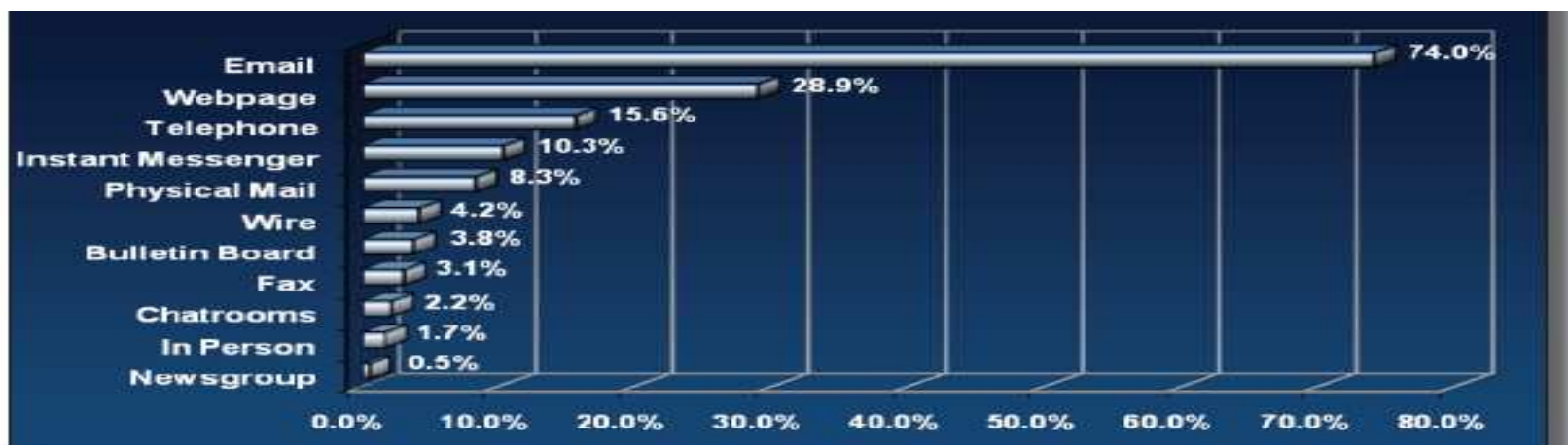


Reports from IC3

2008 Top 10 IC3 Complaint Categories (Percent of Total Complaints Received)

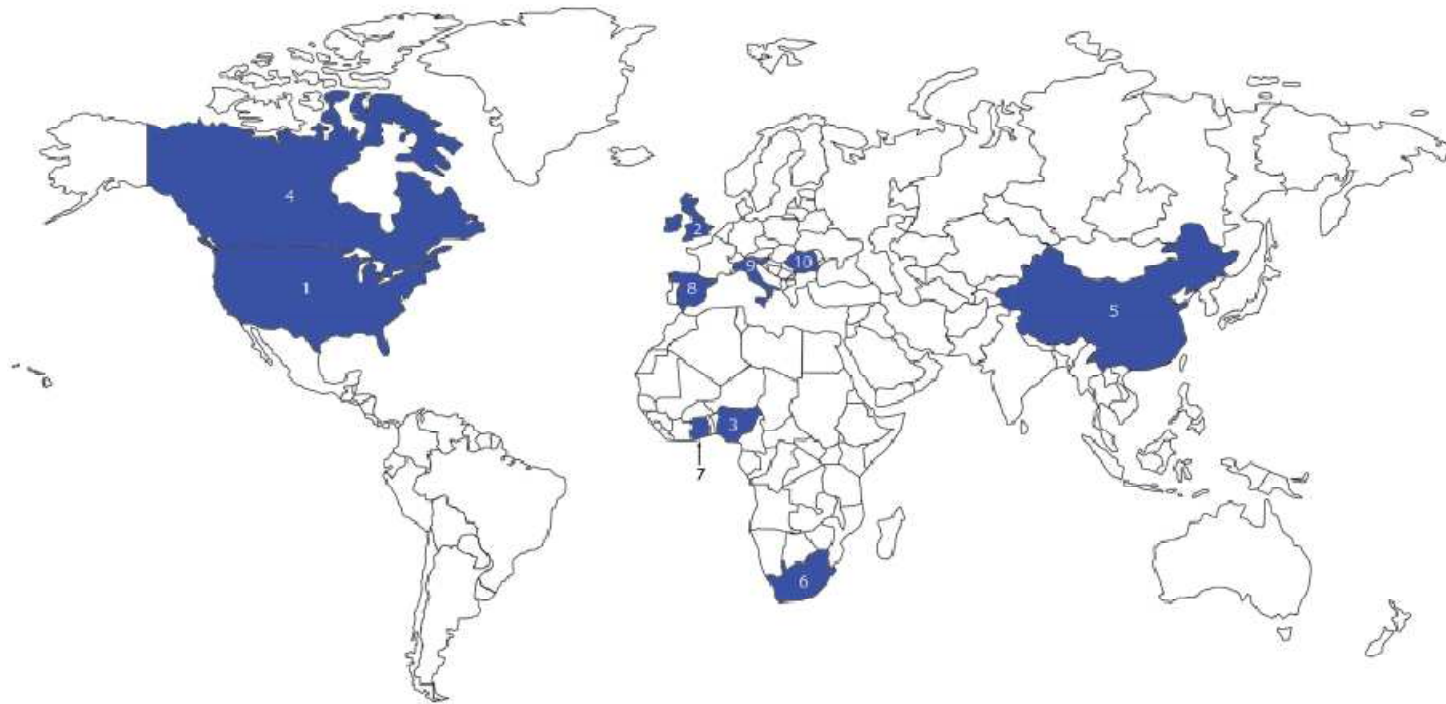


Contact Method



Reports from IC3

Top 10 Countries By Count : Perpetrators



1. United States	66.1%	6. South Africa	0.7%
2. United Kingdom	10.5%	7. Ghana	0.6%
3. Nigeria	7.5%	8. Spain	0.6%
4. Canada	3.1%	9. Italy	0.5%
5. China	1.6%	10. Romania	0.5%

Perpetrators also have been identified as residing the United Kingdom, Nigeria, Canada, Romania, and Italy. Inter-state and international Boundaries are irrelevant to Internet criminals. Jurisdictional issues can Enhance their criminal efforts by impeding investigations with multiple Victims, multiple states/countries, and varying dollar losses.

Reports from IC3

Top 10 Countries (Complainant)



1. United States	92.93%	6. France	0.15%
2. Canada	1.77%	7. South Africa	0.15%
3. United Kingdom	0.95%	8. Mexico	0.14%
4. Australia	0.57%	9. Denmark	0.13%
5. India	0.36%	10. Philippines	0.13%

While most complainants were from the United States, IC3 has also received a number of filing from Canada, the United Kingdom, and Australia.

Essential Weakness of Continuity of Operation (COOP) / Business Continuity Plan (BCP) include CyberSecurity

Any Pre-Planned BCM/BCP have a Large Security (Scenario) Hole

- ➡ ***How do you contact your emergency team to announce BCP officially?***
- ➡ ***How are you going to communicate with your boss, emergency team in order to activate BCP (unless you have absolute authority to order) under unpredictable emergency situation?***

Under a wide variety of Emergencies, it is highly probable that organizations will suffer huge loss in Communication capability. Loss in communications capabilities (email, wire line phone, wireless phone, satellite phone, IP Phone, SMS) is unacceptable for today's business executive. Restoration of telecommunications services is the number one priority when considering Continuity of Operations (COOP) and Business Continuity Management (BCM/BCP).

Your BCP needs Disaster Communications

NEED OF SURVIVAL COMMUNICATION OR BACK UP COMMUNICATION PLAN

Almost any pre-planned BCP/BCM/COOP usually start to contacting with emergency team or secure the communication, so you have to have secure and survival communication infrastructure in any disaster cases. It must be located in different cyber-space in order to avoid single point of failure. If an emergency would hit us with exactly same scenario as planned..... Unfortunately it would never happen in that way, that's why we call it as Emergency.

How Do You Maintain Communication Continuity During a Disaster?

- The **cause** of the telecommunications outage is Unknown.
PBX failure, Pandemic, Terrorism, Floods, etc€46
- The **impact** on the public infrastructure is unknown.
Wireline, Wireless, Satellite and Internet – what platform will be viable for call delivery?
- The **access** to alternate infrastructure could be limited.
Agency Communications and Internet, Private Communications – Home Phone, Cell Phone, Public Internet.
- The **duration** of the Event is Unknown.
Hours, Days, Weeks, Months€46

BCP Communications Requirements

- **Location Independence**

Staff must be able to receive calls made to their work number and make outbound calls regardless of where they are located as they cope with the changing disaster conditions.

- **Network Independence**

To assure telephone service, incoming and outgoing calls must be able to make immediate use of any and all surviving networks (TDM and IP) that are available to make and receive telephone calls.

- **Device Independence**

The solution must allow staff to utilize any communication device available to them.

- **Survivable Telecommunications Services**

The service must have geographic diversity and be capable of maintaining service through dynamic re-routing even though service points have been destroyed. There must be no single point of failure anywhere in the system.

- **Isolation and Independence from the Disaster Site's Local Loop**

The solution must provide both forwarding capability and independence from the local loop such that if forwarding is lost or is unattainable staff can still be reached.

References

- (1) Securing Our Nation's Cyber Infrastructure, Speech by President Obama, May 29, 2009.
http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure
- (2) CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, at 11.
- (3) Cyber in Security/ Strengthening the Federal Cybersecurity Workforce, Booz Allen Hamilton, July 2009
- (4) *High Risk Series: An Update* (GAO-09-271), Government Accountability Office, January 2009.
- (5) Securing Our Nation's Cyber Infrastructure, Speech by President Obama, May 29, 2009.
http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure
- (6) www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5,
CIA presentation, SANS SCADA Security Summit, January 16, 2008.
- (7) www.bankinfosecurity.com/article.php?art_id=1197, February 5, 2009.
- (8) www.infoworld.com/d/security-central/retailer-tjx/reports-massive-data-breach-952, January 17, 2007.
- (9) www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html.
See also <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>, McAfee,
"Unsecured Economies: Protecting Vital Information", January 2009. Projection based on survey by Purdue's Center for
Education and Research in Information Assurance and Security.
- (10) National White Collar Crime Center, 1. The National Public Survey on White Collar Crime, August 2005.
- (11) Next Generation Risk Management, Information Security Transformation for the Federal Government UCDMO Conference
September 1, 2009 Dr. Ron Ross, Computer Security Division, Information Technology Laboratory
- (12) Brecht, Lyle A., Capital Markets Research, "National Cyber Systems Infrastructure Security Review Concept Paper
" February 15, 2009
- (13) 2009 Business Software Alliance, "National Security & Homeland Security Councils Review of National Cyber Security Policy,"
March 19, 2009
- (14) Homeland Security Business Report, BUSINESS CONTINUITY & DISASTER RECOVERY /EMERGENCY RESPONSE,
July 11, 2007

Contact Information

U.S.A.

Mr. Michael Rosenberg

Executive Vice President

Office: (240) 453-6308 (U.S.A.)

mrosenberg@telecontinuity.com

JAPAN:

Mr. Takanobu Ito (Taka Ito)

Managing Director

Asian Pacific & Middle East Operations

Cell: 090-3095-4481 (Japan)

taka@telecontinuity.com

Thank you very much.