Cyber Security & Defining Enterprise Security Frameworks

www.infogistic.com

Background & Agenda

- Session 1: Understanding Cyber Security (45 min)
- Session 2: Critical Controls for Cyber Security (45 min)
- Session 3: Developing Enterprise Security Frameworks (45 min)

Presentation Team

- **Muhammad Furqan Khan, Chief Consulting Officer**
  - 20+ years diverse IT experience
  - Only Authorized Certified CMMI® Instructor in Pakistan
  - Certified in Risk and Information Systems Control (CRISC) by ISACA
  - Lead Auditor for ISO 9001 (QMS) & ISO 27001 (ISMS)
  - Led and managed projects to achieve & retain CMMI ML 5 Rating, certifications against ISO 20000 (ITSM), ISO 27001 (ISMS) and ISO 9001 (QMS)
  - Promoted CMMI & Information security and enabled more than 12 organizations to implement CMMI model, and several organization to achieve ISO 27001 certification

Presentation Team

- **Syed Abid Ali, Chief Commercial Officer**
  - Over 10 years of experience in Technology Management & Information Security
  - Graduate in Technology Management from University of London
  - Technology Consultant for the Doha Asian Games 2006
  - Co-Chapter Leader for OWASP Lahore
  - Member of the “CIIP” Law Review committee of Qatar
  - Worked with Technology Partners like Raytheon and Lockheed Martin for developing cyber security frameworks for sensitive organizations

INFOGISTIC

- Founded in 2011 with a vision to play a major role in Information Technology in the global landscape
- Headquartered in Lahore, Pakistan with our regional office in Doha, Qatar
- Strategic Presence in ME with our regional partners in Oman & KSA
- Strong focus on Consulting & Technology
- Global Customer base
- ISO 27001
- WINNER|Best Start-Up|P@SHA ICT Awards 2012
- WINNER | Start up to Watch | All World Network

Understanding Cyber Security

www.infogistic.com

Advent in Technology

- Information Technology becoming a corner stone
- Cloud Computing
- Social Media
- Business beyond boundaries

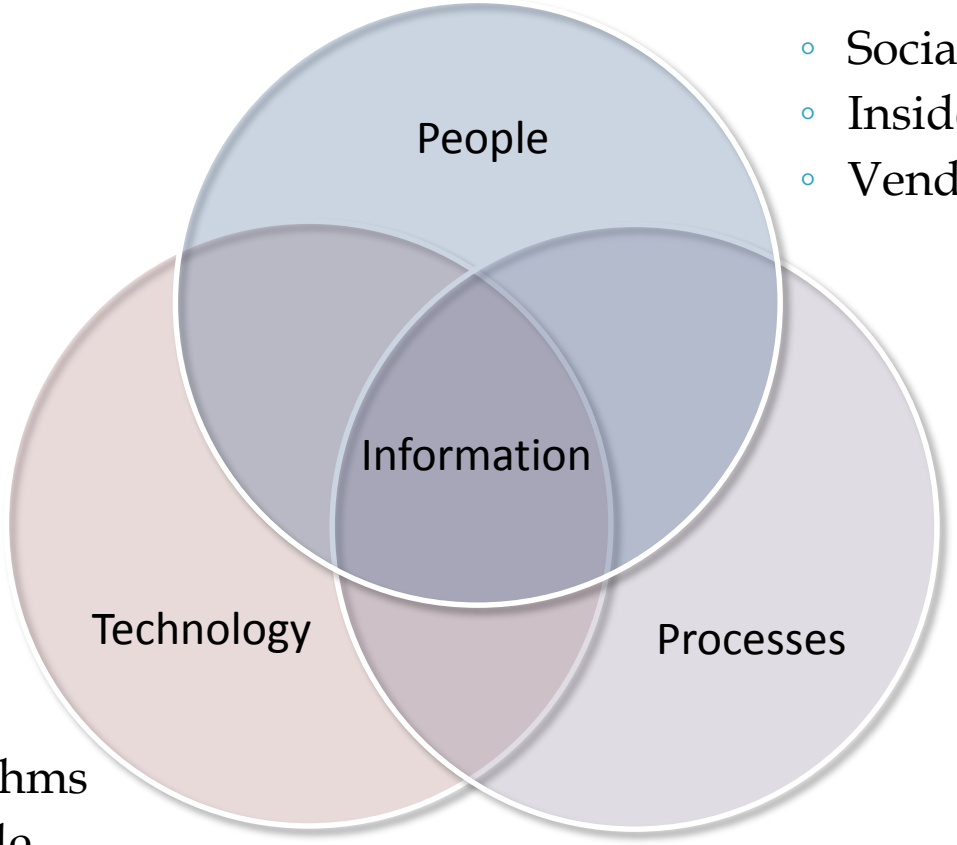
What made it possible ?

INTERNET

Managing Identity

Financial Network	• Credit Card • Account Number • Debit Card Number
Transportation Network	• License ID • Boarding Number
Health Network	• MR Number • Insurance Number
Internet	• ?????

Threats & Risks

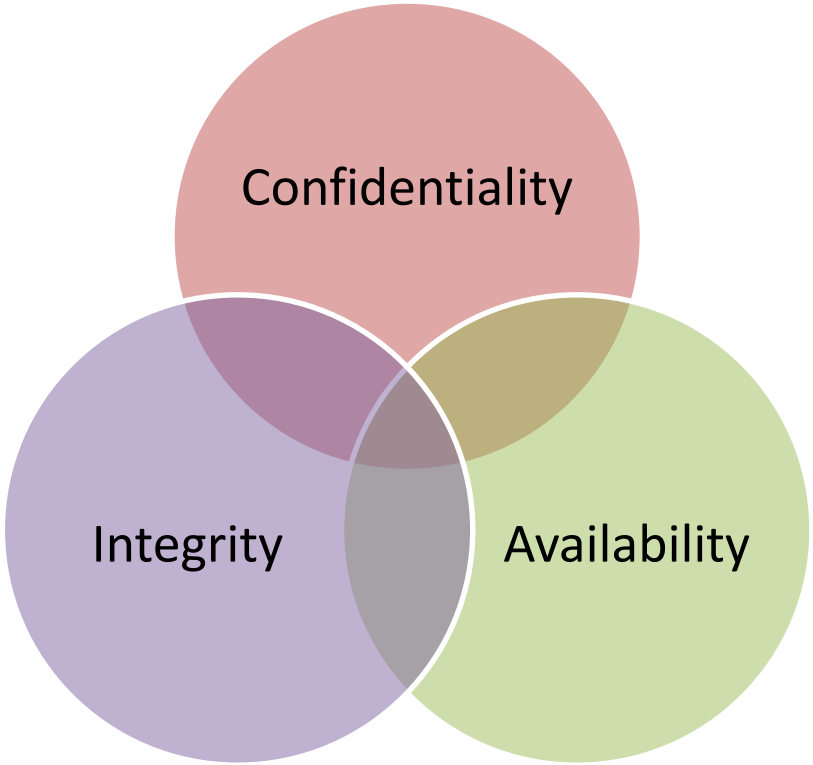


- Social Engineering
- Insider Threats
- Vendors & Employees

- Key Loggers
- Hacking
- Weak Algorithms
- Malicious code
- Denial of Service

- Natural Disasters
- Access Controls

Pillars of Information Security



Information Security vs Cyber Security

Cyber Security – Military Context

- Military leaders define cyberspace as using electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and related physical infrastructures.

"Cyberspace is a domain that we need to defend, just like the air, land, and sea,"

- Cyber Security means protecting critical infrastructure assets from unauthorized and unintended use

Understanding the difference

Cyber Security

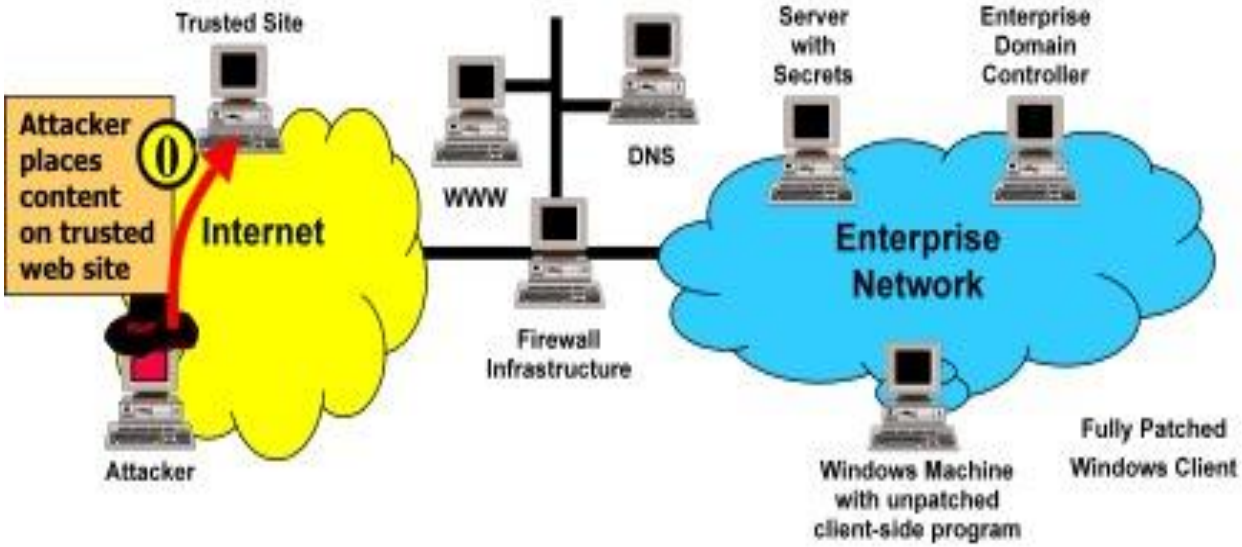
- Focus is on Infrastructure and information assets both
  - Electricity
  - Production
  - SCADA
  - Building Management
  - Command & Control
  - Information Systems
- Far reaching impact

Information Security

- Focus is on Information Assets
  - Databases
  - Servers
  - Website
  - Critical records
  - Applications
- Limited impact

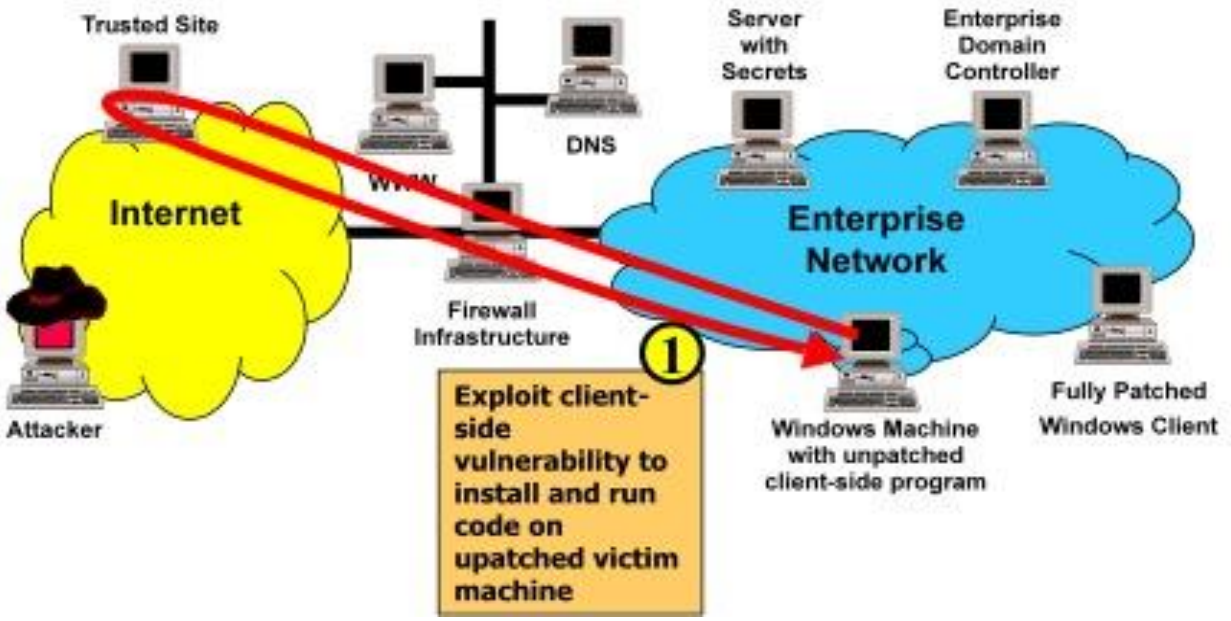
How it Works

- Step – 0 : Placing Content on Trusted Site



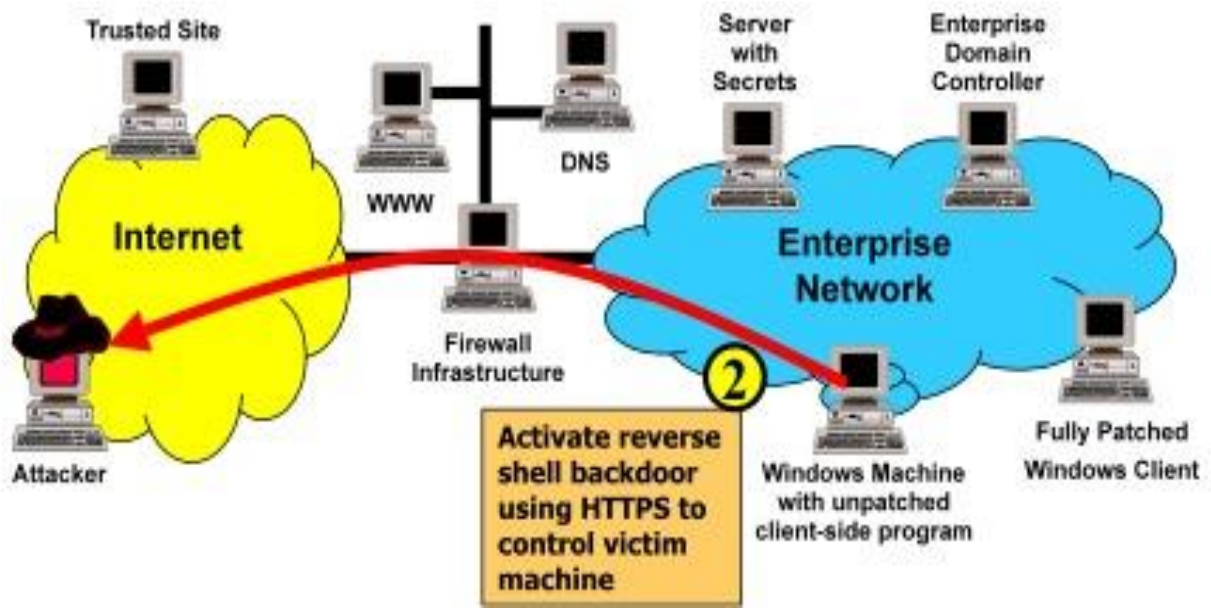
Cyber Security – Example cont..

- Step – 1 : Client Side Exploitation



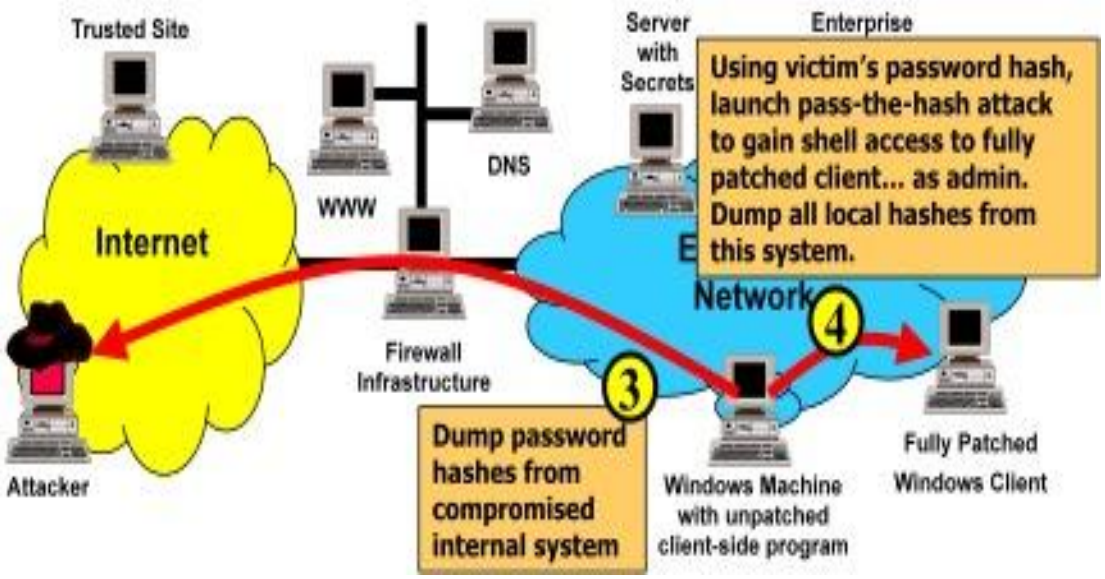
Cyber Security – Example cont..

- Step 2 : Establish Reverse Shell Backdoor using Https



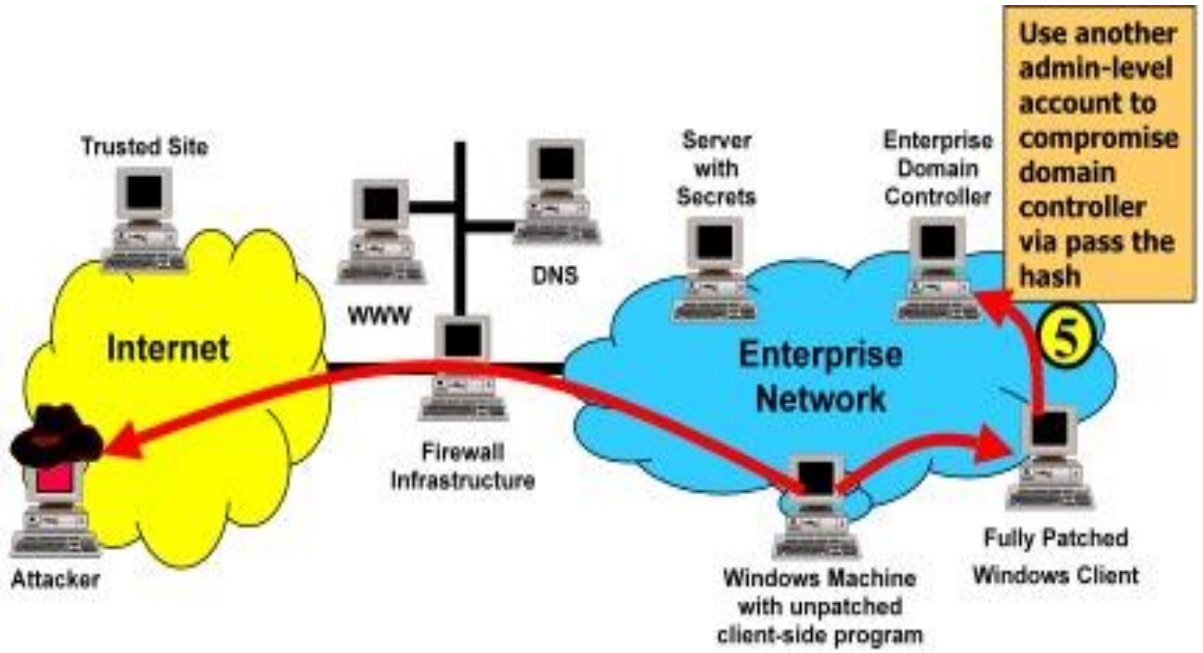
Cyber Security – Example cont..

- Steps 3 & 4: Dump Hashes and Use Pass-the-Hash Attack to Pivot



Cyber Security – Example cont..

- Step 5: Pass the Hash to Compromise Domain Controller



Cyber Security – Example cont..

- Steps 6 and 7: Exfiltration
  - In Step 6, with full domain administrator privileges, the attacker now compromises a server machine that stores secrets for the organization.
  - In Step 7, the attacker exfiltrates this sensitive information. The attacker pushes this data out to the Internet from the server, again using HTTPS to encrypt the information, minimizing the chance of it being detected.

Cyber Security - Events

- Events in Estonia (2007) – Redefined Cyberspace
  - A series of cyber attacks that began in April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks and ministries.
- Conflicts between Russia & Georgia (2008)
  - A series of cyber attacks that disabled websites of numerous South Ossetian, Russian, Georgian, and Azerbaijani organizations.
- Stuxnet,(*a virus developed to impact SCADA systems*) discovered in June 2010, 60% of infected systems were in Iran.
- Computer spies broke into the Pentagon's $300 billion Joint Strike Fighter project
- Cyber Attack on Saudi Aramco (KSA) & Ras Gas (Qatar) impacting entire network and disturbing services.

Cyber Security - Threats

- **Stuxnet: Cyber Security Trojan Horse:**
  - Stuxnet is a computer worm discovered in June 2010
  - It initially spreads via Microsoft Windows, and targets Siemens industrial software and equipment
- **Stuxnet: How it worked:**
  - Through the use of thumb drives in computers that were not connected to the Internet, a malicious software program known as Stuxnet infected computer systems that were used to control the functioning of a nuclear power plant

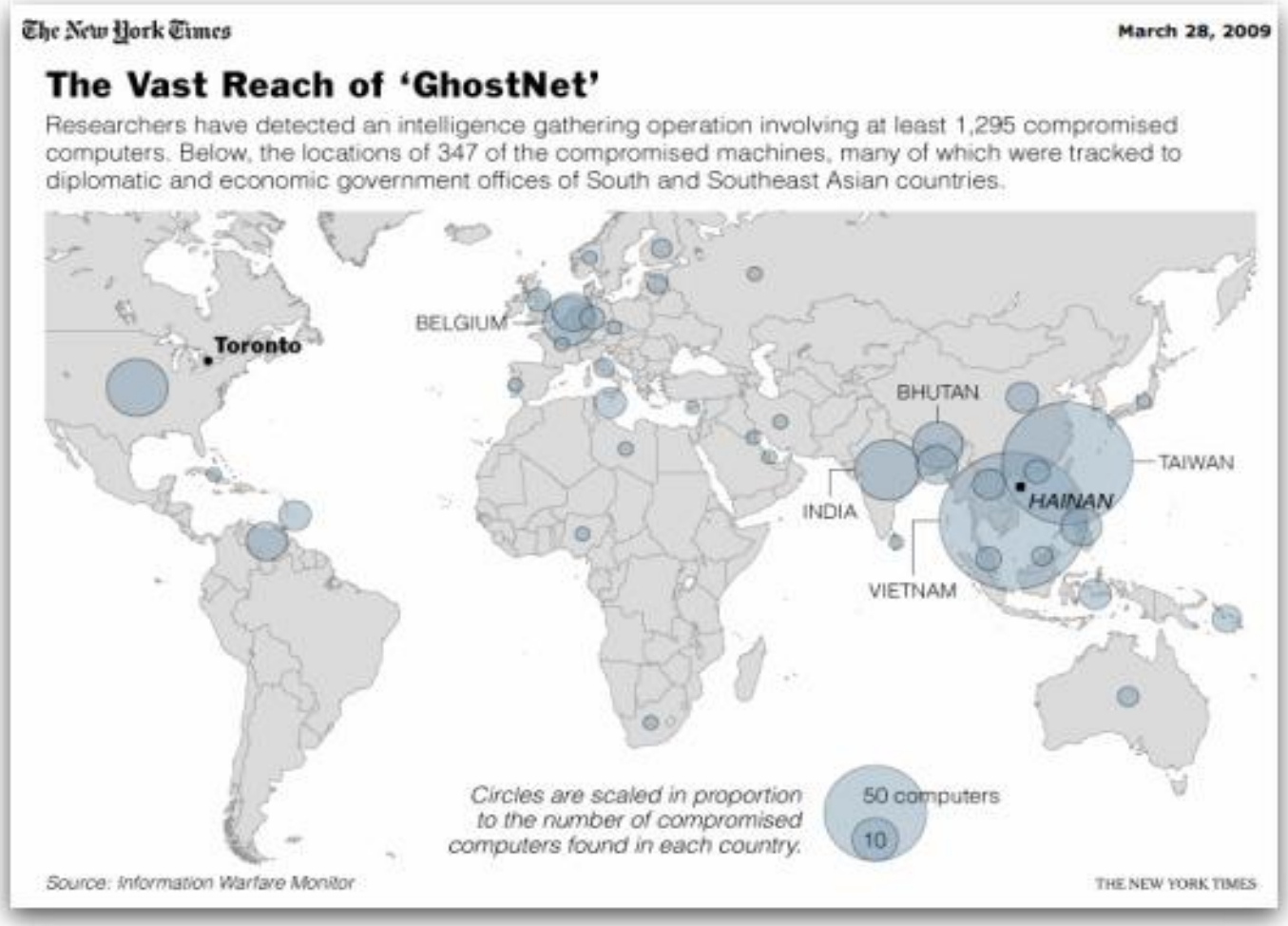
Congressional Research Service - The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.

Cyber Security - Threats

- **GhostNet: Cyber Security - RAT:**
  - GhostNet is the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying operation discovered in March 2009
  - The operation is likely associated with an Advanced Persistent Threat
  - Its command and control infrastructure is based mainly in the People's Republic of China and has infiltrated high-value political, economic and media locations in 103 countries
  - Computer systems belonging to embassies, foreign ministries and other government offices, and the Dalai Lama's Tibetan exile centers in India, London and New York City were compromised

Cyber Security - Threats

- **GhostNet: The Vast Reach:**



Cyber Security - Threats

- **GhostNet: Cyber Security RAT:**
  - Infecting at least 1,295computers in 103 countries, of which close to 30% can be considered as high-value diplomatic, political, economic, and military targets
  - Documentation and reverse engineering of the *modus operandi* of the GhostNet system—including vectors, targeting, delivery mechanisms, data retrieval and control systems—reveals a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems

Cyber Security - Threats

- **GhostNet – How it work:**
  - Emails are sent to target organizations that contain contextually relevant information. These emails contain malicious attachments, that when opened, drop a Trojan horse on to the system
  - This Trojan connects back to a control server, usually located in China, to receive commands. The infected computer will then execute the command specified by the control server
  - Occasionally, the command specified by the control server will cause the infected computer to download and install a Trojan known as Ghost Rat that allows attackers to gain complete, real-time control of computers running Microsoft Windows
  - Such a computer can be controlled or inspected by attackers, and even has the ability to turn on camera and audio-recording functions of infected computers, enabling monitors to perform surveillance

A real time example

Reply Reply All Forward

Tue 10/8/2013 10:45 PM

ali.abid@infogistic.com

Fw: Annual Form - Authorization to Use Privately Owned Vehicle on State Business

To akmal.javed@infogistic.com

Message Form_infogistic.com.zip (10 KB)

*** This Message Has Been Sent Using BlackBerry Internet Service from Mobilink ***

-----Original Message-----
From: "Newton Young" <Newton@infogistic.com>
Date: Tue, 8 Oct 2013 08:57:28
To: <ali.abid@infogistic.com>
Subject: Annual Form - Authorization to Use Privately Owned Vehicle on State Business

All employees need to have on file this form STD 261 (attached). The original is retained by supervisor and copy goes to Accounting. Accounting need this form to approve mileage reimbursement.

The form can be used for multiple years, however it needs to re-signed annually by employee and supervisor.

Please confirm all employees that may travel using their private car on state business (including training) has a current STD 261 on file. Not having a current copy of this form on file in Accounting may delay a travel reimbursement claim.

Cyber Security – Insider Threats

- In announcing results of the 2010 CyberSecurity Watch Survey, conducted by CSO magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University, and Deloitte, the authors wrote:

> "*While outsiders are the main culprits of cybercrime in general, the most costly or damaging attacks are more often caused by insiders*"

- Department of Defense, USA (DoD) report indicates that 87 percent of identified intruders into DoD information systems were either employees or others internal to the organization

(DoD, Insider Threat Mitigation Report, 2000)

Cyber Security – Insider Threats

- **Obama Helicopter Plans Leaked via P2P**
  - On 25 February 2009, Tiversa, a peer-to-peer (P2P) monitoring services provider, announced that it had discovered files with highly sensitive military information — including engineering details about U.S. President Barack Obama's helicopter — on a file-sharing node at an IP address in Tehran, Iran
  - Tiversa reported having traced the files' origin to a military contractor with an IP address in Bethesda, Maryland
  - The company found a file detailing the helicopter's blueprints and avionics package, which it then traced to its original source

http://blogs.computerworld.com/obama_marine_one_helicopter_iran_p2p_theskyisfalling

http://www.gartner.com/id=903312

http://www.foxnews.com/politics/2009/03/01/report-marine-information-iran/

Cyber Security Attack Types

Type	Motivation	Target	Method
Information Warfare	Military or political dominance	Critical infrastructure, political and military assets	Attack, corrupt, exploit, deny, conjoint with physical attack
Cyber Espionage	Gain of intellectual Property and Secrets	Governments, companies, individuals	Advanced Persistent Threats
Cyber Crime	Economic gain	Individuals, companies, governments	Fraud, ID theft, extortion, Attack, Exploit
Cracking	Ego, personal enmity	Individuals, companies, governments	Attack, Exploit
Hactivism	Political	Governments, Companeis	Attack, defacing
Cyber Terror	Political	Innocent victims, recruiting	command and control, computer based violence

Recent Incidents

Security Bugs in Telenor Website Could Reveal IMEI, Handset Details and Other Info of 30 Million Customers

A hacker from Pakistan yesterday unveiled a critical vulnerability in Telenor Pakistan's website that could be exploited to find out handset related information of Telenor's entire customer base.

Instead of mis-using this vulnerability in Telenor's system, the hacker decided to report the bug to Telenor Pakistan — through ProPakistani — which was eventually fixed by Telenor later in the evening.

Through this specific security flaw anyone, with little computing knowledge, could find out the handset model of Telenor number holders. Additionally, the IMEI number, IMSI, ICCID numbers could also be displayed to anyone. With this bug, anyone could blacklist a Telenor number.

By simply entering the Telenor number of a customer into the system, anyone could find out the history of mobile phone models that the customer had used during his relationship with Telenor Pakistan.

Hacker, who wants to remain anonymous, told ProPakistani that he had found this vulnerability while browsing the website, exposing that anyone could have found the bug and had mis-used this serious bug to find out information of Telenor customers.

Responding to ProPakistani's query on the matter, Ms. Atifa Asghar, Director Corporate Communications & Responsibility, Telenor Pakistan said that her company places a strong emphasis on confidentiality

"Yesterday, we became aware that through a particular mechanism it had become possible to extract handset related information like IMEI".

Atifa Asghar, Director Communications, Telenor Pakistan

And it continues….

Why

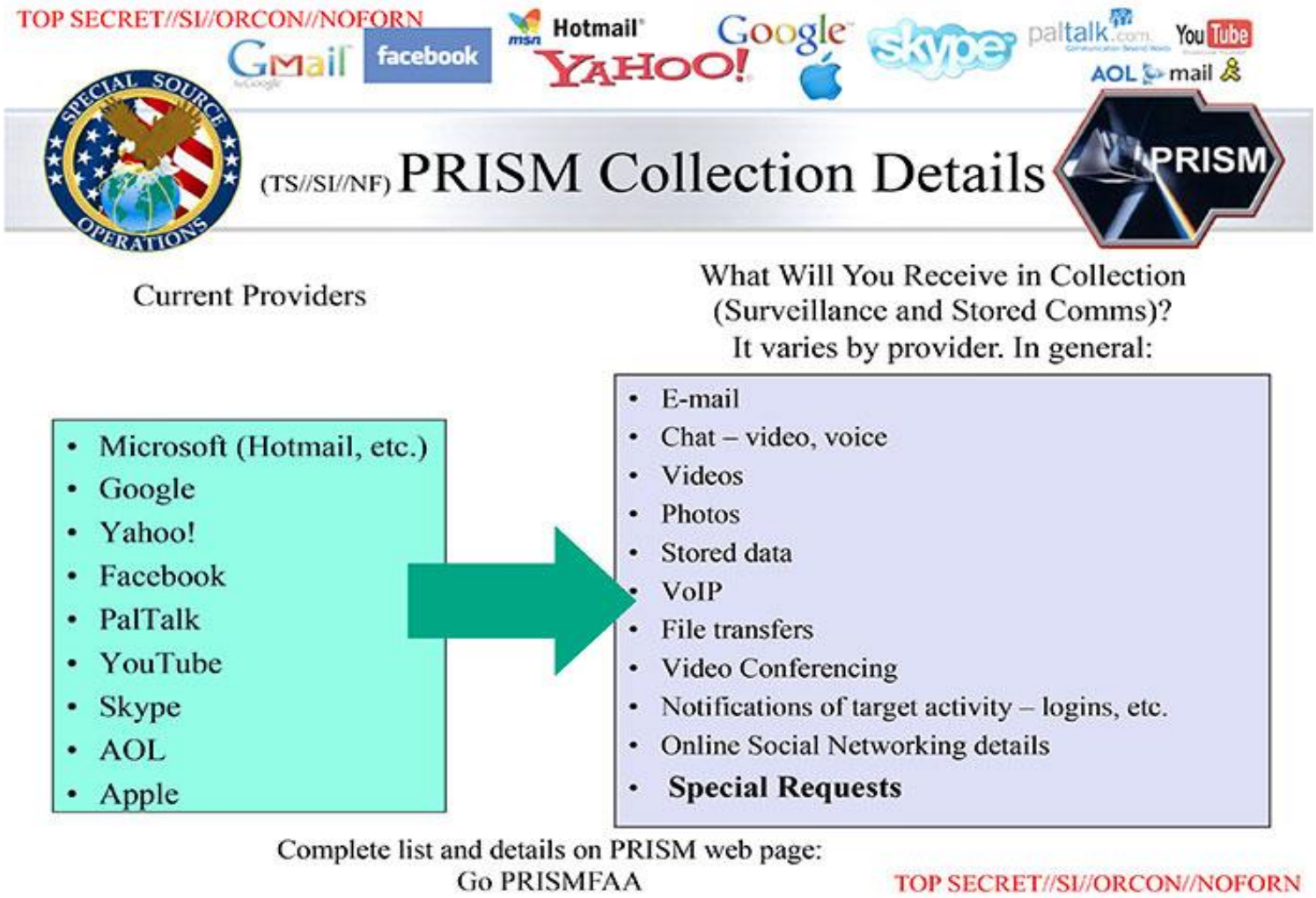
- No identification of the cyber crime groups
- No active law for cyber crime exists
- People believe that data & information security is the responsibility of the IT and specifically IT Security team which is wrong
- Too much emphasis on security technology controls
  - What a firewall can stop if runs on any- any?
  - What an IPS can stop that is not fine tuned properly
  - What a technology can do if the employee willfully shares his salary with his colleagues
  - What an administrator can do if the user do not change his password
  - What an information security officer can do if confidential documents are found in the dust bins

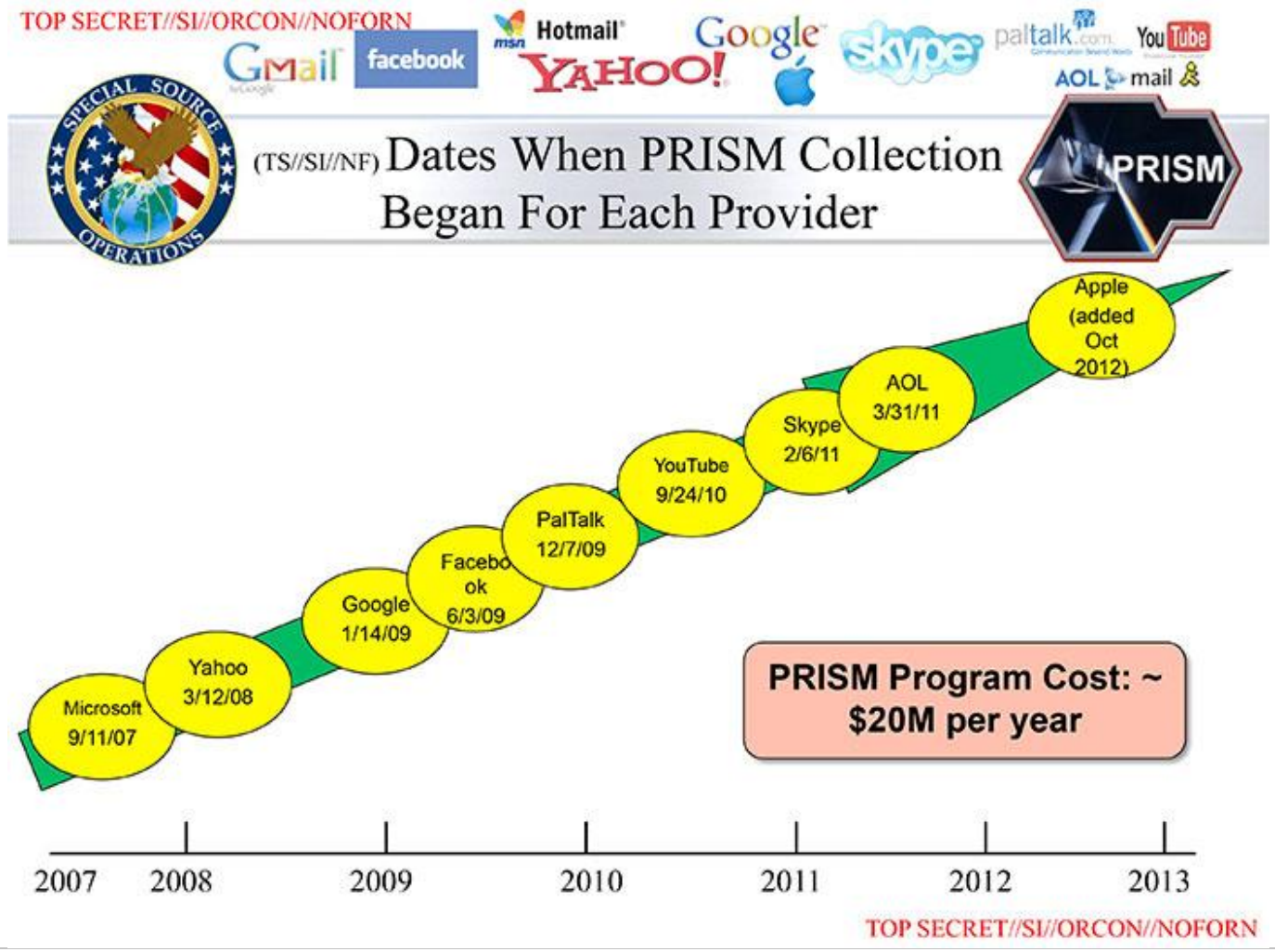
Story of the day

What he leaked

- Over 200,000 confidential and secret documents of National Security Agency leaked
- NSA collects records of every U.S. phone call under a call log metadata program.
- In October, the Washington Post revealed that the spy agency managed to infiltrate the clouds of Google and Yahoo, from which Americans' data can be collected.
- NSA collected 21.98 billion phone calls in Afghanistan, **12.76 billion in Pakistan**, 7.8 billion in Iraq, 7.8 billion Saudi Arabia, 1.9 billion in Egypt, 1.73 billion in Iran, and 1.6 billion Jordan.
- Spying operation on world leaders like German Chancellor, Cuban President etc.

How it is done





Conclusion

Privacy as they say is a 20th Century Concept

Thank You