Economic and Social Impact of IT Security

Eng. Qusai AlShatti

Board Member

Kuwait Information Technology Society

Conduct in Cyberspace

- Transactions ⟹ E-Commerce, E-Government
- Actions (Interaction) ⟹ E-Mail, Social Networks, Hacking
- Content (Publishing) ⟹ Text, Videos, Music
- Rights ⟹ Intellectual Property, Consumer Protection
- Security and Privacy ⟹ Infrastructure, Data, Assets – Cross Cutting with the Above.

Cyber Threats

Threats	Targets
• Against information • Against ICT infrastructures	• Governments • Private sector • Citizens

Threats Against Information

- Espionage. Within this category all varieties of espionage are included, from state espionage to industrial espionage.
- Theft and publication of classified or sensitive information.
- Theft and publication of personal data.
- Digital identity theft.
- Fraud.
- Advanced Persistent Threats (APT).

Threats against ICT infrastructure

- Attacks against critical infrastructures.
- Attacks against networks and systems.
- Attacks against internet services.
- Attacks against industrial networks and control systems.
- Malware infection.
- Attacks against networks, systems or services through third parties.

Cyber Threats Impact

- Loss (Information, Financial)
- Miss-handling (Information, Infrastructure)
- Disclosure (Information)
- Misuse (Information)
- Temporary, partial or total interruption of certain services or systems

Authorship

- **State sponsored attacks:** Real world or physical conflict has extended to the virtual world of cyber space. Cyber attacks have been detected against the critical infrastructures of countries and specific strategic objectives.
- **Attacks by private organizations:** The objective of many private organizations is to obtain industrial secrets from other organizations or governments.

Authorship

- **Terrorism, political, ideological extremism:** Terrorists and extremist groups use cyber space to plan and publish their actions and acquire recruits to carry them out.
- **Attacks by groups of organized crime:** gangs obtaining sensitive information for fraudulent use and for significant economic gains.
- **Hacktivism:** Attack the cyber space that violate any of their principles or interests making it susceptible to denial of service attacks (DDoS) or stealing sensitive information for free distribution on the Internet.

Authorship

- **Low profile attacks:** Cyber attacks of a highly heterogeneous nature executed by people with certain ICT knowledge for fundamentally personal reasons.
- **Personal privileged access attacks (insiders):** This group poses one of the greatest threats to the cyber space security of nations and companies as they are often an integral part of all the attacks outlined above.

Cyber Statistics

Poll Conducted By EastWest Institute (Global Companies CEOs):

- **93%** think that the cyber security risk is higher than one year ago.
- **33%** feel protected online.
- **41%** think their online privacy is not sufficiently protected.
- **50%** think that corporate boards grossly underestimate the cyber security problem.
- **17%** think that they are too confused.
- **55%** doubt their countries can defend itself against sophisticated cyber attacks.
- **62%** think their country at an early stage of understanding cyber security problems.

Cyber Statistics

Cybercrime	Estimated Daily Activity
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

Major Threats of IT Security

- Online Identity Theft
- Industrial & State Espionage
- Critical Infrastructure Attack
- Botnets (Fishing & Spam)
- Unauthorized access
- Theft or breach of confidential information
- Denial-of-service attack

Financial Loss

- In 2014, it is estimated that cybercrime cost the world between $345 billion and $445 billion which is 0.62% of the global economy of GDP.
- In 2016, it is estimated that cybercrime cost the world $600 billion which is 0.8% of the global economy of GDP.

In Terms of Regions

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

SPAM (Botnet) Threats

- In 2010 the “King of Spam” was arrested in the United States, a 23 years old Russian who sends daily 10 billion emails from a network of over 500,000 computers (Zombies) controlled by a botnet “Mega-D”.

Emerging Trends in Cybercrime

Ransomware: Toolkits available online from $10 - $3000. Currently, it is estimated more than 6,000 online criminal marketplaces sell ransomware products and services, offering more than 45,000 different products.

Cybercrime-as-a-Service: "The Onion Router" (TOR) dubbed as The Dark Web, allows users to browse the internet anonymously by encrypting their traffic and then routing it through multiple random relays on its way to its destination.

Europol found that the Tor network had more than 2.2 million users and hosted almost 60,000 unique onion domains with 57% hosting illegal content.

Underground Economy

- **Real asset theft:** stealing money from the stolen bank accounts or credit cards;
- **Network virtual asset theft:** stealing virtual currency, equipment from stolen online game accounts, and selling them for real money;
- **Internet resources and services abuse:** taking advantage of the snatched Internet resources including compromised hosts, hacked servers, and infected smart phones, to abuse the Internet services for profit;
- **Black hat techniques, tools, and training:** selling Trojan horses and attack tools employed to provide technical support for the cybercriminals, and providing training services to newbies.

Organizations Not Reporting IT Security Incidents

- Negative publicity would the organization.
- Unaware competent authorities were interested.
- The perpetrators would not be caught.
- Organization didn’t believe competent authorities had the capability to effectively investigate the incident.
- Did not think incidents was serious enough.
- Civil remedy seemed the best option.

Social Impact of IT Security

- Children disclosure of private information to strangers.
- 87% of Parents who their children had a negative experience online became victims of cybercrimes.
- 82% of Children who broke Internet House rules suffered negative experience online.

Risky Behavior on Social Networks

- 1 out of 3 users do not log out after each session.
- 1 out of 5 users do not check shared links.
- 1 out of 6 users do not know if their settings are public or private.
- 3 out of 10 users received posts or messages suspect not actually from friends.
- 36% accepted friendship from people they do not know.

Email Potential Threat

- 50% send personal photographs using emails.
- 22% send Bank statements
- 17% send passwords for other online accounts.
- 40% do not use complex passwords or change passwords regularly.

Remedies

- Information Sharing and Encourage Reporting
- Social Contract
- Make information security everyone's responsibility including Senior management
- Make education and training an ongoing exercise
- Hold Security Audit
- Keeping abreast of changes in security technology and best practices - a priority
- Regulation (Accountability)
- Underpin a robust security culture with frequent and rigorous testing

Thank You