Insecure Cyberspace: Today’s Cyber Threats

25/11/2014
4th ISACA Athens’ Chapter Conference
Athens, Greece
Francesca Bosco
Presentation Overview:

- What is UNICRI?
- Today’s Cyber threats
  - Cybercrime & its Costs
  - The world of Hackers
  - Ransomware
  - Organized Crime and Cyberspace
    - The Underground Economy
    - Links to Human Trafficking
- Case studies
- Conclusions
UNICRI: What we do...

The activities of the Emerging Crimes Unit regarding fighting and preventing cyber threats concentrate on:

- Profiling hackers and cybercriminals
- Evolution of the criminal business model: organized crime links
- Analysis of cybercriminals’ modus operandi
- Comprehensive evaluation of case studies
- Specific focus: terrorists’ use of the internet, cyberwar and cyberterrorism
- Evolution of cybersecurity
Europol’s annual iOCTA provides stakeholders in the field of cybersecurity with the ability to share information and gain an up-to-date understanding of the major threats and trends in the field of organized cyber crime.

This year’s key findings can be found here:
Today’s Cyber Threats

CYBER SECURITY THREATS ARE RISING
## Current Cyber Threats

<table>
<thead>
<tr>
<th>Top Threats</th>
<th>Current Trends</th>
<th>Top 10 Threat Trends in Emerging Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Drive-by Downloads</td>
<td>↑</td>
<td>↑</td>
</tr>
<tr>
<td>2. Worms/Trojans</td>
<td>↑</td>
<td>↑</td>
</tr>
<tr>
<td>3. Code Injection</td>
<td>↑</td>
<td>↑</td>
</tr>
<tr>
<td>4. Exploit Kits</td>
<td>↑</td>
<td></td>
</tr>
<tr>
<td>5. Botnets</td>
<td>←</td>
<td>↑</td>
</tr>
<tr>
<td>6. Physical Damage/Theft/Loss</td>
<td>↑</td>
<td>↑</td>
</tr>
<tr>
<td>7. Identity Theft/Fraud</td>
<td>↑</td>
<td>↑</td>
</tr>
</tbody>
</table>

Sources: Enisa, Threat Landscape Report December 2013
<table>
<thead>
<tr>
<th>Top Threats</th>
<th>Current Trends</th>
<th>Top 10 Threat Trends in Emerging Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>8. Denial of Service</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>9. Phishing</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>10. Spam</td>
<td><img src="image" alt="Stable" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>11. Rogueware/Ransomware/Scareware</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>12. Data Breaches</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>13. Information Leakage</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>14. Targeted Attacks</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
<tr>
<td>15. Watering Hole</td>
<td><img src="image" alt="Increasing" /></td>
<td><img src="image" alt="Increasing" /></td>
</tr>
</tbody>
</table>

Legend:  Trends: ![Declining](<image>) Declining, ![Stable](<image>) Stable, ![Increasing](<image>) Increasing

Sources: Enisa, Threat Landscape Report December 2013
Estimating the Enormous Cost of Cybercrime

<table>
<thead>
<tr>
<th>CRIMINAL ACTION</th>
<th>ESTIMATED COST</th>
<th>PERCENT OF GDP</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOBAL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Piracy</td>
<td>$1 billion to $16 billion</td>
<td>0.008% to 0.02%</td>
<td>IMB</td>
</tr>
<tr>
<td>Drug Trafficking</td>
<td>$600 billion</td>
<td>5%</td>
<td>UNODC</td>
</tr>
<tr>
<td>Global cyber activity</td>
<td>$300 billion to $1 trillion</td>
<td>0.4% to 1.4%</td>
<td>Various</td>
</tr>
<tr>
<td>US ONLY</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Car Crashes</td>
<td>$99 billion to $168 billion</td>
<td>0.7% to 1.2%</td>
<td>CDC, AAA</td>
</tr>
<tr>
<td>Pilferage</td>
<td>$70 billion to $280 billion</td>
<td>0.5% to 2%</td>
<td>NRF</td>
</tr>
<tr>
<td>US- cyber activity</td>
<td>$24 billion to $120 billion</td>
<td>0.2% to 0.8%</td>
<td>Various</td>
</tr>
</tbody>
</table>

Source: The Economic Impact of Cybercrime and Cyber Espionage 2013 – CSIS & McAfee
The estimated cost of all households impacted by spyware, viruses, and phishing is $4,500,000,000.

- **8 Million Households** have had spyware problems in the past 6 months.
- **24% of PCs** on average worldwide were not protected by up-to-date antivirus software.
- **1 Million Households** lost money or compromised accounts from misused phishing.

Sources:
http://www.statisticbrain.com/computer-virus-statistics/
Cybercriminals: The Hackers Profiling Project
Hacking Eras & Generations

- **First generation** (1970’s): driven by need for knowledge.
- **Second generation** (early 1980’s): driven by curiosity and need for knowledge; later on (1985-1990) hacking becomes a trend.
- **Third generation** (1990’s): driven by addiction, curiosity, establishing networks, information sharing.
- **Fourth generation** (2000-to present): driven by eagerness and money. Here hacking meets with politics (*cyber-hacktivism*) or with the criminal world (*cybercrime*).
Project phases - starting September 2004

1 – Theoretical collection: Questionnaire, Existing literature

2 – Observation: Participation in IT underground security events

3 - Filing: Database for elaboration/classification of data (phase 1/phase 4)

4 - Live collection: Highly customized, new generation Honeynet systems

5 – Gap analysis: data from: questionnaire, honeynet, existing literature

6 – HPP “live” assessment of profiles and correlation of modus operandi through data from phase 4

7 – Final profiling: Redefinition/fine-tuning of hackers profiles used as “de-facto” standard

8 – Diffusion of the model: elaboration of results, publication of the methodology, raising awareness
Variables

- Modus Operandi
- Isolated VS Collective activities
- Motivations
- Selected targets
- Career
- Ethics
- Crashed or damaged systems
- Perception of illegality
- Effect of laws, convictions and technical difficulties as a deterrent
### Analysis and Correlation of Profiles

**TB.1**

<table>
<thead>
<tr>
<th>PROFILE</th>
<th>RANK</th>
<th>IMPACT LEVEL</th>
<th>TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>Amateur</td>
<td>NULL</td>
<td>End - User</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td></td>
<td>LOW</td>
<td>SME</td>
</tr>
<tr>
<td>Specifying Security Flaws</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cracker</td>
<td>Hobbyist</td>
<td>MEDIUM</td>
<td>Business Company</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>Hobbyist</td>
<td>MEDIUM</td>
<td>Vendor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Technology</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled</td>
<td></td>
<td>MEDIUM</td>
<td>On Necessity</td>
</tr>
<tr>
<td>Hacker</td>
<td></td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>Cyber Warrior</td>
<td>Professional</td>
<td>HIGH</td>
<td>&quot;Symbol&quot; Business</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Company</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td></td>
<td>HIGH</td>
<td>Business Company</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Corporation</td>
</tr>
<tr>
<td>Government Agent</td>
<td></td>
<td>HIGH</td>
<td>Strategic Company</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Individual</td>
</tr>
<tr>
<td>Military Hacker</td>
<td></td>
<td>HIGH</td>
<td>Government</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strategic Company</td>
</tr>
<tr>
<td>OFFENDER ID</td>
<td>LONE / GROUP HACKER</td>
<td>TARGET</td>
<td>MOTIVATIONS / PURPOSES</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wanna Be Lamer</td>
<td>GROUP</td>
<td>End-User</td>
<td>For fashion, It’s “cool” =&gt; to boast and brag</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>GROUP: but they act alone</td>
<td>SME / Specific security flaws</td>
<td>To give vent of their anger / attract mass-media attention</td>
</tr>
<tr>
<td>Cracker</td>
<td>LONE</td>
<td>Business company</td>
<td>To demonstrate their power / attract mass-media attention</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>LONE / GROUP (only for fun)</td>
<td>Vendor / Technology</td>
<td>For curiosity (to learn) and altruistic purposes</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>LONE</td>
<td>On necessity</td>
<td>For curiosity (to learn) =&gt; egoistic purposes</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>LONE</td>
<td>“Symbol” business company / End-User</td>
<td>For profit</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>LONE</td>
<td>Business company / Corporation</td>
<td>For profit</td>
</tr>
<tr>
<td>Government Agent</td>
<td>LONE / GROUP</td>
<td>Government / Suspected Terrorist/Strategic company/Individual</td>
<td>Espionage/Counter-espionage Vulnerability test Activity-monitoring</td>
</tr>
<tr>
<td>Military Hacker</td>
<td>LONE / GROUP</td>
<td>Government / Strategic company</td>
<td>Monitoring / controlling / crashing systems</td>
</tr>
</tbody>
</table>
It is becoming increasingly difficult to pin-point the culprits of cyberviolations. The majority of cybercrime can be attributed to **Organized Criminal Groups, Governments and Hacktivists**. However, such a breakdown fails to account for the morphing definitions of the terms 'organized crime', 'government' and 'hacktivism' in cyberspace. The structure of Organized Criminal groups, hacktivist cohorts and the relationships between governments and economic forces, are evolving so quickly that the titles 'Organized Crime', 'Hacktivism' and 'Government' are meaningless in terms of cybersecurity. What is needed is a study that looks at the specific characteristics of each group that commits these crimes. Building upon HPP V1.0, which described the features of individual hackers, this project focuses on identifying the traits of Organized Cybercriminal groups, State sponsored attackers and Hacktivists that constitute cyberthreats.

For further details contact: bosco@unicri.it
What are cybercriminals interested in?

Data: is more valuable than money. Once spent, money is gone, but data can be used and reused to produce more money, or for further leverage.

Intellectual property: keep in mind
• a database of creditcards = easy to monetize
• a database of IP = monetizing stolen IP is much harder BUT also much more lucrative if done correctly.
Which types of data interest cybercriminals?

The top 5 types of data stolen:

1. Payment data (e.g. credit card information)
2. Authentication (e.g. user names & passwords)
3. Copyrighted material (e.g. software)
4. Medical records
5. Any classified information (from corporate and government to personal)
Evolving Threat: Ransomware

The Basics:

• A type of malware that allows hackers to lock you out of your own devices. Only by paying a ransom to the hacker can your device (possibly) be unlocked.

• Spread through botnets, downloads, email attachments, etc.

• Notorious ransomware include Cryptolocker, Reveton, Lyposit, Fake Android Defender (mobile phones).

• Running antivirus software can detect ransomware before it’s too late.
Hacking in the News
The FBI’s Most wanted Cybercriminals

Wanted by the FBI

Cyber’s Most Wanted
Select the images of suspects to display more information.

John Gordon Baden is allegedly responsible for stealing the identities of 10,000 people and then using the stolen information to siphon funds from their brokerage or bank accounts and purchasing expensive electronic items with their credit.

In July 2014, Baden was indicted by a federal grand jury in the Southern District of California. San Diego, California. He was charged with conspiracy to commit wire fraud, computer hacking, and wire fraud. His two co-conspirators, who have since been arrested, were indicted on similar charges.

Baden and his co-conspirators allegedly obtained mortgage applications containing customers’ personal identification information, such as names, dates of birth, social security numbers, addresses, assets, tax information, and driver’s licenses, by hacking into the company’s computer servers. While
Hackers or ‘hacktivists’?

Anonymous Declares War Against Hong Kong Police

The full video can be found here: https://www.youtube.com/watch?v=BFO0hN9Ptdc
Hackers or ‘cyber-warriors’?

21 February 2014 Last updated at 13:46 GMT

South Korea to develop Stuxnet-like cyberweapons

South Korea is to develop cyber-attack tools in an attempt to damage North Korean nuclear facilities.

The country’s defence ministry wants to develop weapons similar to Stuxnet, the software designed to attack Iranian nuclear enrichment plants.

The South Korean military will carry out missions using the software, the defence ministry said.

One computer security expert said that using cyberweapons could be “very dangerous”.

The defence ministry reported its plan to the government on 19 February, the Yonhap news agency reported.

In 2006, North Korea said it had successfully tested a nuclear weapon, spreading alarm through the region. Intensive diplomatic efforts to try to rein in North Korea’s nuclear ambitions continued.

Online propaganda

The development of weapons capable of physically damaging North Korean nuclear plants and missile facilities is the second phase of a
Hackers or ‘cyber-terrorists’?

Syria hackers target New York Times website

NYTimes.com, Twitter and others media websites briefly taken down by hackers loyal to Syrian President Bashar al-Assad.

Last Modified: 28 Aug 2013 02:23

Media companies including the New York Times, Twitter and the Huffington Post lost control of some of their websites after hackers supporting the Syrian government breached the Australian internet company that manages many major site addresses.

The Syrian Electronic Army, a hacker group that has previously attacked media organisations that it considers hostile to the government of Syrian president Bashar al-Assad, claimed credit for the Twitter and Huffington Post hacks in a series of Twitter messages late on Tuesday.

Security experts said electronic records showed that NYTimes.com, the only site with an hours-long outage, redirected visitors to a server controlled by the Syrian group before it went dark.

New York Times spokesman Eileen Murphy tweeted the "issue is most likely the result of a malicious external attack", based on an initial assessment.
Hackers or cyber-criminals?

3 October 2014 Last updated at 00:00 GMT

JP Morgan sees 76 million customer accounts hacked

JP Morgan has revealed it suffered a massive cyber attack on 76 million private and seven million business customers in the US.

The raid gathered account holders names and addresses but the bank said it did not involve critical information such as account and social security numbers.
Blending Cybercrime and Organized Crime
CRIME, ORGANIZED

The Mafia, la Cosa Nostra, the Yakuza, Mexican cartels—the underworld is ruled by a complex network of criminal groups. Here's how they fit together.

Flow of Transnational Organized Crime

Touch each number to read about a criminal organization.

1. United States of America
2. Central America
3. Caribbean
4. Central Africa
5. West Africa
6. West Central Europe
7. Russia
8. Middle East
9. Afghanistan
10. India
11. South-East Asia
12. China
13. Japan
14. South-East Asia
15. Japan

$128 billion
Total estimated value of organized criminal activity.

Click the icon to see a breakdown.
Why is cybercrime so attractive for Organized Crime groups?

• It’s a huge moneymaker: the EU alone lost €290 billion due to cybercrime in 2012. (Romanian President Traian Basescu)

• Relatively easy to recruit hackers in places like Romania, where English is taught in schools and participating in a few scams can easily surpass the average yearly income of about $14000.

• It is a growing field with guaranteed opportunities for cybercriminals to strike in the future. By 2017, approximately 70% of the global population will have mobile broadband subscriptions. (UNODC)
Organized crime typologies in cyberspace

Activities:
**Type A:** activities directed towards the digital environment
**Type B:** activities that switch between and across online and offline contexts
**Type C:** activities predominantly centered on offline criminal projects, but which increasingly intersect with digital environments.

Organization:
**Type A:** Swarms
**Type B:** Clustered Hybrids
**Type C:** Aggregates
**Type D:** Hubs
**Type E:** Extended Hybrids
**Type F:** Hierarchies
OC Activities Shift

**Original Crime**
- Local numbers gambling
- Heroin, cocaine trafficking
- Street prostitution
- Extortion of local businesses for protection
- Loan sharking
- Fencing stolen property

**Current Version**
- Offshore income stream and extortion directed against existing gambling sites
- Internet access to counterfeit prescription drugs/illegal drugs
- Online pornography empires/escort sites backed by human trafficking groups
- Extortion of corporations, kidnappings.
- Money laundering, precious stones, commodities.
- Theft of intellectual property.
Factors Contributing to the Increase in Organized Cybercrime

- Financial Crisis
- ICTs in Emerging Economies
- Availability and accessibility of hacking tools and online markets
A. The Financial Crisis

Criminal ‘commodity’ markets such as the trade of narcotics, prostitution and counterfeit goods have been in decline.

In their place fraud, espionage, and loan sharking markets have seen a steady rise. These activities are all mostly conducted ONLINE.

High rates of unemployment make it easy for criminal organizations to recruit young masterminds
B. ICTs in Emerging Economies

Accelerating developments in ICTs are stumbling across regulatory, cultural and social factors, including:

1. the lack of regulations dealing with data messages and recognition of electronic signatures;
2. the absence of specific legislation protecting consumers, intellectual property, personal data;
3. the lack of appropriate fiscal legislation covering electronic transactions;
4. the absence of laws dealing with cybercrime.
C. The availability and Accessibility of Hacking Tools

“DDoS bot ‘ibot’; price: US$350(for the first 5 customers)’’


<table>
<thead>
<tr>
<th>Offering</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-day DDoS service</td>
<td>US$30-70</td>
</tr>
<tr>
<td>1-hour DDoS service</td>
<td>US$10</td>
</tr>
<tr>
<td>1-week DDoS service</td>
<td>US$150</td>
</tr>
<tr>
<td>1-month DDoS service</td>
<td>US$1,200</td>
</tr>
<tr>
<td>Cheap email spamming service</td>
<td>US$10 per 1,000,000 emails</td>
</tr>
<tr>
<td>Expensive email spamming service using a customer database</td>
<td>US$50-500 per 50,000-1,000,000 emails</td>
</tr>
<tr>
<td>SMS spamming service</td>
<td>US$3-150 per 100-10,000 text messages</td>
</tr>
<tr>
<td>ICQ spamming service</td>
<td>US$3-20 per 50,000-1,000,000 messages</td>
</tr>
<tr>
<td>1-hour ICQ flooding service</td>
<td>US$2</td>
</tr>
<tr>
<td>24-hour ICQ flooding service</td>
<td>US$30</td>
</tr>
<tr>
<td>Email flooding service</td>
<td>US$3 for 1,000 emails</td>
</tr>
<tr>
<td>1-hour call flooding service (i.e., typically takes call center services down)</td>
<td>US$2-5</td>
</tr>
<tr>
<td>1-day call flooding service</td>
<td>US$20-50</td>
</tr>
<tr>
<td>1-week call flooding service</td>
<td>US$100</td>
</tr>
<tr>
<td>SMS flooding service</td>
<td>US$15 for 1,000 text messages</td>
</tr>
<tr>
<td>Vkontante.ru account database</td>
<td>US$5-10 for 500 accounts</td>
</tr>
<tr>
<td>Mail.ru address database</td>
<td>US$1.30-19.47 per 100-5,000 addresses</td>
</tr>
<tr>
<td>Yandex.ru address database</td>
<td>US$7-500 per 1,000-100,000 addresses</td>
</tr>
<tr>
<td>Skype SMS spamming tool</td>
<td>US$40</td>
</tr>
<tr>
<td>Email spamming andflooding tool</td>
<td>US$30</td>
</tr>
</tbody>
</table>

Table 5: DDoS service prices
As **cryptocurrencies** continue to evolve, it is likely that more niche currencies will develop, tailored towards illicit activity and providing greater security and true anonymity. Several Russian language underground forums have created their own private currencies. Schemes such as MUSD, the United Payment System and UAPS have been developed to cater specifically for these markets. Proliferation of these schemes will permit an entire criminal economy to flourish with little possibility of law enforcement intervention.

*(OCTA 2014: Chapter 3.5)*
Stolen Credentials on the Black Market in 2014: >360 million!

• In a recent investigation conducted by the firm Hold Security, an estimated 360 million stolen account credentials are for sale online, in addition to some 1.25 billion hacked email addresses.

• Also, a list of credentials for about 7,800 FTP servers is available on cybercrime forums in the Deep Web.

Average Prices by Account Type, 2013

<table>
<thead>
<tr>
<th>Item</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>$2.50</td>
</tr>
<tr>
<td>Twitter</td>
<td>$2.50</td>
</tr>
<tr>
<td>Wireless Mobile Provider Accounts</td>
<td>$4.00</td>
</tr>
<tr>
<td>Godaddy.com</td>
<td>$4.00</td>
</tr>
<tr>
<td>Groupon.com</td>
<td>$4.00</td>
</tr>
<tr>
<td>Fedex.com; United.com; Continental.com</td>
<td>$6.00</td>
</tr>
<tr>
<td>ITunes</td>
<td>$8.00</td>
</tr>
</tbody>
</table>

http://securityaffairs.co/wordpress/
Deep Web Proliferation

Creating your own black market site on the deep web has become easy with services such as Deepify.

At present, a lack of accountability and security measures have prevented this concept from rapidly evolving; however, it is only a matter of time before Deepify is able to incorporate monitoring standards, accountability, and eventually consumer confidence into its business platform.
Cyber Crime and Human Trafficking

• Organized criminal groups use spam, pop-ups and social network sites to recruit their victims.

• The spammer is often paid on commission, he will generally keep 40% of his sales.

• “Craigslist is the single largest source of prostitution in the nation... missing children, runaways, abused women and women trafficked in from foreign countries are routinely forced to have sex with strangers because they are pimped out on Craigslist” - Thomas J. Dart, Sheriff of Cook County, IL.
It’s a business...
Case Study: The World of Botnets - Gameover Zeus

Gameover Zeus Botnet:

- Infecting thousands of computers worldwide.
- Primarily used to distribute ransomware and engage in bank fraud.
- Run by a group of cybercriminals based in Russia and Eastern Ukraine, headed by criminal mastermind Evgeniy Mikhailovich Bogachev.

Have you seen this man?
Case Study: ATM Card Skimming in Europe

Operation Imperium was carried out by Spanish and Bulgarian police, in conjunction with Europol, in October 2014.

- 31 suspects arrested
- 40 homes raided; 8 Criminal laboratories dismantled
- 1000 devices confiscated

The criminal gang is responsible for skimming credentials from ATMs in Spain, Bulgaria, Italy, Turkey, Germany, and France. The stolen data was used to create fake debit cards, and funds were then extracted from the accounts of the unsuspecting victims.

A point of concern for authorities: The gang utilized 3D printing technology to manufacture fake plastic card entrances (bezels) for use on ATMs.
Case Study: The Home Depot Hack

The major North American home improvement chain revealed in September 2014 that it had been the victim of a hacking scandal.

- Data was stolen from 56 million credit and debit cards used at US and Canadian stores.
- An estimate of the amount of fraudulent charges resulting from this hack hovers around US$3 billion.
- Experts believe that organized crime groups based in Eastern Europe carried out the operation.
Conclusions

• Cyber threats, from hacking and data breaches to the use of malware and botnets is on the rise. Recent incidents, such as the hacks of JP Morgan Chase, Home Depot, and Target are just a few examples of how enormous numbers of people can be affected by single cybercrime incidents.

• The profitability and anonymity of cybercrime in the borderless virtual environment of the internet attracts hackers to become cybercriminals.

• The increased involvement of OC groups in cybercrime is a cause for concern, propogating large scale illegal activity and the growth of the underground economy.
QUESTIONS?
Contacts

Francesca Bosco
Project Officer
bosco@unicri.it

UNICRI:
http://unicri.it/special_topics/securing_cyberspace/