PayPal™

COUNTERING ONLINE CRIME

Enabling Internet Safety through regulatory action

Michael Barrett

March 2011

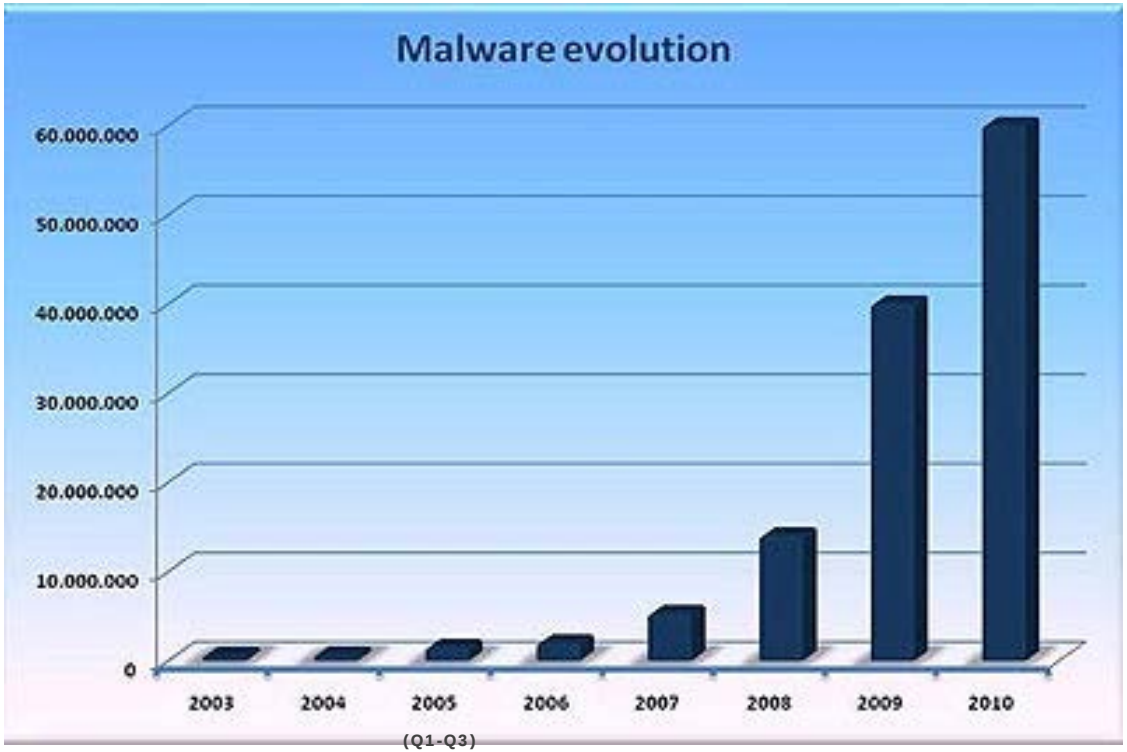
AGENDA

- Cybercrime – the big picture
- Key Challenges in addressing cybercrime
- Policy Responses to Cybercrime
- Summary

CYBERCRIME ENVIRONMENT
NO RULES OF THE ROAD

CYBERCRIME
SCOPE

Growth of Malicious Software



Source: Panda Labs

Since 2003, new malware threats grew by at least 100% every year

CYBERCRIME
CATEGORIES

Fraud

- Theft of funds via unauthorized account access

Money Laundering

- Use of Financial Institution (FI) to “legitimize” stolen funds by sending illegally obtained funds through legitimate financial network
- Use of FI to withdraw funds from stolen financial instrument

Denial of Service

- Aggressive attack at online business presence with goal of serious disruption of access to business by legitimate customers, driven by
  - Political – Organization seen as counter to attacker’s political views
  - Financial gains – Typically associated with a ransom request to stop the attacks

CYBERCRIME
CATEGORIES

Information Theft

- Infiltration of organization's internal infrastructure with goal to obtain or manipulate
  - Financial info
  - Intellectual property
  - Personal information on employees and/or customers
- Personal Identity theft

Corporate Sabotage

- Unauthorized access of internal infrastructure with intent to sabotage within or use confidential info to cause public brand damage

Purchase of Illegal goods / services

- Using common ecommerce infrastructure to purchase illegal goods or services from complicit sellers

CYBERCRIME
PERPETRATORS

Typical Profile - Most sophisticated cybercrime emanates from countries that have:

- Large, well educated technologist population lacking appropriate numbers of well compensated jobs
- Immature cybercrime legal framework
- Inadequate enforcement capacity by government

Geography of Threat Actors

- Cybercrime, like everything else on the Internet, is global
- Unusually higher ratio of online criminal activity is seen from
  - Russia
  - Ukraine
  - China
  - Nigeria (mostly social engineering-based)

Majority of cybercrime committed against PayPal and our customers originates across borders, though much cybercrime enabling infrastructure is located within Western Europe and the US

CYBERCRIME
CRIMINAL TOOLS

Methods

- Malware (Botnets, keyloggers, etc.)
- Social Engineering (fake lottery scams, “emergency funds” for friend, phishing)
- Proxies

Sophistication Increasing

- Exploit packs – Attack software that launches multiple attacks at end-user to perform breach, installation, and full remote control
- Malware management platforms – Infrastructure that manages compromised systems from all over the globe
- “ZeuS” Trojan is an example of most popular current malware tool with widespread use and dozens of “extensions” or “plugins” – the starting turnkey price is $1,000

CYBERCRIME
CRIMINAL TECHNIQUES

Criminal (friendly) Infrastructure - Criminally operated or supportive:

- Web Hosting
- Domain Name Registrars
- False ID Documentation online services
- “Front” legal entities to deter investigation and cooperation with LE as well as protect criminals real identities
- Virtual Private Networks to prevent criminal communication interception by authorities

Follow The Money - Financial gain is at the root of most cybercrime and therefore may be tracked by following the money trail, but challenges include:

- Lack of strong cooperation between private and Law Enforcement (LE) entities
- Lack of operational cooperation between nations on cybercrime investigations (painfully slow between Cybercrime Convention signatories; almost non-existent outside that)

KEY CHALLENGES
MALWARE AND COMPROMISED COMPUTERS

- Botnets and malware infected machines are an ever increasing problem
- More sophisticated malware is becoming increasingly widespread – “Man In The Browser” (MITM) malware is deeply threatening to ecommerce, and is becoming quite commonplace
- There are no requirements on Internet service providers (ISPs) or hosting companies to monitor traffic, or to respond to complaints of abuse in a reasonable timeframe

KEY CHALLENGES
OBSTACLES TO EFFECTIVE LAW ENFORCEMENT

- Insufficient funding for cybercrime law enforcement
- Lack of trained experts in law enforcement on cybercrime
  - Even where laws exist, insufficient training impedes enforcement
- Lack of effective international law enforcement cooperation
  - Mutual Legal Assistance Treaty process is broken and needs a reboot for the 21st century investigation scenario
- Lack of universal legal framework prohibiting some actions
  - Not all countries consider malware creation/distribution a crime
- Statutory minimums in cybercrime laws are a major problem
- Not all parties in the ecosystem are regulated effectively

KEY CHALLENGES
OBSTACLES TO EFFECTIVE LAW ENFORCEMENT

Official Law Enforcement (LE) Cross-Border Process

Mutual Legal Assistance Treaty (MLAT) process was designed for non-digital worlds

- Can take 6 months to complete
- Has taken as much as several years for some to Eastern Europe and Asia
- Creates pervasive dependencies on each step in the process to understand and properly prioritize each request

KEY CHALLENGES
OBSTACLES TO PRIVATE ACTION

- Privacy laws, policies, and brand impact hinder effective cooperation

- Some existing regulations hinder investigations with no corresponding public benefit (e.g. US Electronic Communications Privacy Act (ECPA))
  - Existing regulatory regimes prioritize Privacy over Safety/Security
  - We believe that Privacy can't exist without first ensuring Safety/Security

KEY CHALLENGES
CONSUMER RIGHTS AND OBLIGATIONS

- Consumers have no obligations nor incentives to keep their systems secure
- Consumers are not educated on how to stay safe online
- There is also little curriculum material for school pupils

KEY CHALLENGES
UNRELIABLE DATA ON THE SIZE OF THE PROBLEM

- Roughly, three questions need answering:
  - How much money is being lost?
  - Where is it going?
  - Do those countries appropriately prioritize addressing cybercrime?

- No suitable or universal sources of data collection and reporting on cybercrime
  - Most are survey based and voluntary
  - No equivalent of US FBI “Uniform Crime Reports”

- Countries have different mandatory reporting regimes of varying granularity

- There is no NTSB (National Transportation Safety Board) equivalent in the Online World

POLICY RESPONSES TO CYBERCRIME
RESPONSIBILITIES

- Too many people – many in the infosec industry - assert that Internet safety is a technical problem; this is like asserting that road safety is a technical problem, without any form of standards on safe driving.

- While analogies are always flawed, there are many useful historical examples of appropriate regulatory models in road transportation, aviation, public health and public safety

- An appropriate regulatory framework should tease out the principles that underpin the collective responsibilities of government, private industry and citizens, so that there can be a well-understood answer to the question “Who’s responsible for making the Internet safe?”

POLICY RESPONSES TO CYBERCRIME
PRINCIPLES

- Involve the least regulatory change needed to accomplish appropriate levels of safety.
- Ensure that laws can be interpreted in ways which credibly allow participants to prioritize safety.
- Make changes which reduce negative externalities in the overall ecosystem.
- The Internet is global: change is needed in any given country, and in every country, using compatible conceptual frameworks.
- Avoid attempts to conflate other related issues, such as: intellectual property theft, free speech rights, privacy, etc
- Find solutions which improve security, without compromising privacy.
- Accept that full anonymity on the Internet is infeasible in today's cybercrime environment.
- Treat data usage for anti-fraud/crime purposes distinct from data usage for marketing purposes.

POLICY RESPONSES TO CYBERCRIME

GOALS

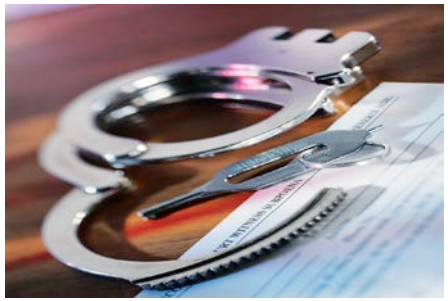
- Faster, more accurate detection and quarantine of cyber threats by Internet Service Providers (ISPs)
- Faster, more effective action by law enforcement agencies when presented with forensic evidence of cyber crime or an ongoing cyber threat
- Better sharing of data useful for anti-fraud and cyber-security purposes
- More comprehensive, effective action against the rewards of cyber crime.
- Consumer safety through safer defaults and education

POLICY RESPONSES TO CYBERCRIME
REGULATE INTERNET SERVICE PROVIDERS

- Require ISPs to monitor their networks for Botnet and Malware Traffic and notify and/or quarantine consumers
- Require rapid response by ISPs and hosting Providers when alerted to malicious content or traffic
- Note: Several programs already active and they are working
  - Australian Internet Security Initiative (AISI)
  - US – Comcast and others

POLICY RESPONSES TO CYBERCRIME
FASTER, MORE EFFECTIVE LAW ENFORCEMENT

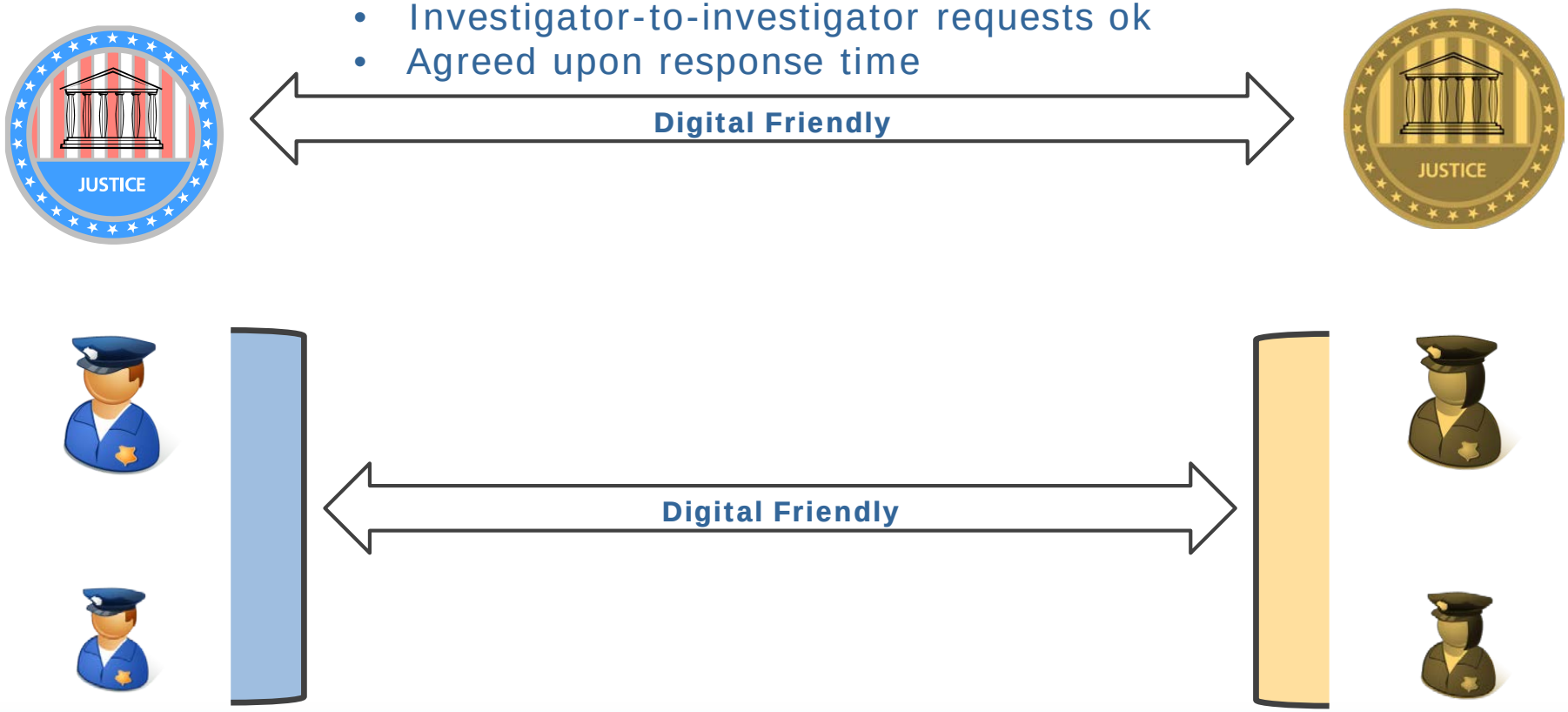
- Modify the Convention on Cybercrime
  - Convention unsatisfactory to some parties because of sovereignty concerns.
  - Concerns by some parties about extradition requirements
- Fix the MLAT process to make it faster, electronic, and suitable for the 21st century
- Governments must spend more on law enforcement resources to investigate & prosecute cybercrime



POLICY RESPONSES TO CYBERCRIME
SIMPLIFY CROSS-BORDER LAW ENFORCEMENT

MLAT process designed for digital world

- Requests made and responded to over digital medium
- Investigator-to-investigator requests ok
- Agreed upon response time



POLICY RESPONSES TO CYBERCRIME
ENABLE BETTER DATA SHARING

- Create “Safe Harbor” Laws to allow and incent companies to share fraud data without concerns of violating Privacy regulations

- Require bilateral sharing of data for anti-fraud and cyber-security purposes between Public and Private sectors

POLICY RESPONSES TO CYBERCRIME
TAKE ACTION AGAINST THE REWARDS OF CYBERCRIME

- Impose broader requirements on banks and money transfer agents to help solve the “Money Mule” Problem
  - Be careful of knock-on effects on legitimate money transfers

- Investigate and prosecute the middle-men in the cybercrime equation
  - Money Mules
  - Money Mule Recruiters

POLICY RESPONSES TO CYBERCRIME
ENABLE CONSUMER SAFETY

- Mandate safer default configurations for computer systems
  - Software should default to “Auto Update” for security patches

- Consumers should be educated about safety basics
  - Mandatory public education campaigns in schools
  - Start at a young age
  - Substantially increase investment in consumer oriented public awareness campaigns (e.g. Get Safe Online)

SUMMARY
THE TIPPING POINT

- Internet usage has reached critical mass in terms of the enablement of widespread online crime
- Without countermeasures being taken in terms of policies and regulations, the growth of cybercrime will continue unabated, likely threatening the continued usage of the Internet itself
- Governments have the opportunity to enable a more effective response to cybercrime activities by proactively addressing fundamental policy needs
- Early adopters of “Internet safety rules” will reap the biggest benefits in terms of being able to shape the direction of standards and to be among the first to reduce the economic impacts while increasing overall confidence in online commerce

SUMMARY
RULES OF THE ROAD ENABLE INTERNET SAFETY