Forum on DNS Abuse

Jeff Moss

Moderator

Session 1- Latest Developments in the Fight Against DNS Abuse

Bill Smith
Paypal

Edmon Chung
APRALO and .ASIA

Kai Koon Ng
SYMANTEC

Session 1- Latest Developments in the Fight Against DNS Abuse

Bill Smith
PayPal

PayPal™

Combating Cybercrime

Principles, Policies, and Programs

Bill Smith

CYBER ISSUES

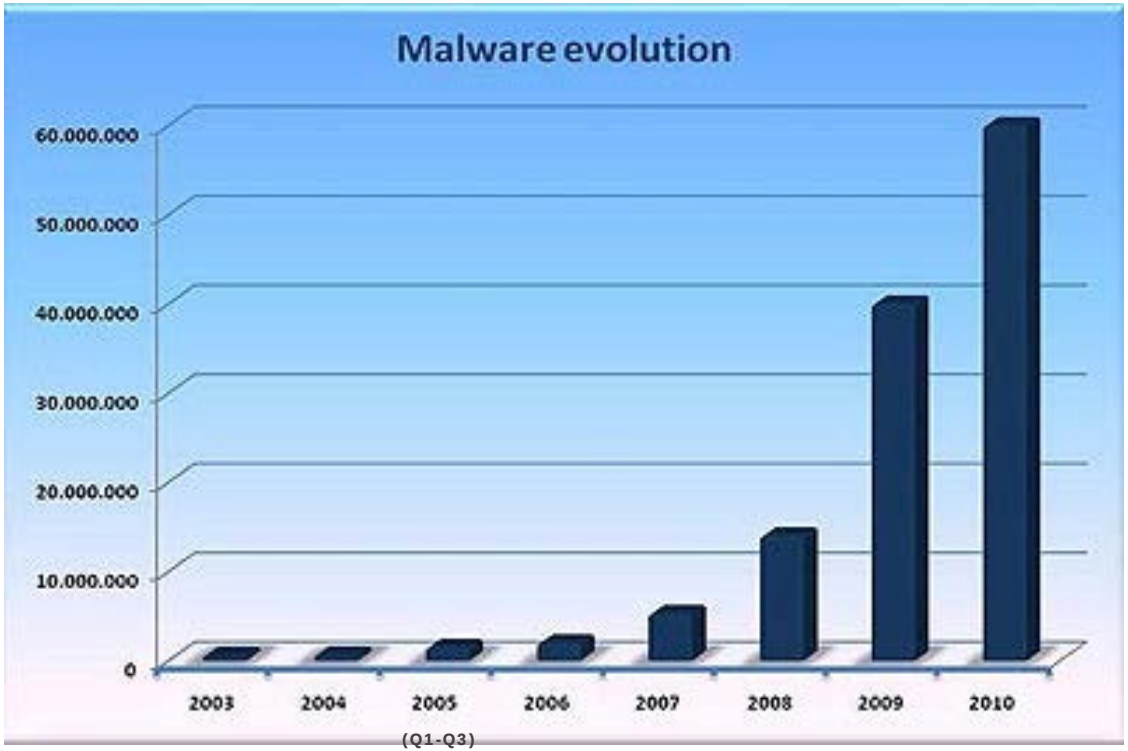
- CyberCrime
- CyberEspionage
  - Individuals or groups
  - State actors
- CyberTerrorism
- CyberWarfare

THE PROBLEM

- Malware and Insecure Computers
- Obstacles to Effective Law Enforcement
- Obstacles to Private and Public/Private Cooperation
- Individual Rights and Obligations
- Unreliable Data on Scope and Scale of the Problem

CYBERCRIME
SCOPE

Growth of Malicious Software



Source: Panda Labs

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

PRINCIPLES

1. Involve the last regulatory change needed to accomplish appropriate levels of safety
2. Ensure that laws can be interpreted in ways which credibly allow participants to prioritize safety
3. Make changes which reduce negative externalities in the overall ecosystem
4. Accept that the Internet is is global – change is needed in every country, using compatible conceptual frameworks
5. Avoid attempts to conflate other related issues, such as: intellectual property theft, free speech rights, privacy, etc.

PRINCIPLES

6. In general, governments should not mandate nor manage technical controls
7. Find solutions which improve security, without compromising privacy
8. Full anonymity on the Internet for e-commerce and financial transactions is often infeasible in today's environment
9. Treat data usage for anti-fraud/crime purposes as distinct from data usage for marketing purposes
10. Organizations that perform Internet Governance are part of the solution, not part of the problem

INITIATIVES

- Build the Internet NTSB
- Substantially increase investment in cybercrime law enforcement
- Incent ISPs to notify customers of malware (AISI model)
- Incent, if not mandate that transit providers screen for criminal traffic such as botnet activity
- Ensure that networks do not allow traffic to exit their networks that perform IP Spoofing

INITIATIVES

- Substantially improve consumer education on CyberSecurity
- Charter an organization to directly attack botnets
- Drag MLATs out of the 19th century into the 21st
- Create an international law enforcement model that allows for prosecution without requiring extradition
- Require that Internet devices “fail safe”
- Force unsupported devices off the Internet

INITIATIVES

- Take enforcement action against “bulletproof hosters”
- Have SLAs for hosting companies to remove phish/malware sites
- Create safe ways for companies to share information about compromised customers, which are exempt from normal rules
- Ensure that ICANN properly enforces ecosystem safety initiatives

CONCLUSION

- CyberCrime is on the rise
- Technical measures, while necessary, are not sufficient
- This is a global, multi-stakeholder issue …
- Requiring local, multi-stakeholder action

Session 1- Latest Developments in the Fight Against DNS Abuse

Edmon Chung
APRALO and .ASIA

Forum on DNS Abuse

2011.06.20

.Asia DNS Abuse Prevention Mechanisms

- Afilias team

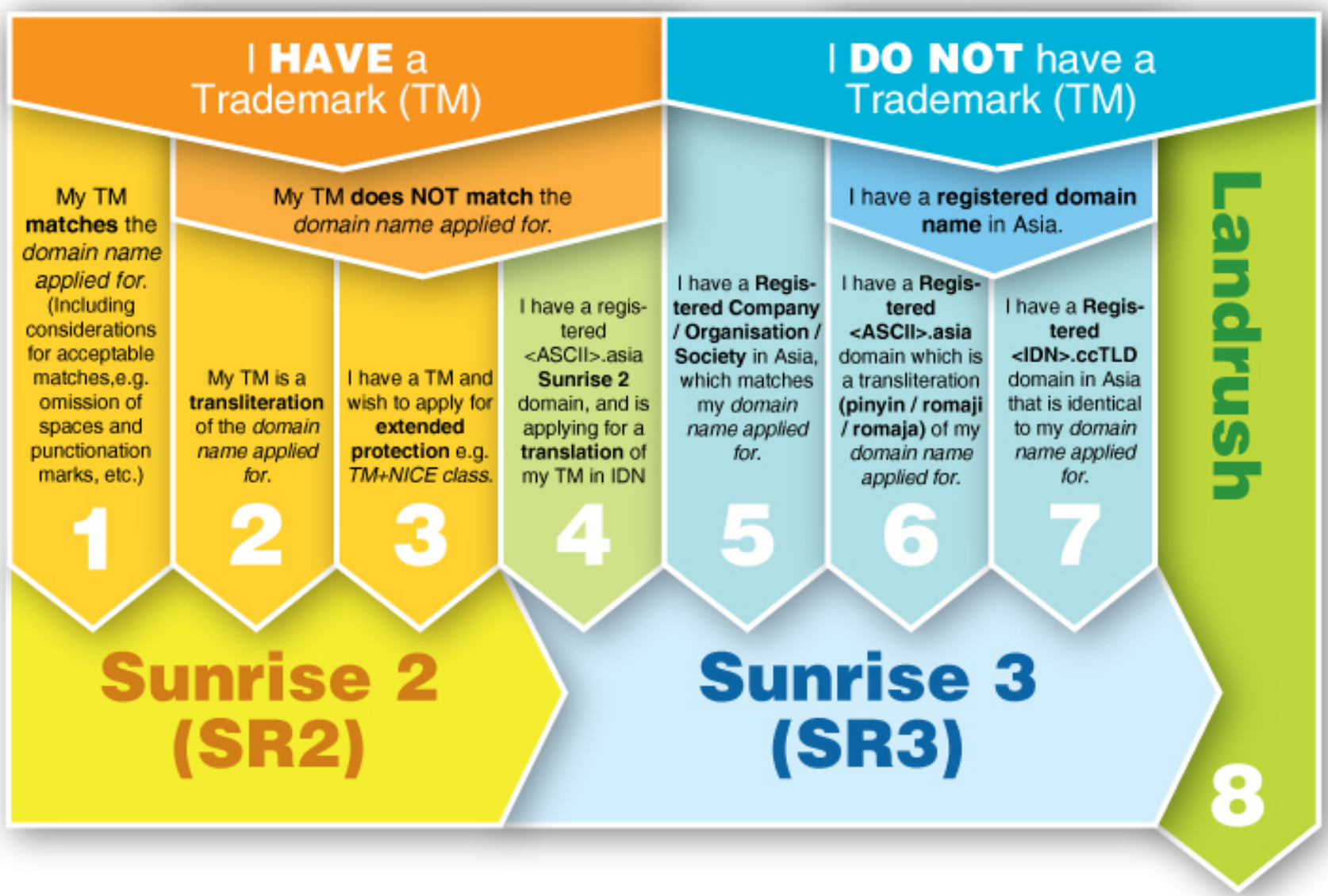
- Abuse Prevention Commitments
- APWG Proposal
- MPAA MoU
- URS

- APCERT & HKCERT Drills
- Sunrise Mechanisms

.Asia IDN Sunrise & Landrush:

- **Sunrise**
  - OPEN: May 11, 2011 (Wed – 12:00UTC)
  - CLOSE: **July 25, 2011** (Wed – 24:00UTC)
  - 70 Days
- **Landrush**
  - OPEN: August 2, 2011 (Tue – 12:00UTC)
  - CLOSE: **October 11, 2011** (Tue – 24:00UTC)
  - 70 Days
- **Pioneer Domains Program**
  - May 11 – **July 20, 2011**
  - Community Pioneers
  - Celebrity Pioneers
  - Social Pioneers
  - Global Brand Pioneers
  - Partner Pioneers

Summary of IDN Sunrise Eligibility



Sunrise Eligibility Highlights

- .ASIA **ASCII SR2 registrants** invited to apply for translation of their name in IDN Sunrise:
  - hyatt.asia → **凱悅**.asia | **ハイアット**.asia
  - mcdonalds.asia → **麦当劳**.asia | **맥도날드**.asia
- Existing **Romanized ASCII .Asia domain** holders:
  - pinyin.asia → **拼音**.asia
  - romaji.asia → **ローマ字**.asia
  - romaja.asia → **로마자**.asia
- **IDN.ccTLD domain** holders in Asia:
  - 中文域名.cn → **中文域名**.asia
  - 日本語ドメイン名.jp → **日本語ドメイン名**.asia
  - 한글도메인.kr → **한글도메인**.asia

.Asia IDN TLD Commitment

- Commitment to offer domain automatically to same registrant
  - Actual process dependant on ICANN policies

- Grandfathering NOT for translation:
  - chinese.asia ≠ 中文.亞洲
  - japanese.asia ≠日本語. アジア
  - korean.asia ≠ 한국어. 아시아

.Asia IDN Variant Policies

- Simplified and Traditional Chinese
  - CDNC Table (incorporating both CNNIC and TWNIC provisions)
  - Hong Kong (Cantonese) Supplementary Characters

- Consideration for Japanese Kanji in the Context of a gTLD
  - 日本語.jp | 漢語.jp → Japanese
  - 漢語.cn | 日本語.cn → Chinese
  - 漢語.asia | 日本語.asia ?

Work with CHIP

- CHIP: ClearingHouse for Intellectual Property
- Sunrise Verification & Pre-Verification
- CHIP Trademarks Claims Service


www.大兵小將.asia
聯合出品 成龍影業有限公司 北京龍苑堂文化藝
特別推薦 林鵬 主演 劉承俊 王寶強 于榮光 杜玉明 徐冬
總製片人 成龍 製片人 蘇志鴻 張哲 監製 袁農 蘇志鴻 仁
©2010 成龍影業有限公司 保留所有版權
大兵小將
LITTLE BIG SOLDIER
成龍
導演
動作導
www.大兵小將.asia
聯合出品 成龍影業有限公司 北京龍苑堂文化藝術有限公司 北京乾坤星
特別推薦 林鵬 主演 劉承俊 王寶強 于榮光 杜玉明 徐冬梅 盧惠光 吳樾 牛犇 冀
總製片人 成龍 製片人 蘇志鴻 張哲 監製 袁農 蘇志鴻 仁衣萬 張行 策劃 劉芳 黃昭敏
©2010 成龍影業有限公司 保留所有版權
2月25日浩瀚出征
大兵小將
LITTLE BIG SOLDIER
英皇電影
EMPEROR MOTION PICTURES
新巴
FIRST BUS


我們
憑相同信念，於各地匯聚知音
星展銀行 — 亞洲最安全，新加坡最佳
www.dbs.asia
星展集團獲《全球金融》評選為2009、2010年"亞洲最安全銀行"，
《歐萬利》、《亞洲金融》及《全球金融》評選為2010年"新加坡最佳

.mo

Every .Asia Domain Contributes to Internet Development in Asia

ISOC HK Work

- Working Group on Security and Privacy
  - Jun 2009: Dissection of Green Dam with Regards to Internet Security
  - Feb 2010: Security Issues arising from IPv6 Deployment
  - May 2010: Armament Race in Internet Content Filtering
  - Jun 2010: APrIGF session on security
  - Dec 2010 (and Nov 2009): Response to and Forum on the Result of the HK Government's Review of the Personal Data (Privacy) Ordinance

Internet Society
Hong Kong 香港互聯網協會

Developments in Asia

- DotAsia .Asia – APCERT
- CNNIC .CN
- HKIRC .HK – HKCERT
- JPRS .JP – JPCERT/CC
- SGNIC .SG – SGCERT
- APAPA: Asia Pacific Anti-Phishing Alliance
  - APRICOT Meetings 2011 (in Hong Kong) Feb 19, 2011
  - CNNIC / DotAsia / TWNIC / JPRS / KISA / HKIRC / SGNIC

Internet Society Hong Kong 香港互聯網協會

User Perspectives

- Security &/vs. Privacy
- WHOIS
- Phishing
- Spam

Internet Society
Hong Kong 香港互聯網協會

Thank You

- Edmon Chung
- edmon@isoc.hk

Internet Society Hong Kong 香港互聯網協會

Session 1- Latest Developments in the Fight Against DNS Abuse

Kai Koon Ng
SYMANTEC

The Evolving Cyberspace Threat Landscape

Kai Koon Ng

Senior Manager, Legal and Public Affairs

Global Intelligence Network

Identifies more threats, takes action faster & prevents impact

Worldwide Coverage | **Global Scope and Scale** | *24x7 Event Logging*

Rapid Detection

Attack Activity	Malware Intelligence	Vulnerabilities	Spam/Phishing
• 240,000 sensors • 200+ countries	• 133M client, server, gateways monitored • Global coverage	• 40,000+ vulnerabilities • 14,000 vendors • 105,000 technologies	• 5M decoy accounts • 8B+ email messages/day • 1B+ web requests/day

Preemptive Security Alerts | **Information Protection** | *Threat Triggered Actions*

Threat Landscape

Who are the players?

Hackers

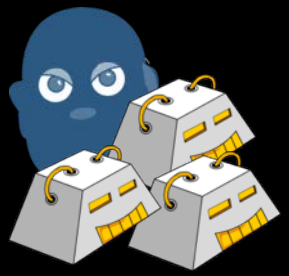
Cyber Criminals

Cyber Spies

Hactivists

What are they doing?

Steal Resources



- Send spam
- Part of a DDOS attack

Steal Information

- Steal sensitive info e.g. banking credentials

Extortion Money

- Old fashion 'con'
- Sit back and wait for the $s to roll in

Destroy

- Hacktivism
- Cyber-Sabotage

Rustock	Zeus	Rogue AV	Stuxnet

How are they doing it?

- Dumpster Diving has given way to the riches of Social Networking sites
  - Few realise the dangers of posting Personably Identifiable Information (PII) Online
  - Even knowing who your 'friends' or who are 'linked' to is significant!

- Search Engine Optimisation (SEO) Poisoning
  - Any significant regional or global event now routinely triggers large numbers of fake and malicious sites all optimised for 'search'

Who is being attacked?

Enterprises

- Targeted Attacks
- Data Breaches
- End-user disruption
- DDOS attacks

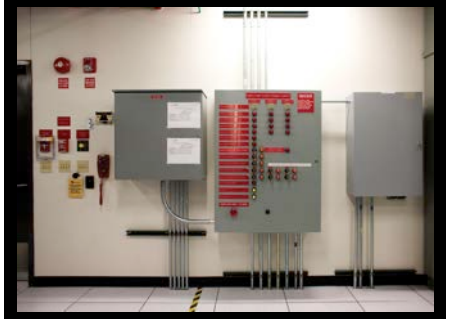
Small Businesses

- Bank accounts
- Business disruption

End-Users

- ID Theft
- Scammed for dollars
- Removal costs

Governments



- Cyber Sabotage
- Cyber Espionage
- Hactivism

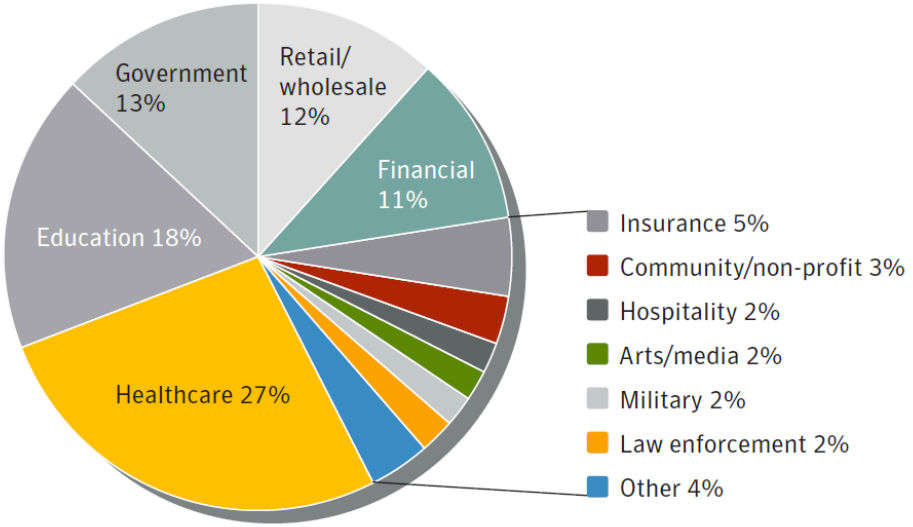
Targeted Attacks

What are Targeted Attacks?

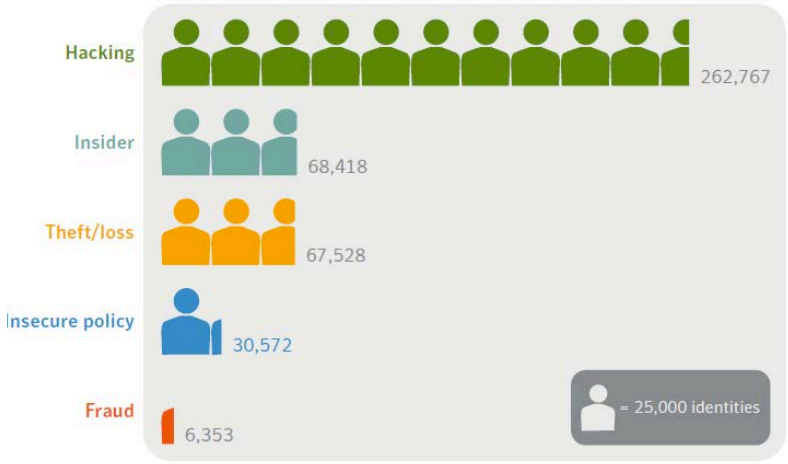
- Cyber attacks that target individuals or organisations
- Use information that are specific to target of attack
  - IP Address in the case of Denial of Service attack
- Frequently use social engineering techniques or exploit vulnerabilities to gain access
- Hidden in plain sight
  - Stay hidden as long as possible to extract as much information or do as much damage as possible
- Two High profile cases in 2010
  - Hydraq
  - Stuxnet

So, what has Stuxnet taught us?

- Level of targeting would not be possible without specific information about the target
- Stuxnet provided a means where information could be stolen
- Increasingly, targeted attacks are used to steal information



Volume of Data Breaches by Sector

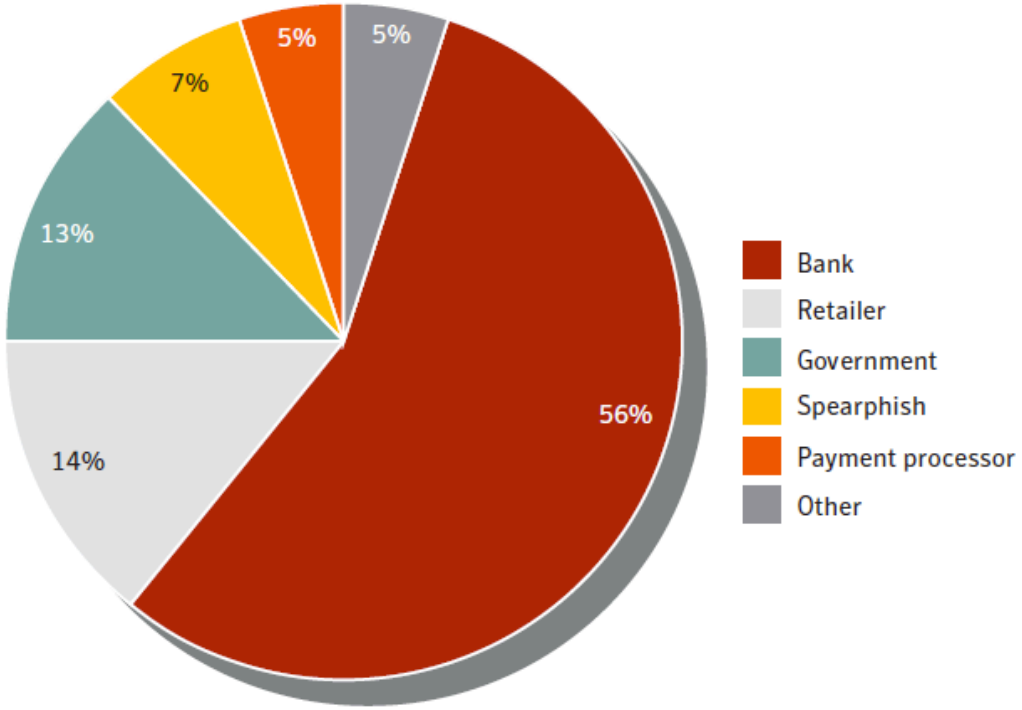


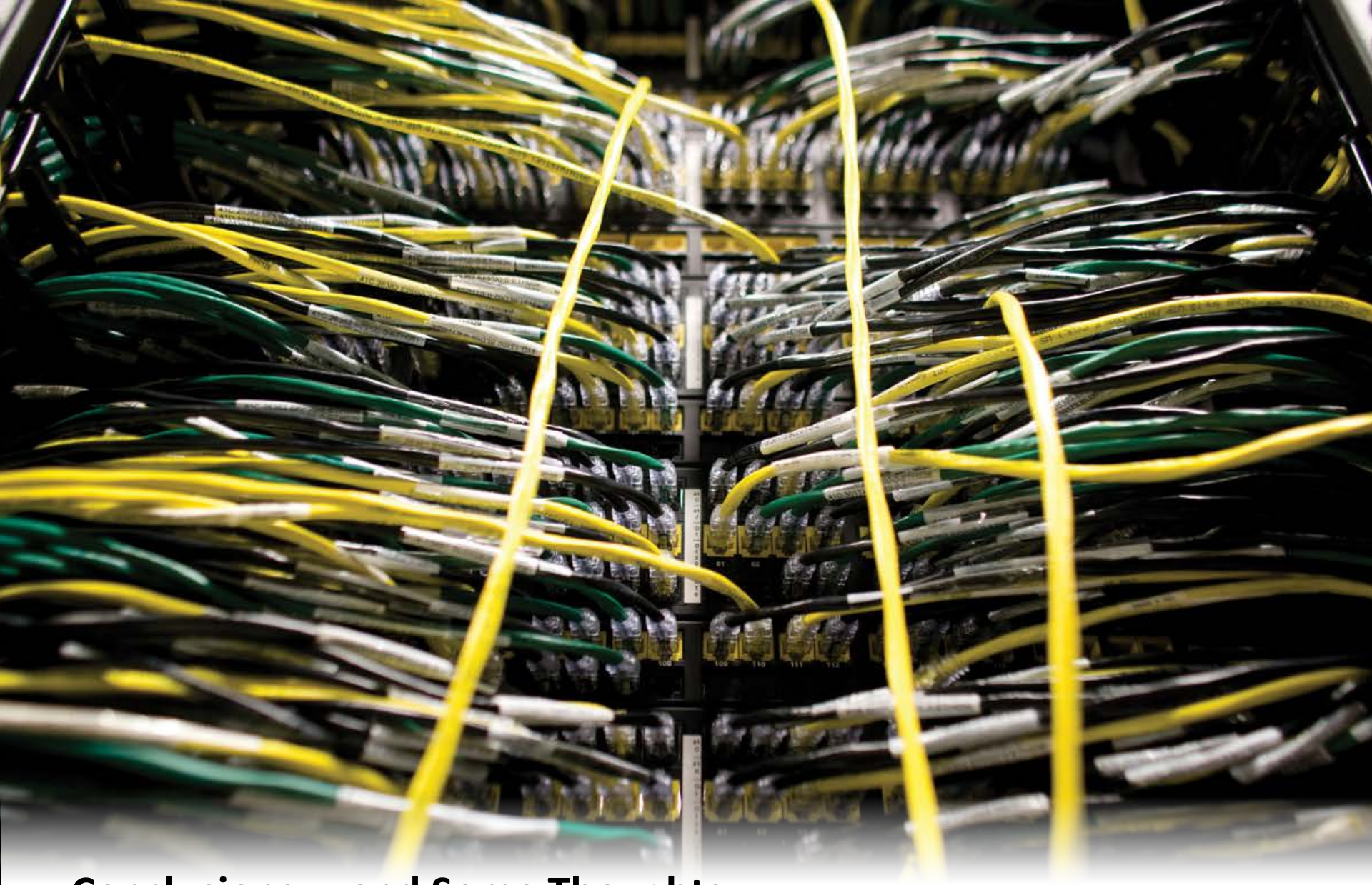
Average Number of Identities Exposed per Data Breach by Cause

Phishing categories

Def: "Phishing" is a derivative of "fishing" and alludes to the use of "bait" to "catch" personally identifiable information

- 56% of phishing attacks imitated banks
- Many email-based fraud attempts referred to major sporting, news and pop-culture events in 2010





Conclusions… and Some Thoughts

Challenges are There…

- The Bad Guys are innovating
  - New forms of attacks like Stuxnet
  - Harness and adopt latest technologies
- Malicious activities are no longer just an annoyance
  - Most usually have a specific goal in mind
  - Financial gain or espionage
- Information is the new Gold
  - System-centric to Information-centric defense

Warren Buffett

> “Predicting rain does not count,
> Building Arks does.”

Building ‘Arks’

Collaborating with Governments around the World

- Jointly funded security research
  - Wombat, Lobster, Antiphish, Vampire
- Jointly funded critical infrastructure protection projects
  - European Programme for Critical Infrastructure Protection (EPCIP)
- Joint deployment of security intelligence technologies
  - Attack Quarantine System (AQS), Deepsight Analyser
- Joint cyber-security exercises
  - Coalition Warrior Interoperability Demonstration (CWID), Cyberstorm, Cybershockwave, Cyber-Endeavour
- Participation in expert groups, committees etc
  - ENISA, ITSCC
- Awareness raising
- Philanthropy/CSR activities

Thank you!

Kai Koon Ng
kaikoon_ng@symantec.com
+65 9002 0214

Questions

Session 2- Probing ICANN's Role in Responding to E-Crime

Danny McPherson
Verisign

Eleanor Bradley
Nominet

Mick Moran
INTERPOL

Prof. Ang Peng Hwa
Nanyang Technical University

Marilyn Cade
ICT Strategies

ICANN Singapore 41 19-24 June 2011

nominet

The UK response to DNS abuse

Eleanor Bradley, Director of Operations
Nominet UK

Types of abuse

nominet

- Technical
  - Direct technical attack against the Domain Name System itself
  - Abuse using the DNS, where the criminal needs the DNS to function
- Social
  - Exploiting the people that manage the DNS
  - Exploiting the people that use the DNS

Abuse against the DNS

nominet

- Example
  - DDOS
- Response
  - Working with and developing networks and best practice
  - Well established response and technologies
  - Make use of third parties

Abuse using the DNS

- Example
  - Conficker
  - Sale of counterfeit goods
- Response
  - We work with Law Enforcement
  - Engage broad range of stakeholders to develop policy

Exploiting the people that manage the DNS

nominet

- Example
  - Social engineering
- Response
  - Constantly looking at our own processes and practices
  - Learning from others' mistakes
  - Working collaboratively within the wider registry community
  - Working with specialists to attempt to crack our security and people

Exploiting the people that use the DNS

- Example
  - Phishing
- Response
  - Tools
    - Publish a list of all phishing sites as a clearing house
    - Provide tools for registrars to immediately lock sites out of the DNS
  - Work as part of Anti-Phishing Working Group to identify measures to help prevent
  - Work proactively with registrars to educate

Questions?

Session 2- Probing ICANN's Role in Responding to E-Crime

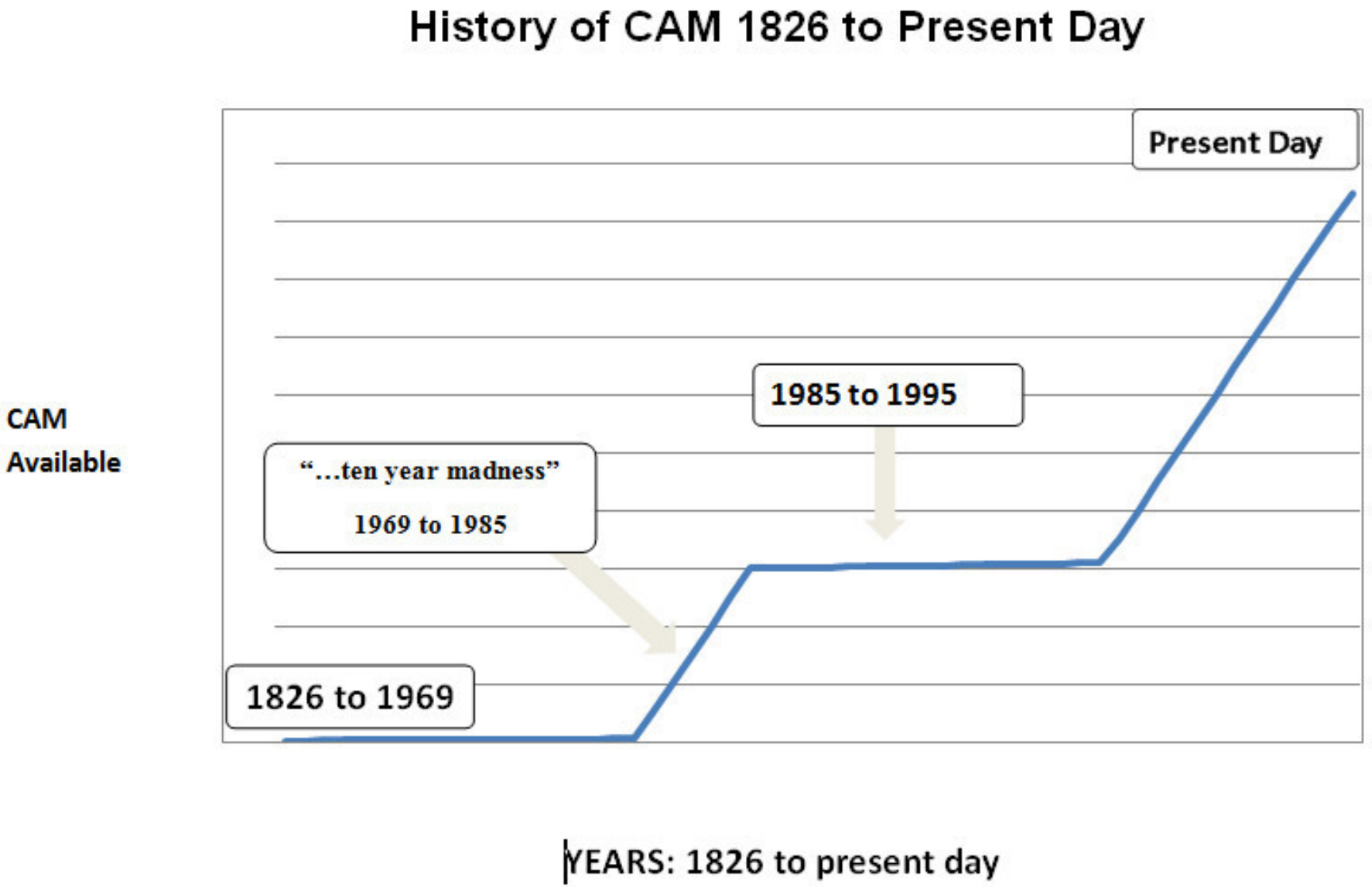
Mick Moran
INTERPOL


OIPC ICPO
INTERPOL


ICANN

1	**Indicative**	Non-erotic and non-sexualised pictures showing children in their underwear, swimming costumes from either commercial sources or family albums. Pictures of children playing in normal settings, in which the context or organisation of pictures by the collector indicates inappropriateness.
2	**Nudist**	Pictures of naked or semi-naked children in appropriate nudist settings, and from legitimate sources.
3	**Erotica**	Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness.
4	**Posing**	Deliberately posed pictures of children fully clothed, partially clothed or naked (where the amount, context and organisation suggests sexual interest).
5	**Erotic Posing**	Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses.
6	**Explicit Erotic Posing**	Pictures emphasising genital areas, where the child is either naked, partially clothed or fully clothed.
7	**Explicit Sexual Activity**	Pictures that depict touching, mutual and self-masturbation, oral sex and intercourse by a child, not involving an adult.
8	**Assault**	Pictures of children being subject to a sexual assault, involving digital touching, involving an adult.
9	**Gross Assault**	Grossly obscene pictures of sexual assault, involving penetrative sex, masturbation or oral sex, involving an adult.
10	**Sadistic/Beastiality**	a. Pictures showing a child being tied, bound, beaten, whipped or otherwise subject to something that implies pain. b. Pictures where an animal is involved in some form of sexual behaviour with a child.

History of CAM

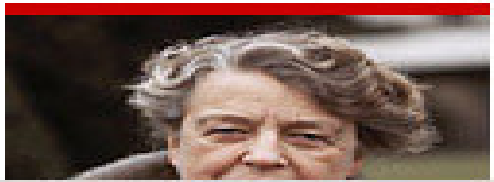


Click to edit Master text styles
Second level
- Third level
- Fourth level
- Fifth level

The Sexes: Child's Garden of Perversity

Monday, Apr. 04, 1977

More on TIME.com



Lollitots magazine is one of the milder examples. It features preteen girls showing off their genitals in the gynecological style popularized by Penthouse and Playboy. Other periodicals, with names such as Naughty Horny Imps, Children-Love and Child Discipline, portray moppets in sex acts with adults or other kids. The films are even raunchier. An 8-mm. movie shows a ten-year-old girl and her eight-year-old brother in fellatio and intercourse. In another film, members of a bike gang break into a church during a First Communion service and rape six little girls.

ICANN

- Less Carrott Please

INTERPOL

Michael Moran

Coordinator

Crimes against Children

NANYANG TECHNOLOGICAL UNIVERSITY

Can DNS Offences Be Self-Regulated?

Peng Hwa Ang
Director, Singapore Internet Research Centre,
Wee Kim Wee School of Communication and Information

Presentation at
DNS Abuse Forum
ICANN 2011 Singapore

But First:
What is Self-Regulation?

Self-Regulation:

- Strictly speaking, it is industry regulating industry
- Here, ICANN and the Internet community regulating the Internet community

And you there
the always-law-abiding Singaporean,
what's so bad about
NOT regulating?
Response: George Akerlof

NANYANG TECHNOLOGICAL UNIVERSITY

George Akerlof

From Wikipedia, the free encyclopedia

George Arthur Akerlof (born June 17, 1940) is an American economist and Koshland Professor of Economics at the University of California, Berkeley. He won the 2001 Nobel Prize in Economics (shared with Michael Spence and Joseph E. Stiglitz). His father was Swedish and his mother a Jewish/German-American.[1] Akerlof graduated from the Lawrenceville School and received his B.A. degree from Yale University in 1962, and his Ph.D. degree from MIT in 1966, and has taught at the London School of Economics. His maternal great-grandfather was born in Oakland, California and was an alumnus of UC Berkeley (class of 1873). His maternal grandfather was also a Berkeley alumnus. His wife Janet Yellen is president of the Federal Reserve Bank of San Francisco and a professor of economics at UC Berkeley and served on President Bill Clinton's Council of Economic Advisors.[2][3] Akerlof is perhaps best known for his article, "The Market for Lemons: Quality Uncertainty and the Market Mechanism", published in *Quarterly Journal of Economics* in 1970, in which he identified certain severe problems that afflict markets characterized by asymmetrical information.

Contents [hide]

Berkeley and trip to India [edit]

After Akerlof graduated from MIT in 1966 he obtained an assistant professorship at Berkeley. He wrote the original draft of "The Market for Lemons" in his first year at Berkeley. In 1967-68 he took leave from Berkeley to spend a year at the Indian Statistical Institute in New Delhi, where Steve Marglin headed a group that was seeking to develop a program to allocate the waters of the Bhakra-Nangal Dam in northern Punjab. He wanted to produce a timetable for the release of the water so that peasants planting the new varieties of wheat could be assured that they would get the water they needed to make such an investment worthwhile. He was brought into the project as an extra. By joining it, he thought that he would gain a first-hand view why India was so poor. His role in the project very quickly came to an end, when he discovered problems with the basic assumption needed to make the project feasible. Because of unseasonal rain and glacial melt he was unable to predict winter in flow into the reservoir from the rainfall of the previous monsoon. Instead, he wrote a paper on Federal-State fiscal policy in India. Planning had been temporarily suspended in India because of the bad monsoons, and his paper gave principles for planning if it should be revived.

George Akerlof

Keynesian economics

Birth	June 17, 1940 (age 69) New Haven, Connecticut
Nationality	United States
Institution	UC Berkeley
Alma mater	MIT (Ph.D.) Yale University (B.A.)
Influences	Robert Solow
Influenced	Robert Shiller
Contributions	Information asymmetry Efficiency wages
Awards	Nobel Prize in Economics (2001)

Problem of information asymmetry: That if incomplete information is the only means to judge a product/service, then bad information will eventually lead to the downfall of the market

Akerlof's "Market for Lemons"

- Take second hand cars
- Some information is symmetrical, known to both sides
- Some information is asymmetrical, known only to the seller

Akerlof's Market for Lemons

- Assume the "value" of a good second-hand car is $10,000
- Assume the value of a bad second-hand car (a lemon) is $6,000
- Assume half the cars are good and half are lemons
- The market price should be $8,000

NANYANG TECHNOLOGICAL UNIVERSITY

Akerlof's Market for Lemons

- Owners of lemons $6,000 cars) will be eager to sell their cars on the open market
- Owners of good ($10,000) cars will not
- This exerts downwards pressure on price
- Eventually only lemons will be supplied
- Trade in good cars will disappear
- The market is destroyed

NANYANG TECHNOLOGICAL UNIVERSITY

Akerlof's Market for Lemons: Lessons

- Asymmetric (ie unreliable) information can cause markets to fail
- Need for credible information
- Signalling and screening (so that only the good guys are in the market) are ways to demonstrate credibility
- Self-regulatory guidelines

  are a form of signalling

NANYANG TECHNOLOGICAL UNIVERSITY

Ok, so we need to regulate the quality of information. But getting governments to agree is difficult. So how about self-regulation?

Theoretical Underpinnings: Conditions for Successful Self-Regulation

- Motivated Industry
- Maturity in Market
- Small Number of Large Players
- Government Regulatory Backstop

Theoretical Underpinnings: Conditions for Successful Self-Regulation

- Motivated Industry **?**
- Maturity in Market
- Small Number of Large Players
- Government Regulatory Backstop

NANYANG TECHNOLOGICAL UNIVERSITY

Theoretical Underpinnings: Conditions for Successful Self-Regulation

- Motivated Industry **?**
- Maturity in Market **?**
- Small Number of Large Players
- Government Regulatory Backstop

Theoretical Underpinnings: Conditions for Successful Self-Regulation

- Motivated Industry **?**
- Maturity in Market **?**
- Small Number of Large Players ✓
  - How about roping in RIRs?
- Government Regulatory Backstop

Theoretical Underpinnings: Conditions for Successful Self-Regulation

- Motivated Industry **?**
- Maturity in Market **?**
- Small Number of Large Players ✓
  - How about roping in RIRs?
- Government Regulatory Backstop
  - Instead of government regulation, can ICANN be the backstop?

NANYANG TECHNOLOGICAL UNIVERSITY

Even assuming we agree with you the always-law-abiding Singaporean, how do we know it can work? Have you got an example? An illustration? Better yet, a live case. A beta, not an alpha?

Singapore Used Car Dealers

- Motivated Industry ✓
- Maturity in Market ✓
- Small Number of Large Players ✓
- Government Regulatory Backstop ✓

NANYANG TECHNOLOGICAL UNIVERSITY

Complaints Before Self-Regulatory Regime

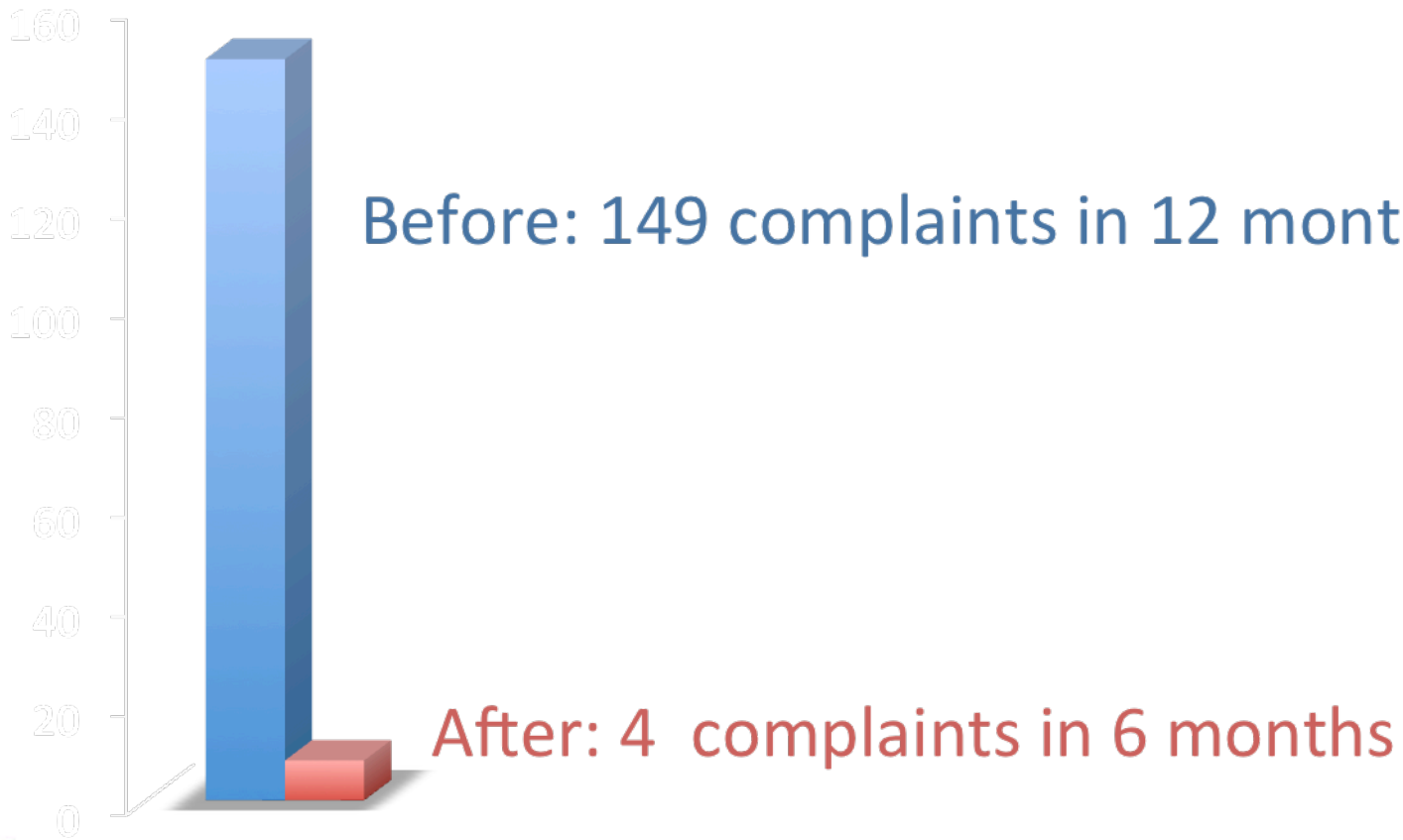
NANYANG TECHNOLOGICAL UNIVERSITY

Complaints After Self-Regulatory Regime

4 in 6 months

NANYANG TECHNOLOGICAL UNIVERSITY

Complaints About Used Car Dealers Before and After Self-Regulation



NANYANG TECHNOLOGICAL UNIVERSITY

So question: who cann be the backstop?

ICANN

Session 2- Probing ICANN's Role in Responding to E-Crime

Marilyn Cade
ICT Strategies

The Debate of Who Should Set the Rules for the Global Internet was just beginning in 1998…

Multi-lateral Entities?

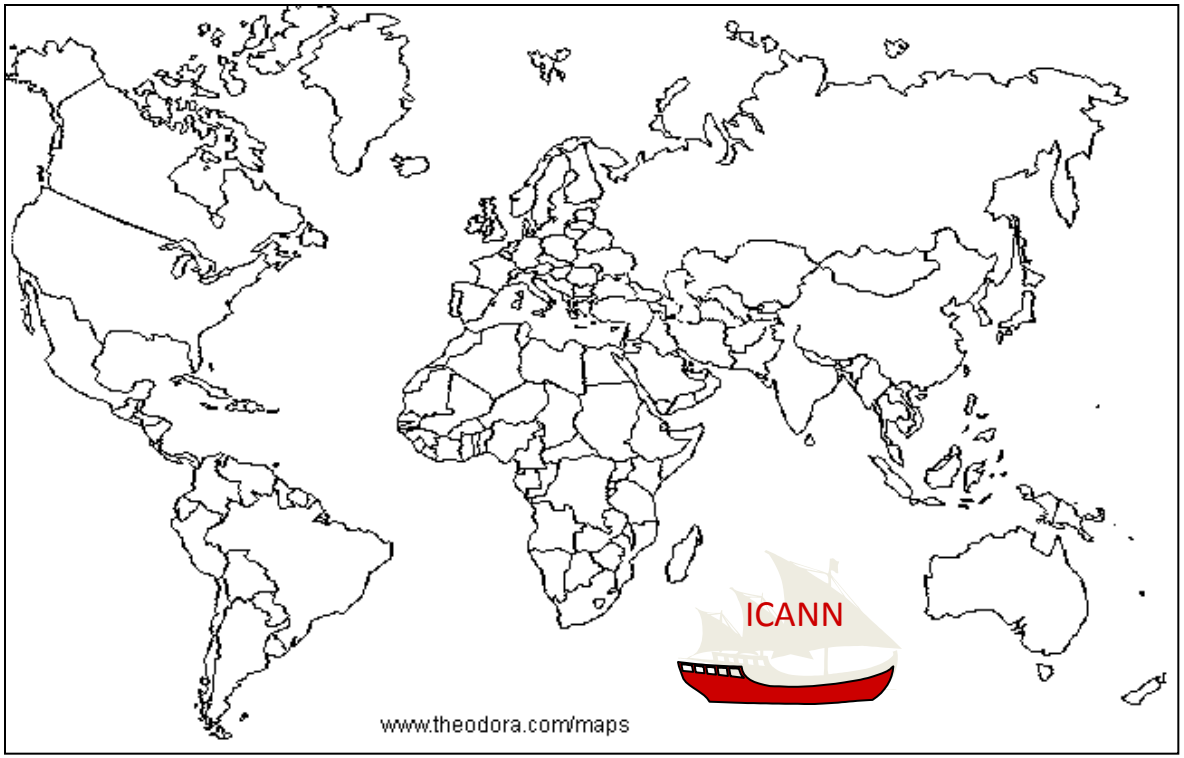
- EC?
- ITU?
- WTO?
- WIPO?

Industry bodies?

- ICANN?
- IETF / IAB?
- Other Standards Bodies?

Governments?

- Parliaments?
- U.S. Congress?
- U.S. Government Agencies?



WHAT WERE WE THINKING ?

OUR JOB AT ICANN IS STILL… TO AVOID COLLISIONS

Session 2- Probing ICANN's Role in Responding to E-Crime

Danny McPherson
Verisign

Eleanor Bradley
Nominet

Mick Moran
INTERPOL

Prof. Ang Peng Hwa
Nanyang Technical University

Marilyn Cade
ICT Strategies

ICANN Singapore 41 19-24 June 2011

One World

One Internet

Questions

ICANN Singapore 41 19-24 June 2011

Thank You