



Cyber Security Trends in 2017 & Beyond

The Mobility of Cyber Threats in a Hyper-Connected World



Trevor Forrest

Senior Advisor, Ministry of Science, Energy & Technology

Glossary of Terms

- **DDoS** – Distributed Denial of Service
- **DDoSaaS** – Distributed Denial of Service as a Service
- **BotNet** – Network of Malware infected computers controlled by hackers
 - Bot - type of malware that allows an attacker to take control over an affected computer
 - Net – Network of Computers/Devices
- **RAT** – Remote Access Trojan
- **C&C** – Command and Control
- **Ransomware** – Holds data/services hostage until ransom is paid
- **IoT** – Internet of Things (Insecurity of Things)

Cost of Cybercrimes

\$USD 2 trillion

The global cost of
cybercrime by 2019

\$USD 445-500 million



The global cost of
cybercrime in 2015



Spend/Cost of Cybercrime and Breaches

\$USD 80 Billion

The global spend to combat cybercrime in 2016

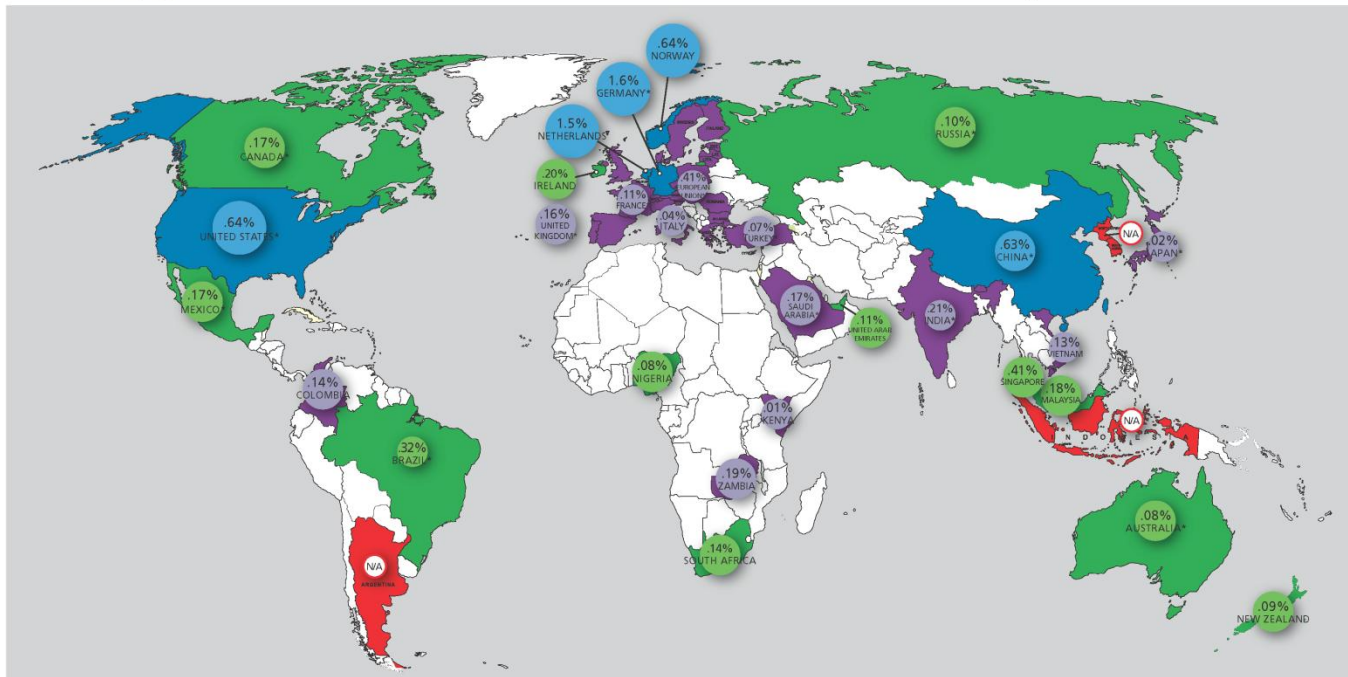
\$USD 4 Million

Average Cost of a Data Breach

Cybercrime Loss as a % of GDP



CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



USA - 0.64%
Mexico - 0.17%
Germany - 1.6%
China - 0.63%
India - 0.21%

Confidence Ranking: Countries Current Tracking of Cybercrime within Their Borders.

- High Confidence Level
- Medium Confidence Level
- Low Confidence Level
- N/A - Countries currently not measuring cybercrime loss
- ✳ G-20 Countries

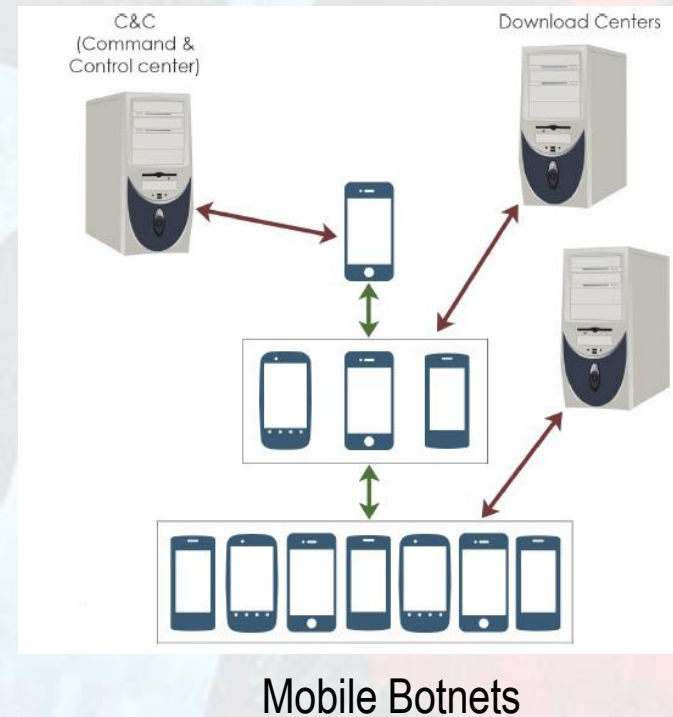
\$445 BILLION
 The annual estimated cost to the global economy from cyber crime



200,000+ Jobs lost in the U.S
150,000+ Estimated in Europe



A New Threat Vector and Delivery Medium



How many mobile phones are out there ?



2 Billion +

The number of
smart phones
globally today



5 Billion +

The number of
smart phones
globally by 2020



How many IoT devices are out there ?



10-15 Billion +

The Number of IoT devices in operation today



30-50 Billion +

The Number of IoT devices in operation by 2020



A New Threat Vector & Delivery Medium







Mobile Devices, Apps and IoT devices will increasingly become the tools used for cyber attacks

Mobile/Wireless broadband networks will become the delivery highway for cyber attacks

Weapons of Mass Destruction

Largest Traditional Botnets

1. **BREDOLAB** -  **30 million computers**
2. **MARIPOSA** -  **12 million computers**
3. **CONFICKER** -  **10.5 million computers**
4. **MARINA** -  **6 million computers**

Notable DDoS Attacks

Dyn – Mirai malware powered, IoT enabled DDoS Attack

100,000+ IoT Devices including DVR's, routers, baby monitors, web cameras

twitter



airbnb



amazon

NETFLIX



BBC



overstock.com[®]

Notable DDoS Attacks (911 Systems)



- Maricopa County attacks (Arizona) via javascript link
- Alabama, Colorado, Florida, Indiana, Oregon, Tennessee and Texas attacks in March via twitter link

Note - iOS fix has since been released



The Effect of this threat

- Increase in unknown/questionable data usage and activity on subscriber devices associated with threat execution
- Increase Data Privacy and Fraud related issues associated with mobile devices
- Mobile devices used as botnet participants
- More combined computing power for attacks
- Attacks will be massively distributed based on wireless networks
- Essential/Emergency service disruption emanating from mobile devices and networks (e.g. 911 or Utilities)
- Rise in activism, criminal & terror related cyber activities because tools are literally in the palm of your hand
- Greater use of IoT devices in DDoS and other attacks
- Security Privacy issues associated with interface-less IoT devices

What are the actions to be taken?

- Increase cyber security awareness through programmes and workshops
- Deploy security controls on BYOD devices connected to corporate networks
- Provide employees/subscribers with a mobile security solution to protect from infections
- Intercept any malicious outbound activity, such as communications with RATs and C&Cs generating a high rate of HTTP/S requests
- Prevent installation of unauthorized applications if possible

What are the actions to be taken?

- A security solution that can protect infrastructure from multi-vector network and application DDoS attacks
- A hybrid solution that includes on premise detection and **DDoS mitigation** with **cloud-based DDoS protection** for volumetric attacks.
- A cyber-security emergency response plan that includes an emergency response team and process
- Monitor mobile security threats
- Telcos need to adopt anti fraud practices of banks and credit reporting agencies



What are the actions to be taken?

Service Providers must get involved

Regulators must get involved

Governments must get involved

Subscribers & Business must get involved

THANK YOU