



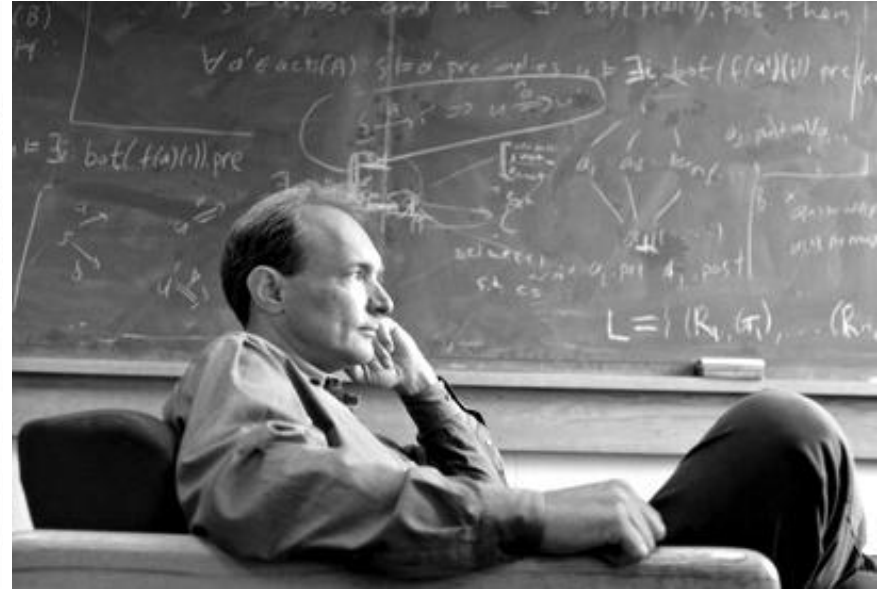
# THE ADVANCING CYBER THREAT

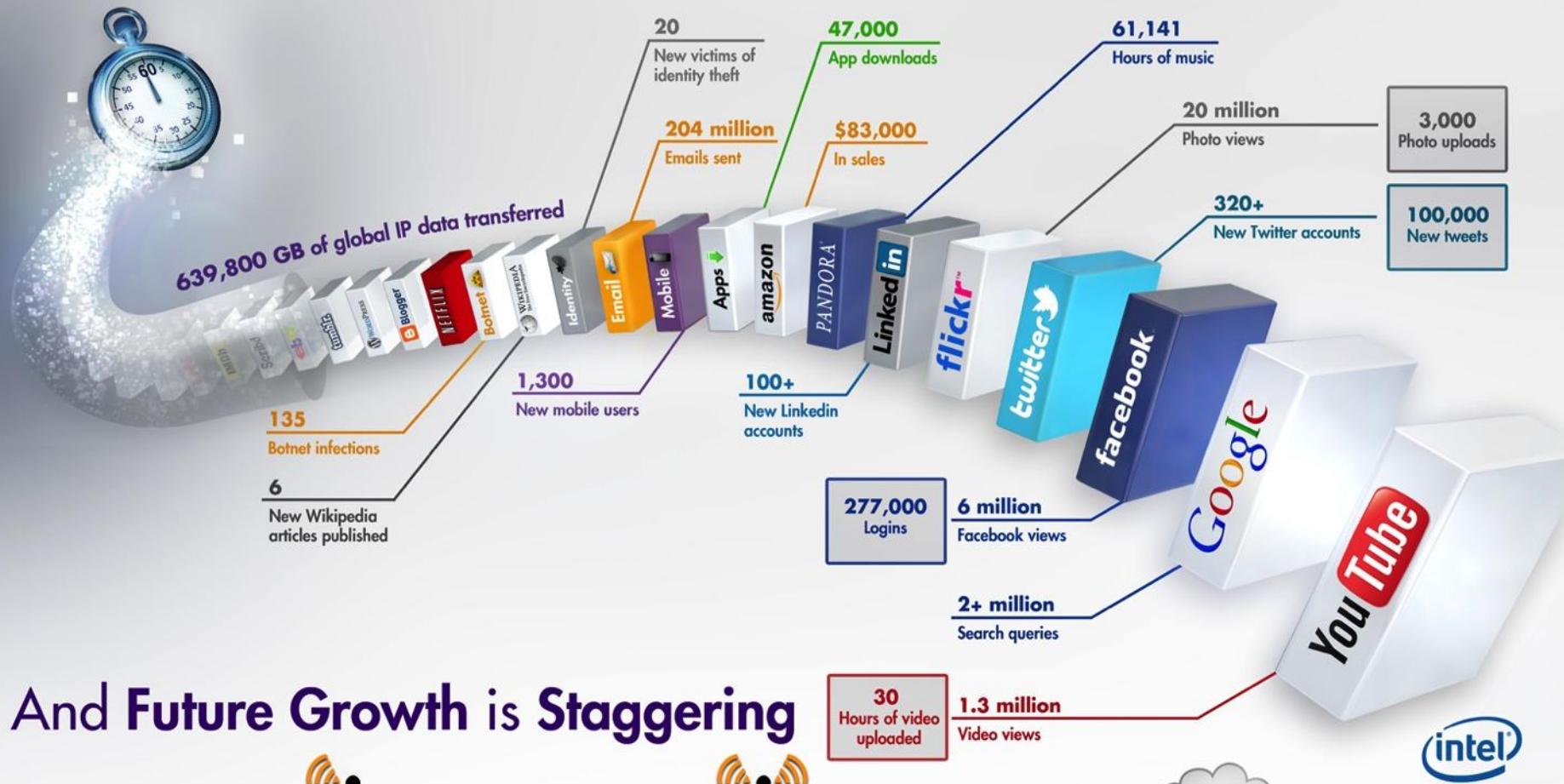
CRAIG RICHARDSON  
CHIEF EXECUTIVE OFFICER  
WYNYARD GROUP

@RICHARDSONCP

# 1989

---





## And Future Growth is Staggering



# THE ISSUES OF OUR TIME



THE CRITICAL BUILDING BLOCKS  
OF THE INTERNET ARE AGEING.

# SKIDDIES (SCRIPT KIDDIES)

## Who are they?

- Individuals or small groups of individuals who experiment with “code”
- Often game players who migrate to WAREZ sites then on to more aggressive action
- Motivated by peer group recognition

## What do they do?

- Web site defacement
- Basic recon of compromised sites
- Post brag notices



# HACKER COLLECTIVES

## Who are they?

- Loosely affiliated, topic motivated groups - ANONYMOUS, LULZSEC
- Spectrum of capabilities – largely based around suites of DDOS “weapons”
- Motivated by topic – privacy, animal welfare, the topic of the day etc.

## What do they do?

- DDOS
- Scareware
- Brag notices




# CRIME SYNDICATES

## Who are they?

- Organised groups driven by financial gain
- PhD qualified, R&D intensity and very professional
- Quasi-autonomous network infrastructures, some can be “rented” (i.e. botnets for hire)
- Cyber crime ecosystem and value chain

## What do they do?

- Zombies
- Botnets
- Social Engineering
- Ransomware
- Credit Card Fraud (large scale)
- Identity theft (and sale)



<b>WALLET</b> \$0.00 add funds	<b>CART</b> 0 view items
BROWSE DUMPS	
<b>WHOLESALE</b>	
ACCOUNT	
CHECKER	
SUPPORT	

\* Dumps from packs are not refundable

<b>1245</b> for \$10,500.00	<b>1110</b> for \$7,500.00
Reseller: <b>McDumpals</b> Base: <b>MA-CT</b> Date pre-sale: <b>2014.03.31</b> Date sale: <b>2014.03.31</b> Age: <b>1 month and 10 days</b> Details: <b>View more</b>	Reseller: <b>McDumpals</b> Base: <b>MA-CT</b> Date pre-sale: <b>2014.03.31</b> Date sale: <b>2014.03.31</b> Age: <b>1 month and 2 days</b> Details: <b>View more</b>
asd <b>Quick buy</b> <b>Add to cart</b>	Buyme! <b>Quick buy</b> <b>Add to cart</b>

## Home Depot confirms security breach following Target data theft

BY NANDITA BOSE

CHICAGO | Tue Sep 9, 2014 12:07pm EDT

1 COMMENTS | Tweet

in Share 139 f Share this Email Print





**Attention!!!**

The privacy of Social activity is protected. According to UK law and Metropolitan Police (Series) and Scotland's Police Inspectorate your computer is locked!

The following website is detected: you IP address "86.1.198.196.87" is located within the Metropolitan Police (Series) and Scotland's Police Inspectorate your computer is locked!

However and e-mail spam was sent to your computer, a code containing harmful materials. This locking serves to stop your illegal activity.

Your details: **IP: 86.1.198.196.87**  
Location: London, United Kingdom, London, UK  
ISP: BT Internet Services Ltd

To release a lock your computer you should pay the fine in amount of £ 1000. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

- 1) Paying through Ukash:  
Use the code received for this purpose, enter it in the space for payment and click OK.  
(If you have more than one code, enter them one after another and then click OK).
- 2) Paying through PayPal:  
Use the code (and a password if needed) received for this purpose, enter it in the space for payment and click OK.  
(If you have more than one code, enter them one after another and then click OK).

To view the details of the website, click on the code in the space for payment and click OK.

**Ukash Where can I buy Ukash?**

You could buy Ukash in many places, for example: shops, stalls, stand alone terminals, on-line or through a retailer (electronic cash), below you could find the list of point of sale Ukash in your country.

**PayPoint** - You could buy Ukash in thousands of supermarkets or Cash Shops which have this sign.

**PayPoint** - Get Ukash whenever you see the PayPoint sign.

**PayPoint** - Ukash available from PayPoint terminals around the UK.

**PayPoint** - You can get a Ukash voucher in values from £10 - £200 and pay using your internet bank.

**paymate** **paymate**

# SYNDICATES FOR HIRE

## Who are they?

- Organised groups often driven by financial gain. PhD qualified, R&D intensity and very professional
- IT professional gangs for hire – often in support of a state or cause
- Quasi-autonomous network infrastructures, some can be “rented” (i.e. botnets for hire)
- Bespoke software written and deployed

## What do they do?

- DDOS
- Web site defacement
- Botnets
- Social Engineering
- Spearphishing
- Remote Access Tool Deployment
- Data Deletion
- Information Theft



# STATE ACTORS

## Who are they?

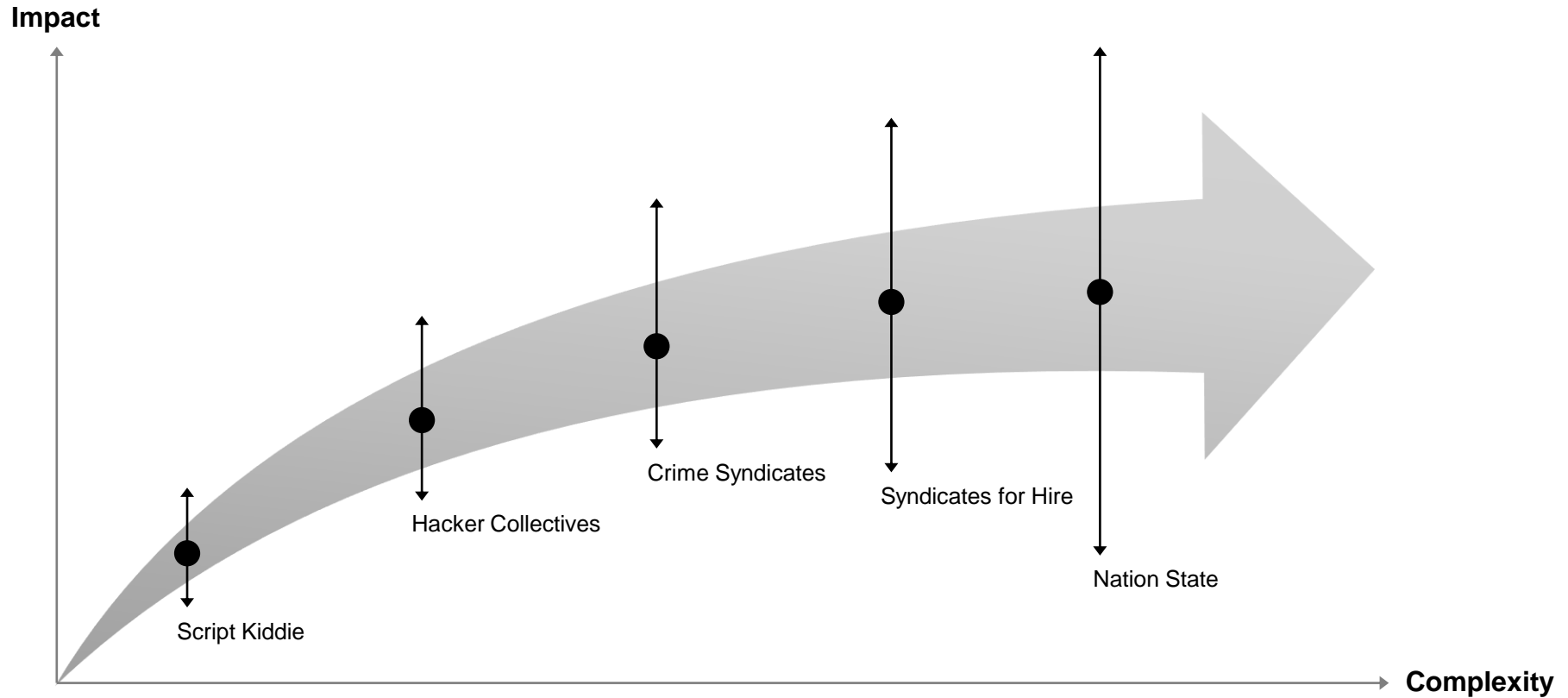
- Government entities – military, intelligence agencies or civilian authorities
- Designers and users of Advanced Persistent Threat (APT) capability

## What do they do?

- Information gathering
- Data manipulation
- Social Engineering
- Spearphishing
- Remote Access Tool
- Large scale information theft
- Offensive actions



# THE CYBER THREAT SPECTRUM



# YOU CAN'T STOP IT. YOU CAN MANAGE IT.



Home > Security > Cybercrime & Hacking

NEWS

## Target CIO resigns following breach

The retailer announces the resignation after data breaches affecting up to 110 million people

Companies & Industries

## As Data Breach Woes Continue, Target's CEO Resigns

By Michael Riley and Dune Lawrence | May 05, 2014



SEND TO [kindle](#)

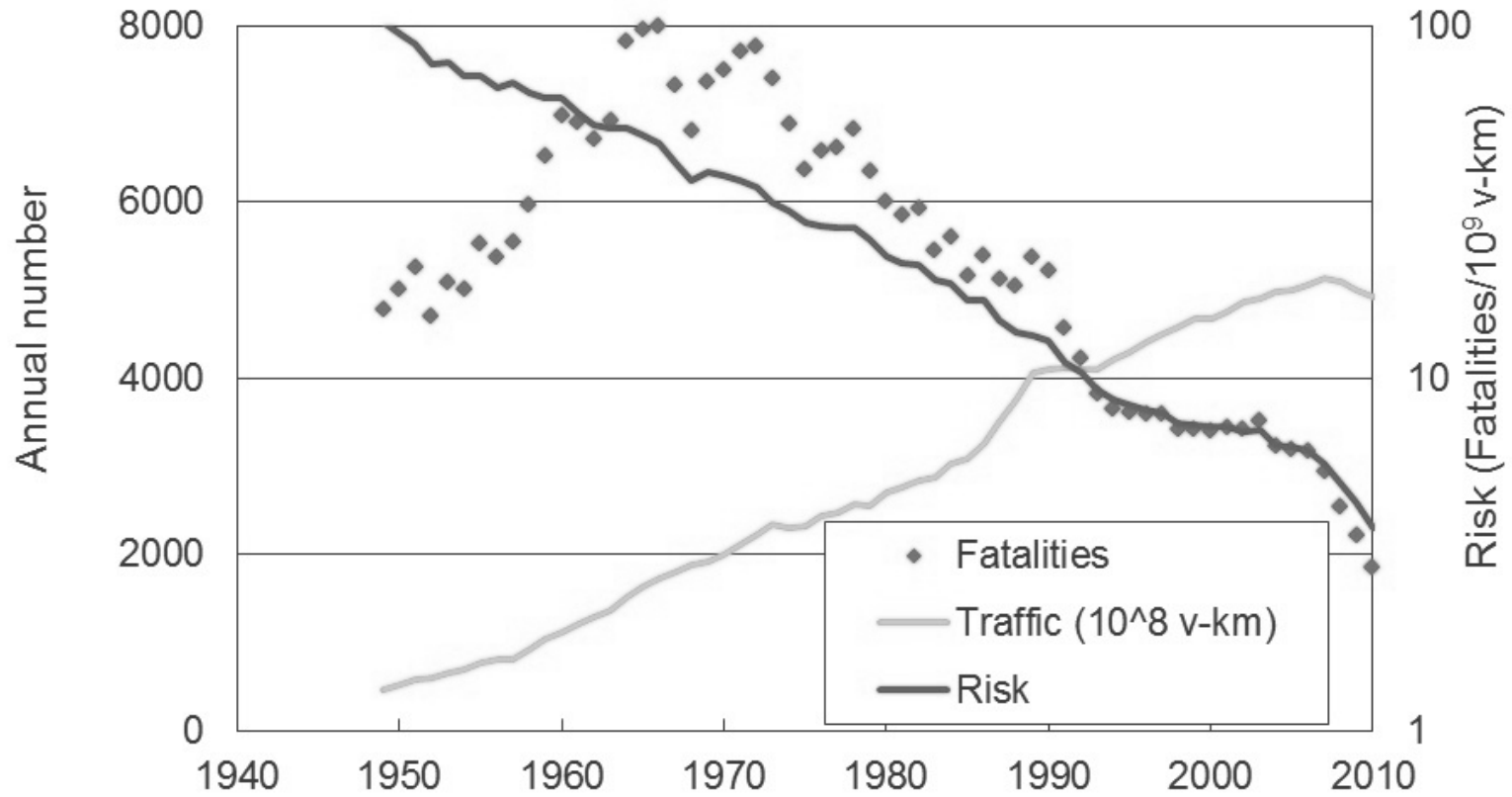


**CYBER THREAT MANAGEMENT IS A  
BUSINESS NOT AN I.T. PROBLEM.**

# LOCOMOTION ACT 1865



# ROAD ACCIDENT FATALITIES - GREAT BRITAIN







WHAT HAPPENS WHEN YOU  
CAN NO LONGER TRUST AN  
ORGANISATIONS DATA?

# REPUTATIONAL, FINANCIAL AND OPERATING IMPACT

	Reputational	Financial	Operational
Normal	1 – Low	1 – Low	1 – Low
	2 – Moderate	2 – Moderate	2 – Moderate
Heightened	3 – Substantial	3 – Substantial	3 – Substantial
	4 – Severe	4 – Severe	4 – Severe
Exceptional	5 – Critical	5 – Critical	5 – Critical

# INFORMATION-DRIVEN SECURITY AND RISK MANAGEMENT WILL BUY YOU TIME TO MAKE SMART BUSINESS DECISIONS



# MANAGING THE ADVANCING CYBER THREAT

---

- This is an unsolvable problem - if you connected to the internet you are a victim waiting to happen
- The critical building blocks of the internet are ageing
- It wasn't designed to carry critical national infrastructure or protect your privacy
- >200,000 vulnerable computers in New Zealand
- Traditional security measures (firewalls, intrusion protection, anti-virus) will not protect you
- You can't protect yourself against "unknown unknown" attacks
- Today's sophisticated threat actors assimilate, integrate and compensate in minutes
- You can't stop it. You can manage it with a dynamic risk management model
  - Risk management
  - Information-driven security
- Cyber threat is a board and executive business risk management issue



**WYNYARD™**

POWERFUL  
SOFTWARE.  
**CONNECTING  
THE DOTS.**

wynyardgroup.com  
@wynyardgroup