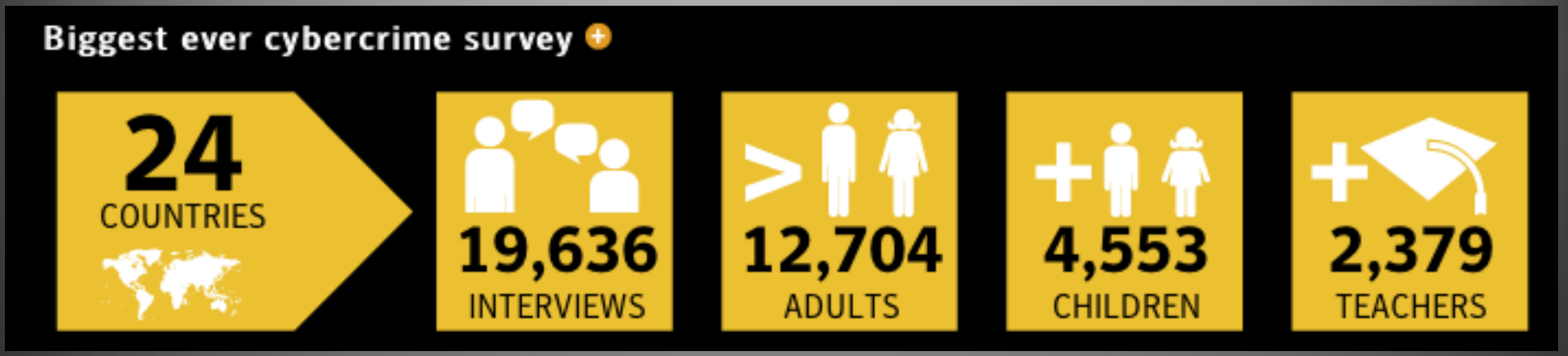
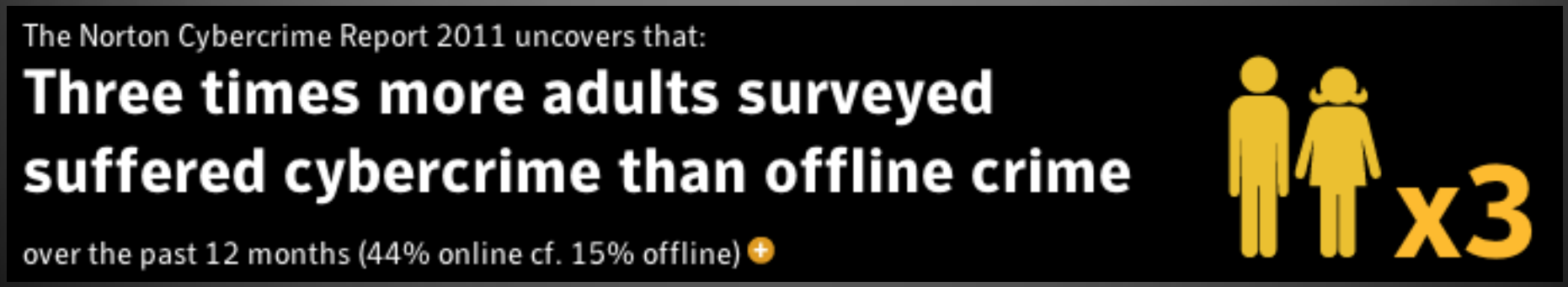
2011 Cyber Threat Landscape

Greg Day
EMEA Security CTO
Director of Security Strategy

Summary of Cybercrime report



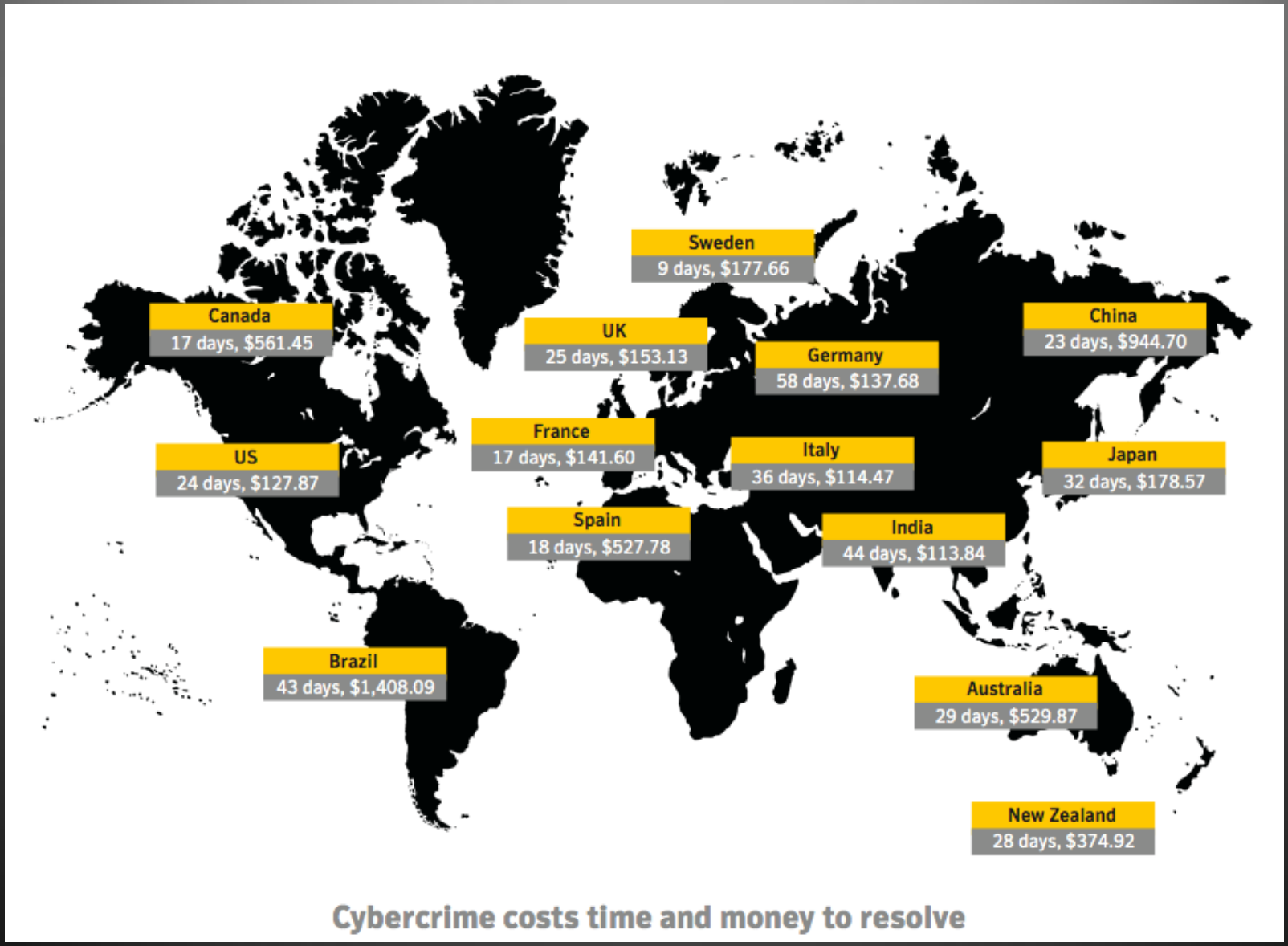


http://www.symantec.com/content/en/uk/home_homeoffice/html/cybercrimereport/

Scale of Cybercrime

Symantec

Time & Money to recovery (from 2010 report)



Where & why?

COMPUTER VIRUSES AND MALWARE ATTACKS

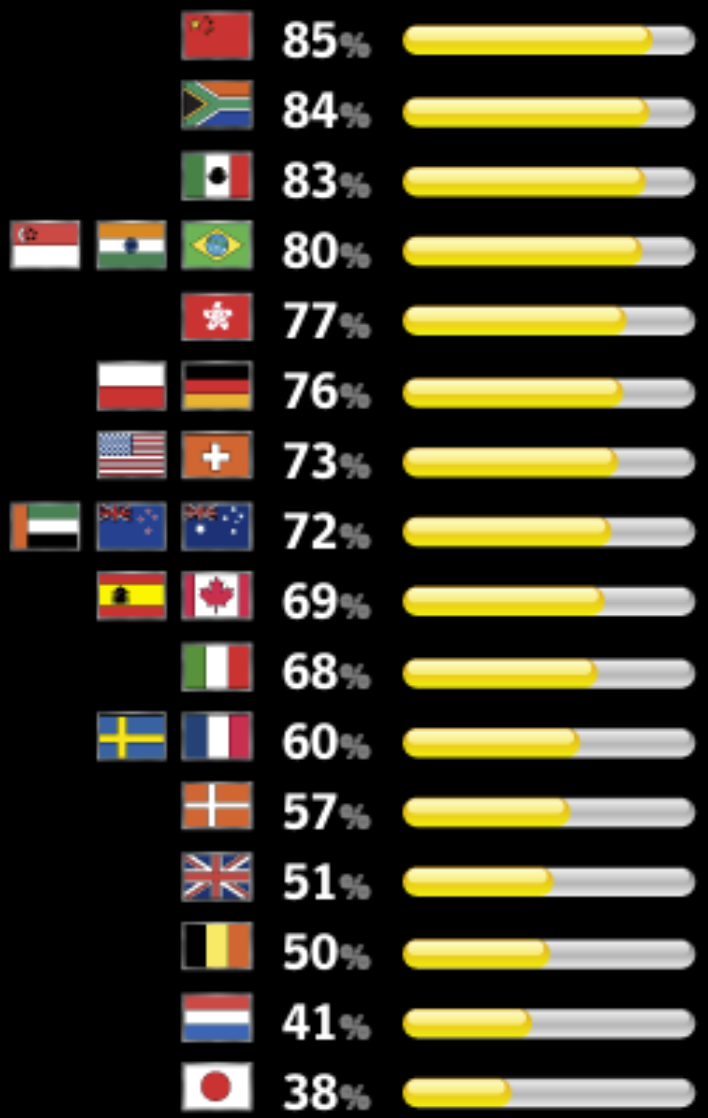
PREVENTABLE YET MORE PREVALENT

41% 4 in 10 adults surveyed do not have an up-to-date security software suite to protect their personal information online

54% 54% of online adults have experienced viruses or malware on their computers

CYBERCRIME HOTSPOTS

Adults(%) who have been a victim of cybercrime

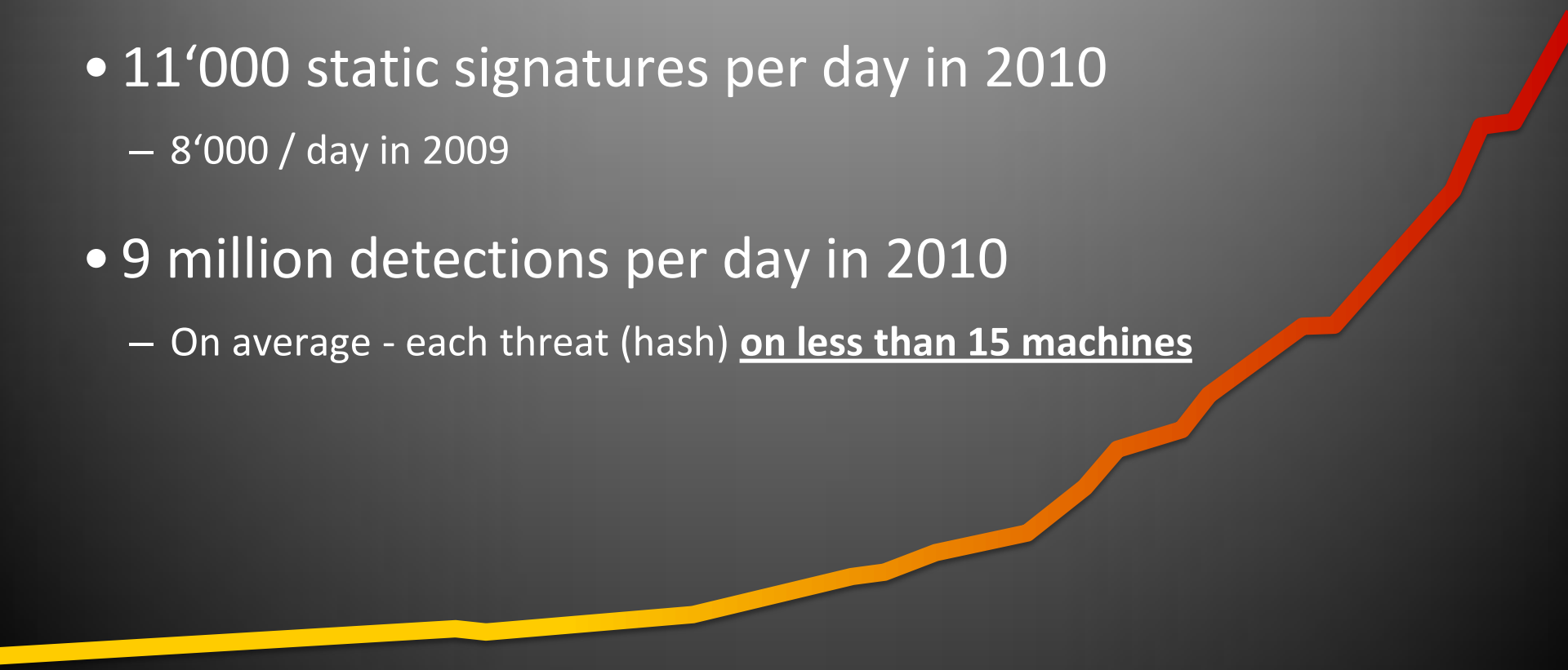


Who and what?

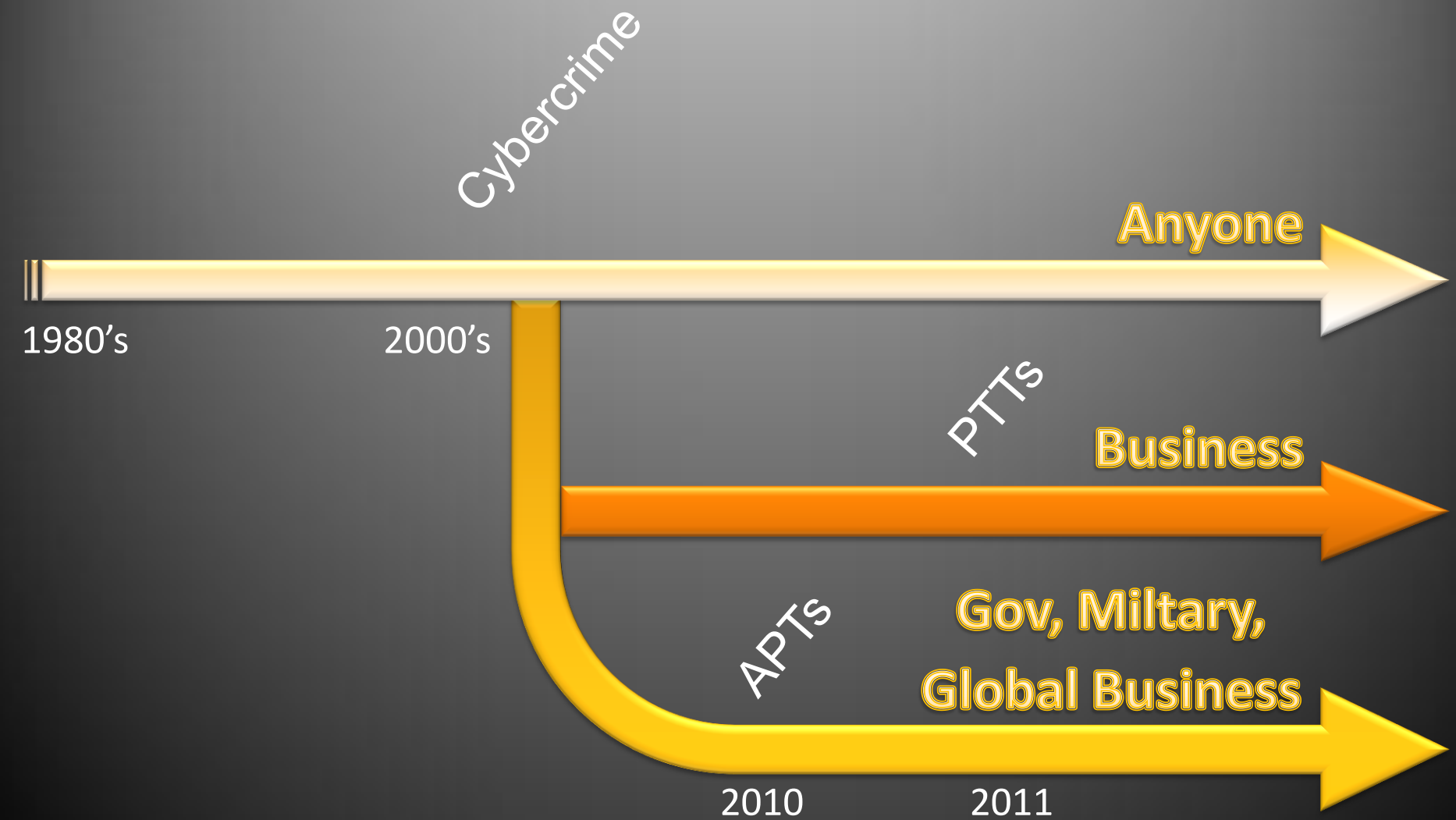

CYBERCRIME'S MO
TAKING LITTLE ACTION
2/10
Only 21% of victims reported cybercrime to the police
6/10
59% of victims who'd suffered both online and offline crime felt there were fewer ways to get help after the cybercrime
9/10
89% of all respondents agree that more needs to be done to bring cybercriminals to justice
75%
OF MILLENNIALS AGED 18-3
HAVE BEEN VICTIMS,
COMPARED TO 61% OF BAB
BOOMERS iv
64%
72%
OF MALES ONLINE HAVE
BEEN VICTIMS, COMPARED
TO 65% OF FEMALE ADULTS

Threat outlook

- 1.82 million new threats per day (>20 / s)
  - 785‘000 / day in 2010 (counted by hash)
- 11‘000 static signatures per day in 2010
  - 8‘000 / day in 2009
- 9 million detections per day in 2010
  - On average - each threat (hash) **on less than 15 machines**



Evolution of cyber attack



Symantec

Great train robberies take planning

- Shady RAT
- Nitro
- Duqu
- ……

Mail Online

Hackers steal secrets of £500m deal to clear WW2 landmines from former intelligence chief

By ROBERT VERKAIK

Last updated at 2:05 AM on 18th September 2011

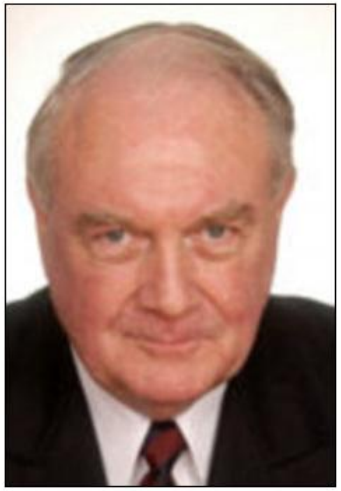
Comments (17) | Add to My Stories | Share Like 21

A former intelligence chief has been targeted by computer hackers alleged to have stolen secret documents relating to £500 million contracts for clearing mines.

One man has been arrested and police are investigating further allegations by Air Marshal Sir John Walker that his company email account was hacked and secret documents were copied and read.

Sir John's company, Countermine Technologies, was drawing up documents to bid for work near Tobruk in Libya where thousands of mines were laid during the Second World War. Company executives were also working on a Nato deal to clear mines on the Turkish-Syrian border.

Sir John and other Countermine executives suspect the information may be used by other companies to bid for mine-clearance work in the Middle East.



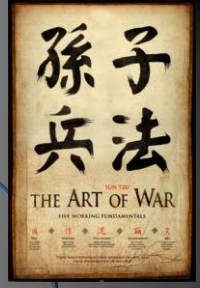
Victim: Air Marshal Sir John Walker's, pictured, e-mail was hacked and secret documents stolen

The arrest of a 52-year-old Swedish citizen, Lars Nylin, came after the firm instructed accountants PricewaterhouseCoopers to investigate the breach of Countermine's security.

The Sophisticated Actors Leverage the Market for Scale

APT / PTT	Attacker (Malicious Outsider)	Insider (Malicious and Non-malicious)	Hack-tivist	State Nation	Cyber Criminals
RESEARCH	Free Scanners	Insider Knowledge	Social Networks / Google	Espionage / Collusion	Data Mining
INCURSION	Basic Scripts /MetaSploit	Privileged Access	Social Engineering	Tailored Malcode / 0-Day	Attack Kits / Malcode / Bots / Affiliates
DISCOVERY	Random Targeting	Asset Awareness	Targets of Chance	Targets of Choice	Targets of Chance / Choice
CAPTURE	Visible / Low Value	Critical Assets	Media Worthy Asset or Access	High Value IP / Government Secrets	Monetized Assets
EXFILTRATE	Tagging and Damage	Theft and Damage	DDoS, Theft and Damage	Gain / Maintain Strategic Advantage	Fraud and Financial Gain

Rethink: Anatomy of an attack

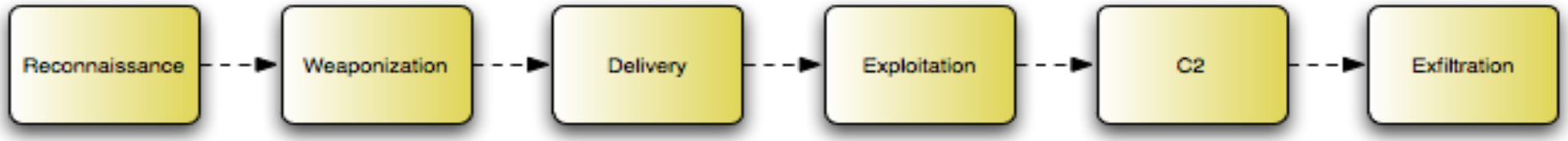


Required Capability

1. Research
2. Incursion
3. Discovery
4. Capture
5. Exfiltrate

Risk Posture and Policies

- Strong security awareness, counter intelligence
- Continuous enforcement of controls according to risk policy (mgmt and protection)
- Actively monitor infrastructure (endpoint to perimeter), information and users
- Control unusual internal movement and access of sensitive data
- Counter intelligence, forensics, damage mitigations and information recovery



Outlook

- Cyber Crime continues
  - More advanced mobile threats – profit oriented
- Increase in targeted attacks with personal touch (Social networking feeds)
- Persistent Targeted threats grow.
- Companies Attacks on the cloud - through the cloud

Symantec.

Thank You

Greg Day

Greg_Day@Symantec.com

GregDaySecurity