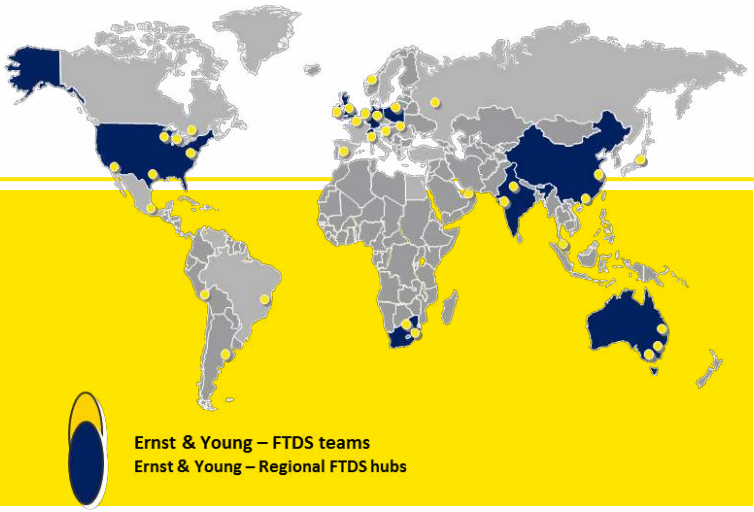

Cyber Warfare
„Infrastruktura ir žmones ivykus (kiber) atakai“.
„Infrastructure and the people in the event of (cyber) attack“.
EY
Building a better working world

Who am I

Massimo Cotrozzi
Assistant Director

Tel	+44 207806 9153
Mobile	+44 7552282328
Email	mcotrozzi@uk.ey.com



Background

- Massimo is an Assistant Director in the Fraud Investigation & Dispute Services practice, focusing on cybercrime, data breach investigations, network Intrusion, incident response and computer and network forensics.
- He joined Ernst & Young in 2013 and is based in London. Massimo has previous experience with firms supporting Corporations as well as Law Enforcement, Military Intelligence and Defence. He has been active in protecting from Cyber attacks and Digital Frauds and has performed a number of forensics activities and expert witness testimonies.

Skills

- Massimo has conducted and managed Information security activities, fraud prevention activities and forensic investigations for entities in all sectors, including FTSE 100 businesses and governmental organisations and agencies.
- He has presented at a number of security and e-Crime conferences around the world and has conducted local training and workshops to a variety of audiences (both technical and non technical).

Professional experience

- Investigation and identification of a conspiracy to commit fraud towards an UK financial organisation from management in their China HQ. The forensics activity was done remotely and involved bypassing local countermeasures that fraudsters had put in place to avoid IT forensics and bypassing Chinese Government "Great Firewall" in order to report evidence to the client and the authorities.
- Investigation on a major banking fraud involving the use of a botnet. The activities involved forensic analysis of a waterholing server, exploit kit deconstruction, malware identification and analysis, Command & Control Centre accessing in order to reveal which clients had been compromised. This led to the dismantling of a large money mule network organisation and the takedown of a multi thousand "clients" botnet.
- Investigation and forensic analysis on a state sponsored attack on an European Defence company, following a Military Intelligence Briefing. This involved working closely with the client's Incident Response Team and identifying which area of the company was breached and which data leaked.
- Forensic analysis on a multinational Legal Group regarding a breach which involved a data leak for a multi billion dollars litigation process.
- Provision of Information Security Audit and Computer Forensic support and data breach remediation to a Luxury Fashion brand following third-party disclosure of high value Intellectual property.
- Provision of Expert Witness testimony in support of litigation disputes involving copyright infringement and software piracy in complex file structures.
- Investigation and forensic support related to a Business Identity Theft and an international financial fraud perpetrated by a well known cyber criminal organisation, which resulted in several arrests.
- Network and systems forensic Analysis for two Formula 1 companies (in non related engagements) regarding the theft of intellectual property resulting in international cross border investigation assisting the companies and Law Enforcement.
- Investigation and forensic execution of a pre-acquisition fraud related to the chemical industry, where a company exported intellectual property to another firm days before an acquisition by an US company took place.
- Supply chain forensic support for a Luxury Retail brand in order to verify the source of an Intellectual Property breach related to a new material research.
- Investigation and tracking of the source of the sender of several anonymous threatening email.

What are we talking about

EY

The cyber threat landscape

Cyber attacks are headline news

- It is no longer possible to prevent attacks or breaches
- With organizations increasingly relying on vast amounts of digital data to do business, cybercrime is growing ever more damaging to an organization and its brands.
- The interconnectivity of people, devices and organizations opens up new vulnerabilities.
- New technologies, regulatory pressure and changing business requirements call for more security measures.
- What companies used to know and do to protect their most valued information is no longer enough.

What everyone wants to know is *"what can companies do about cybercrime?"*

The growing attacking power of cyber criminals

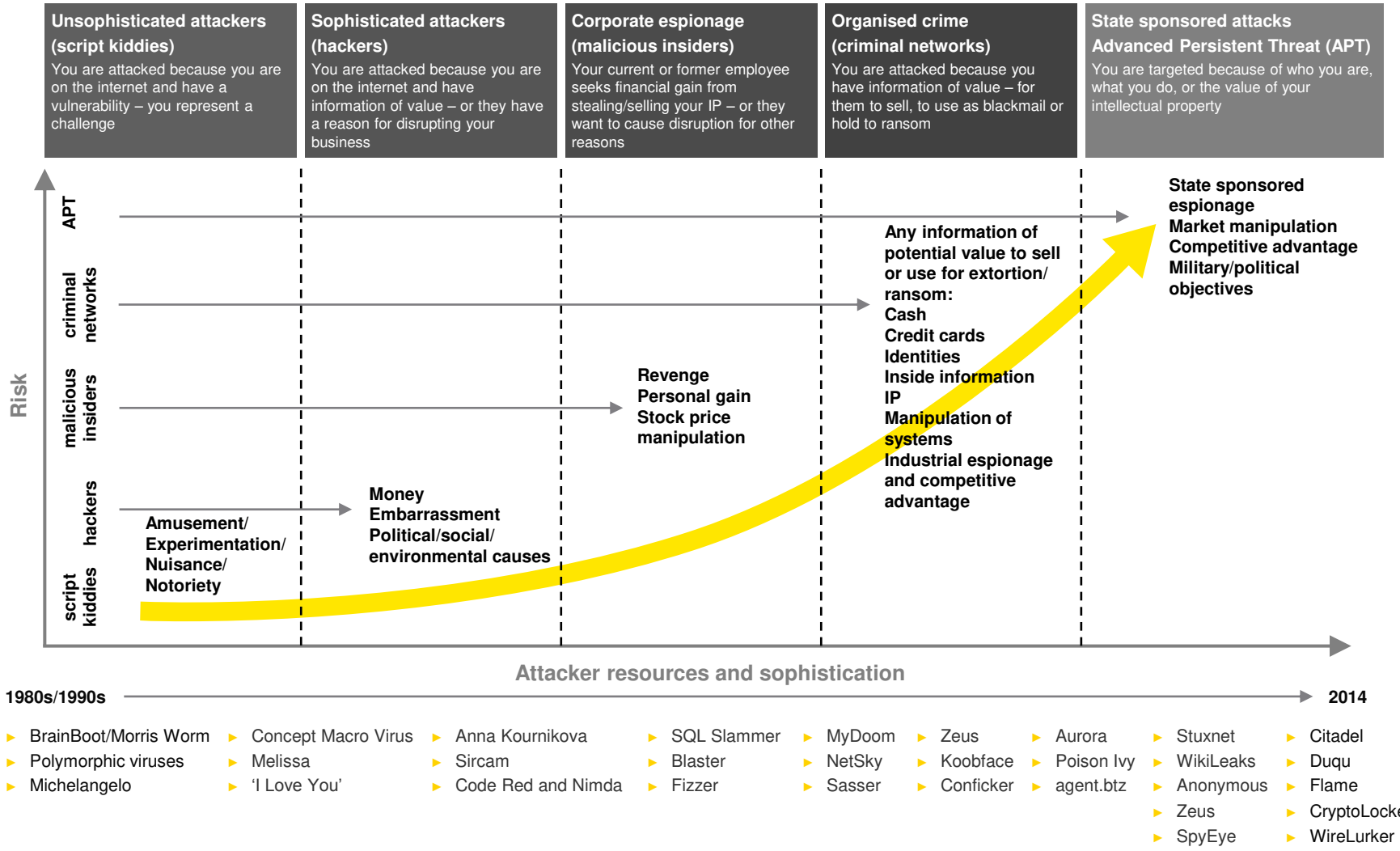
Cybercrime is big business. Today's attackers:

- Are more organized – they are not just opportunists
- Have significant funding
- Are patient and sophisticated – they will often gain access and wait until the right moment to pounce

Cybercrime is an organization-wide issue

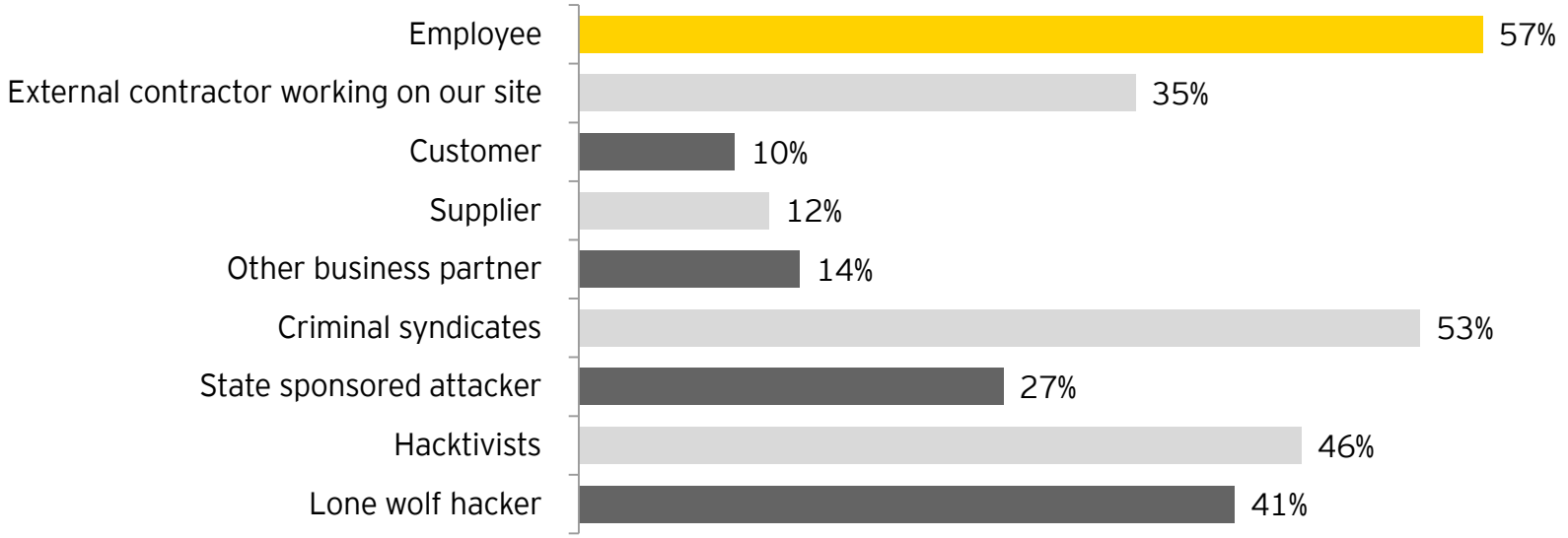
- Attackers take advantage of vulnerabilities in the whole operating environment – including people and process.
- Due to the relative ease of access via IP-addresses, operational technology systems are often targets for cyber criminals

Evolution of threats – attacks become better funded and more sophisticated

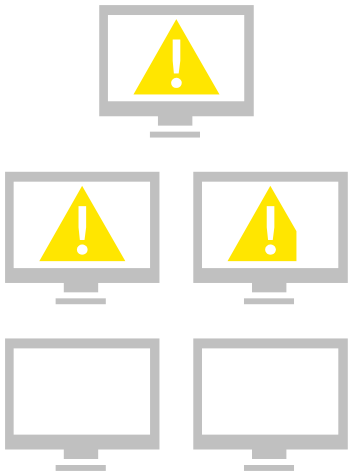


GISS 2014 results: "Who or what do you consider the most likely source of an attack?"

Respondents were asked to choose all that apply.



Organizations are simply not prepared for today's cyber threats - never mind tomorrow's



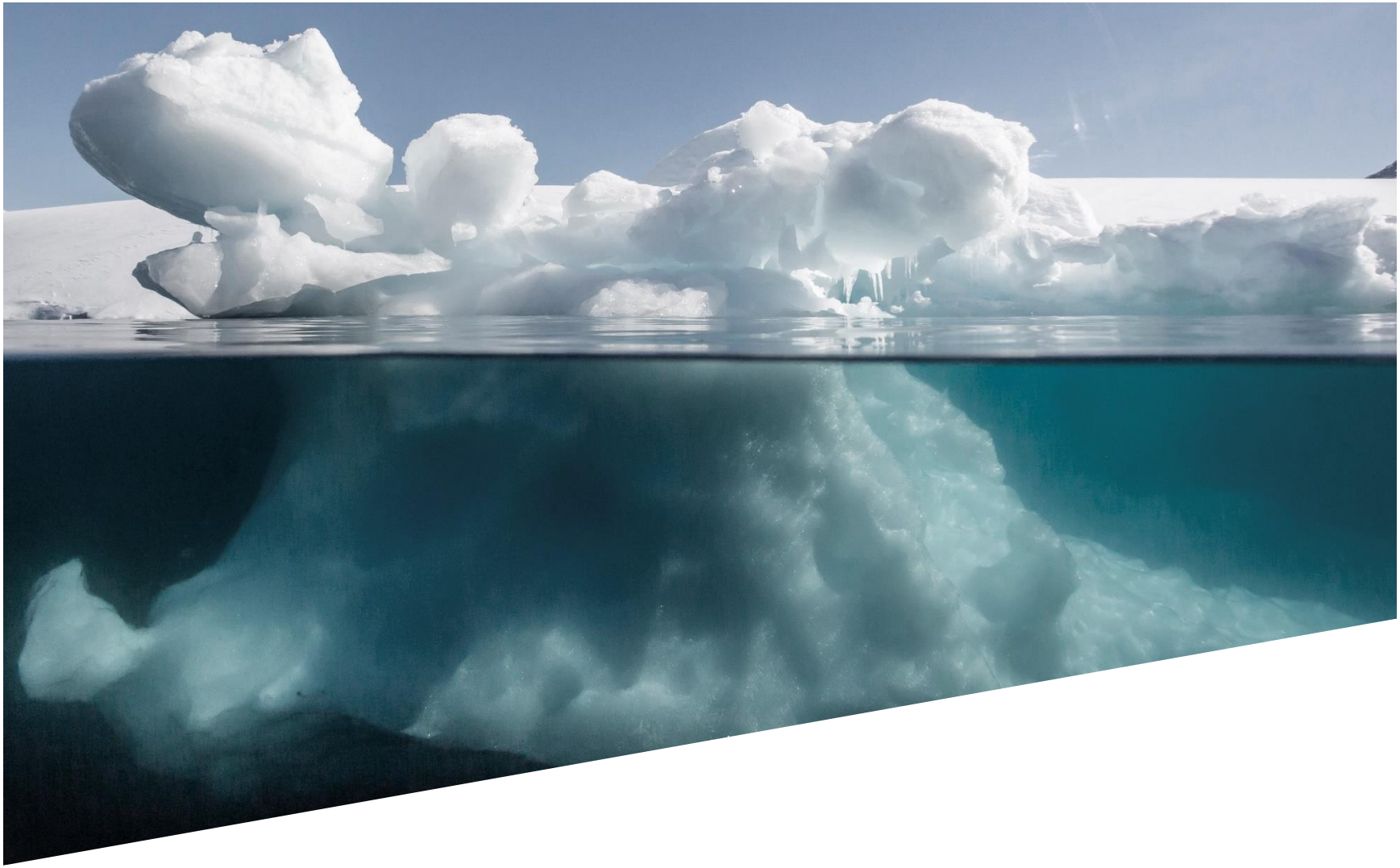
56%

of GISS 2014 respondents say that it is "unlikely" or "highly unlikely" that their organization would be able to detect a sophisticated attack.

The roadblocks facing today's organizations

- Roadblock 1 — Lack of agility
  - Organizations admit there are still known vulnerabilities in their cyber defenses and they are not moving fast enough to mitigate these. They are therefore lagging behind in establishing foundational cybersecurity.
  - **65% tell us that they lack real-time insight on cyber risks**
- Roadblock 2 — Lack of budget
  - For the first time, we see more organizations reporting that their information security budgets will not increase. There is a need for more money and resources to face the growing threats effectively.
- Roadblock 3 — Lack of cybersecurity skills
  - The lack of specialists is a constant and growing issue. Organizations also need to build skills in non-technical disciplines (like analytics) to integrate cybersecurity into the core business.

Meanwhile, in the military world…



Cyber attack realms

- Cyber warfare plays on many levels
- Military: objective: stealth / we don't want to get noticed and remain invisible till it's the time.
- This is also achieved by leveraging in-country access, which would have been gained through years, possibly decades, of pre-positioning.
- Formal structured teams working on gaining access using technological and HUMINT equities.
- Multi-billion dollar programmes working on this year after year.

Cyber attack – did you say billions?

- UK: £650 million over the next four years for cybersecurity
- Offensive activities are classified within the Single Intelligence Account: £2.1 billion (2011/2012) HUMInt, SIGInt, ELInt.
- US DoD provided budget estimates 2012 $3.2 billion, without offensive operations, which are funded from the national intelligence and military intelligence program budgets.

Cyber attack realms

- Civilian: objective: disruptive / we want to be impacting social life and threatening critical civilian infrastructure, finance and economy
- Geo-political: objective: retaliation / computer network attack (CNA) conducted by the military

Timeline

- Cyber warfare doesn't start when a war starts, it happens before the actual war
- It's happening now and it has been going on for quite a while

- Years or decades beforehand if it’s nation state actors.
- A battle of attrition, assets will be gained and lost continually.
- Time will be spent understanding the target and keeping the ‘weapons’ relevant.

Targets

- What would we want to do?
- Infiltrate
  - Technology firms
  - Financial institutions
  - Critical infrastructure
  - Telecommunications
  - Medical systems
  - ...

Methodology

- How would we do it?
- If infiltration is discovered it shouldn't be possible to revert back to us
- We don't want to burn our research (i.e the latest 0day)
- Large scale cyber warfare is difficult to hide attribution, political scene will make it obvious.
- Pre-positioning work and the ‘how’ of it must employ some covering of the tracks.
  - Utilise hackers, underground groups, standard criminals to achieve the goal….

Methodology/cont

- …. and there's where the problem arise
- "managing hackers is like herding wild cats“

- Not all hacks are related to military, not all military operations are connected to "non military" operators
- Due to the exchange of information, criminals are increasing their capability (still some years behind)

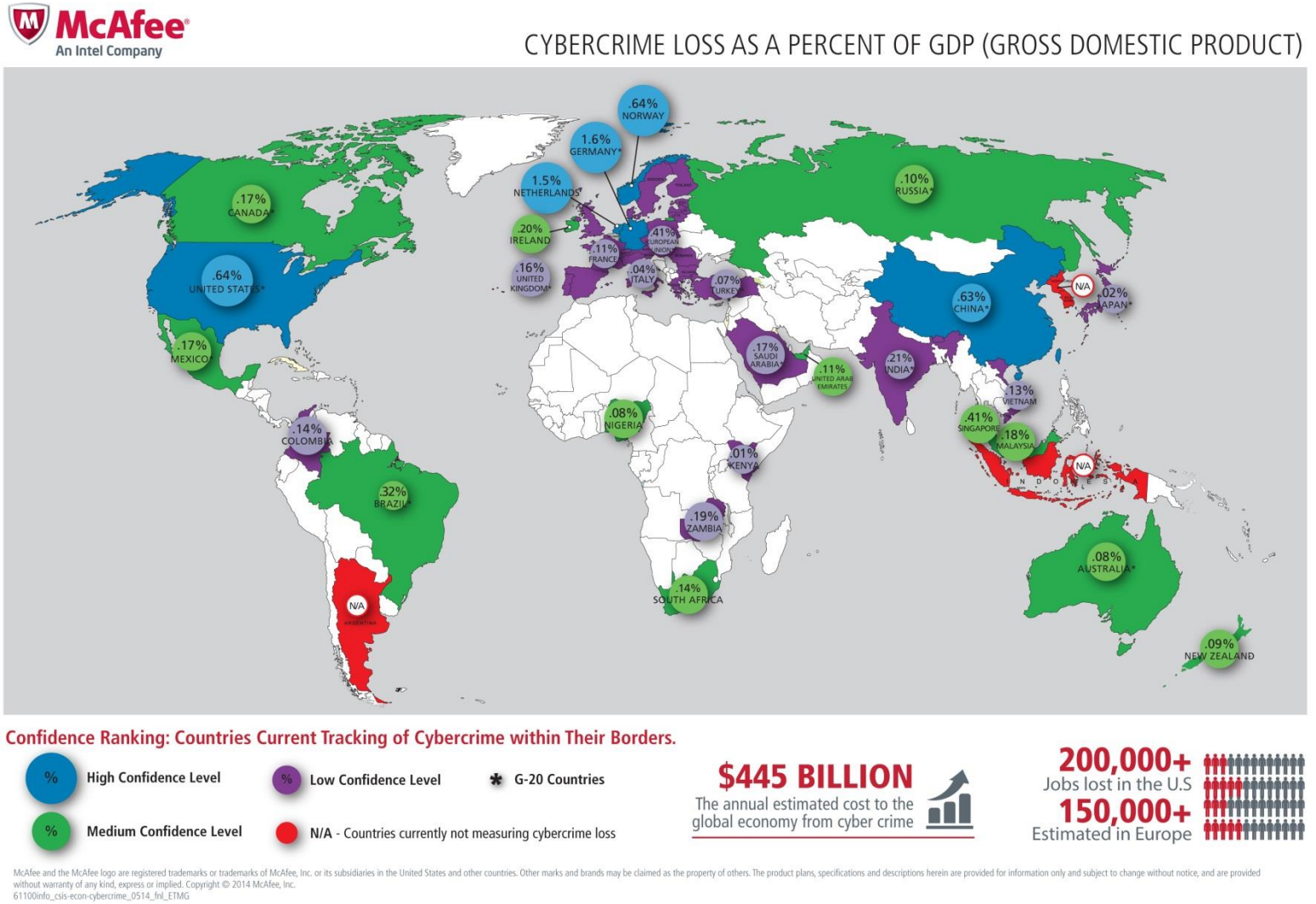
Results

- What damage is currently being caused?
- What damage would be caused in case of a proper cyber attack?

What is possible today

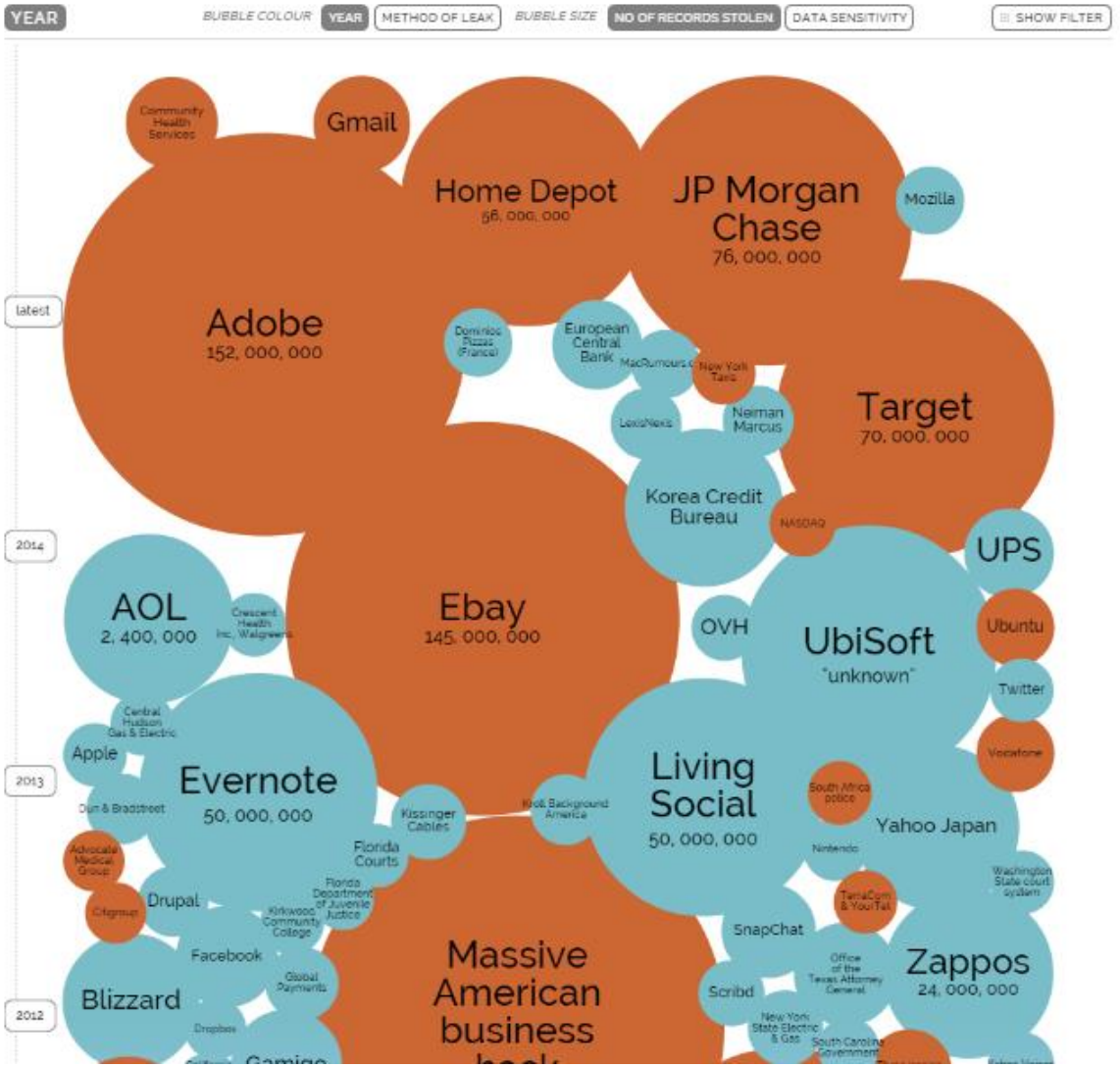
- Examples of cyber warfare tools:
  - Can make mobile phones explode
  - Can make nuclear turbines burn
  - Can make pharma companies mix ingredients in the wrong amounts
  - Can make planes divert from routes and disappear
  - Can make nuclear missiles launch
  - Can make nuclear submarines land in the wrong place
  - Can make drones land in the wrong airfields
  - Can make satellites report on wrong events (or viceversa)
  - Can make… you name it. If there's a computer, it can be done…

Cyber Crime has a material impact on GDP and employment



http://www.mcafee.com/in/resources/misc/infographic-cybercrime-loss-gdp.pdf

World's Biggest Public Data Breaches
Selected losses greater than 30,000 records



(Source http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)

Latest Financial Industry public breaches

RANK	ORGANIZATION BREACHED	DATE BREACHED	RECORDS BREACHED	LOCATION	INDUSTRY	SOURCE OF BREACH	TYPE OF BREACH	RISK S CORE
1	JPMorgan Chase	8/27/2014	76,000,000	United States	Financial	Malicious Outsider	Identity Theft	**10.0**
2	Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Kookmin Card	1/20/2014	104,000,000	South Korea	Financial	Malicious Insider	Identity Theft	**10.0**
3	Visa, Mastercard, American Express, and Discover cards	3/25/2014	7,000,000	Ukraine	Financial	Hacktivist	Financial Access	**8.3**
4	SuperValu,loyaltybuild, Axa Insurance, Electricity Supply Board	10/25/2013	1,500,000	United Kingdom	Financial	Malicious Outsider	Financial Access	**8.3**
5	Affin Bank Berhad and Affin Islamic Bank Berhad	9/27/2014	1,271,000	United Kingdom	Financial	Malicious Outsider	Financial Access	**8.2**
6	Court Ventures, Experian	10/21/2013	500,000	United States	Financial	Malicious Insider	Identity Theft	**7.8**
7	Iranian bank	11/1/2013	3,000,000	Iran	Financial	Accidental Loss	Financial Access	**7.7**
8	NongHyup Life Insurance Co,NongHyup Financial Group Inc	1/5/2014	350,000	South Korea	Financial	Malicious Insider	Identity Theft	**7.6**
9	Affinity Gaming	3/14/2013	300,000	United States	Financial	Malicious Outsider	Financial Access	**7.6**
10	Boleto	7/4/2014	275,730	Brazil	Financial	Malicious Outsider	Account Access	**7.3**

(Source http://breachlevelindex.com/#!breach-database) HSBC recently announced the loss of 2,7M record

Thank you

Building a better working world