



**VAUBAN**  
GROUP

**CYBER SECURITY**  
**NOT ALL ROCKET SCIENCE**

**BIBF FORUM**

**MAY 2017**

## Chief Strategy Officer at Vauban

### My Background

- **Languages (French and Spanish)**
- **Foreign Office (New York, Moscow)**
- **MBA**
- **Unisys**
- **PwC**
- **Defence Strategy and Solutions**
- **General Dynamics**
- **Aegis Advisory**

What happens....

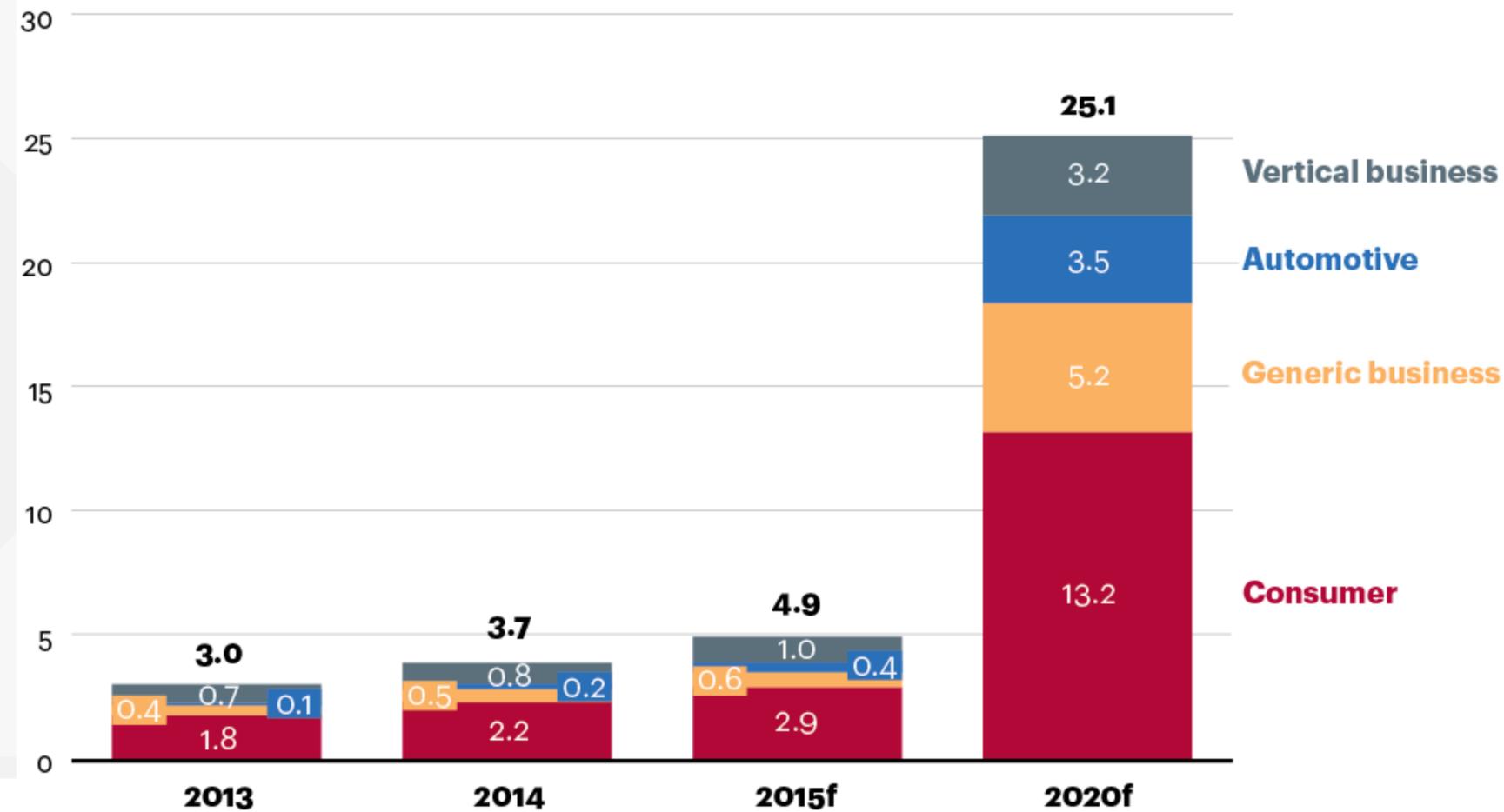
.....in an internet minute?



Figure 17  
**Staggering growth of the Internet of Things (IoT)**

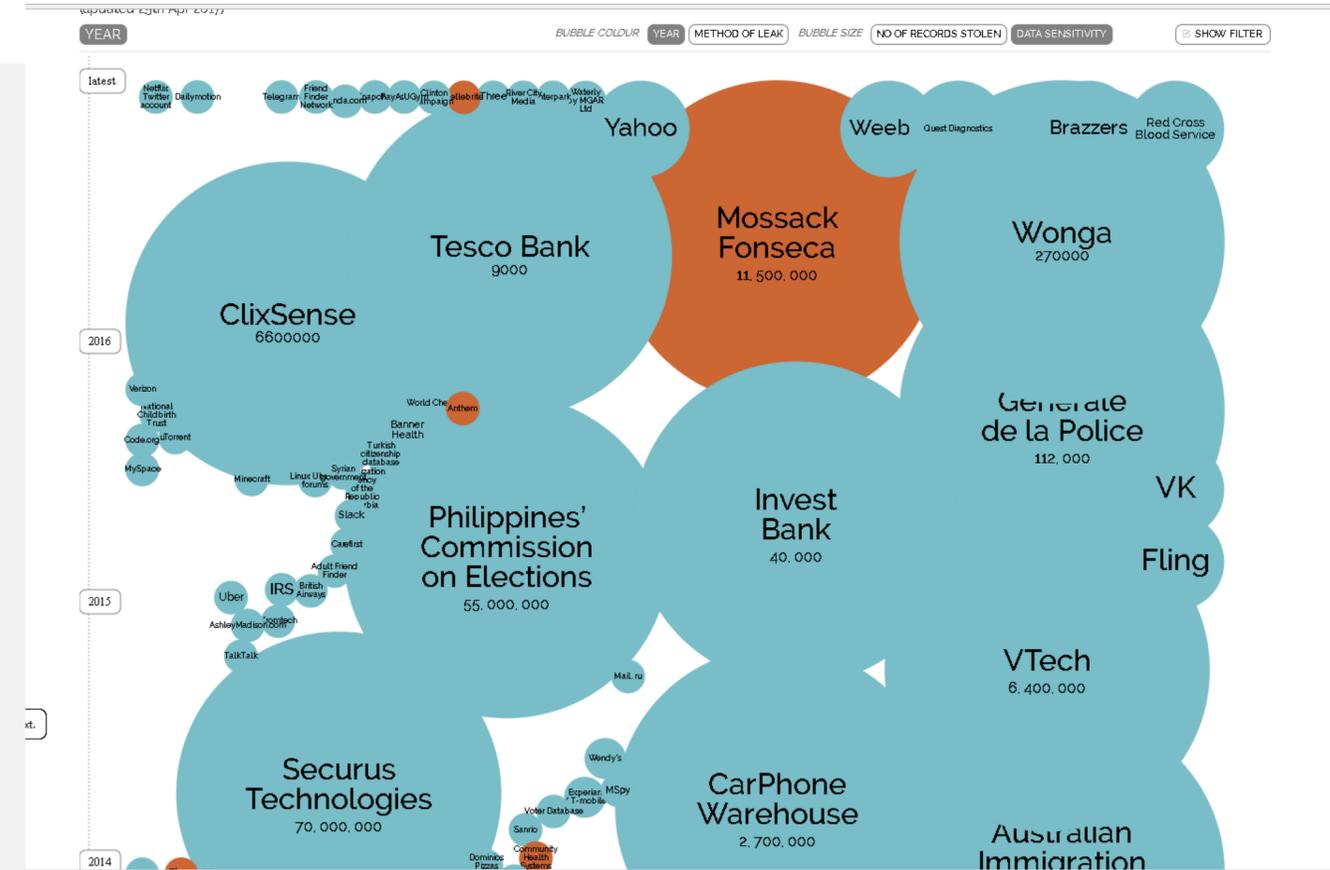
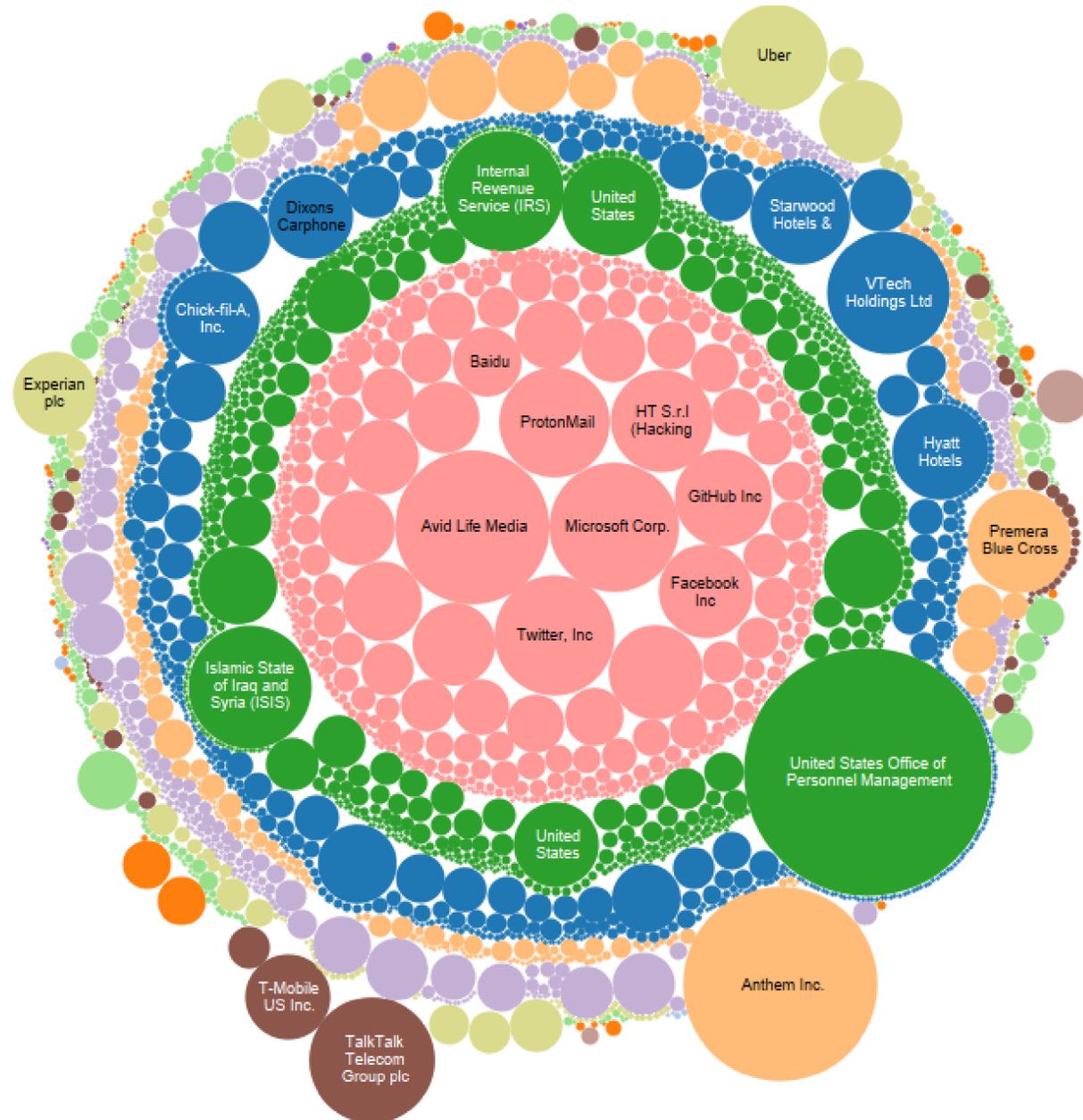
**IoT units installed**

Billion



Sources: Gartner Symposium/ITxpo; A.T. Kearney analysis

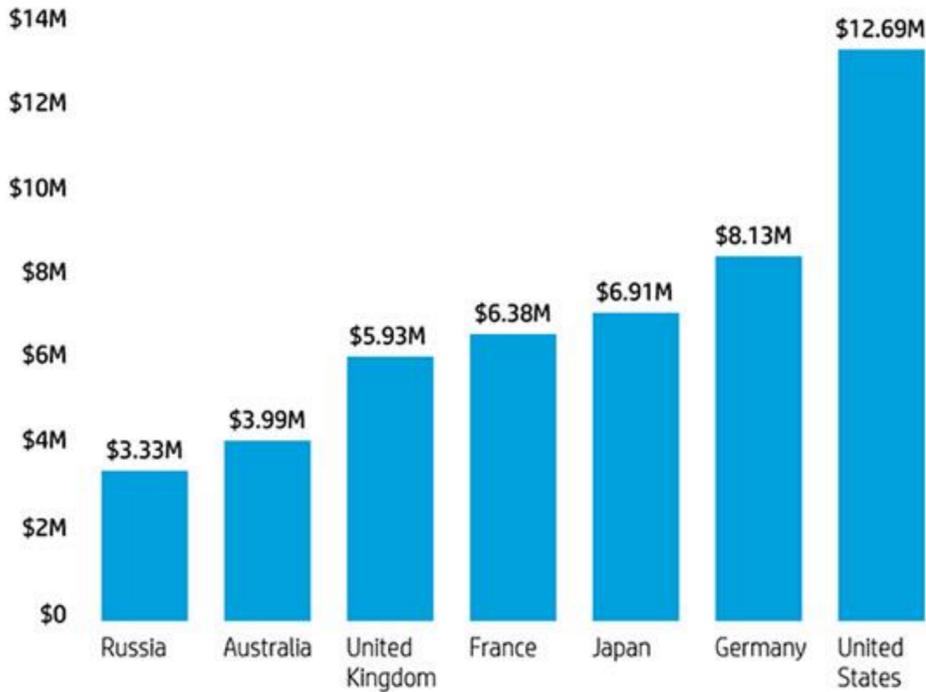
# CYBER CRIME



**EVERY SECTOR  
EVERY COUNTRY  
ALL THE TIME**

- IT
- Consumer Goods
- Other Orgs
- Telecom
- Entertainment
- Energy
- Government
- Financials
- Industrials
- Healthcare
- Utilities
- Materials

**Average cost of cyber crime in seven countries**

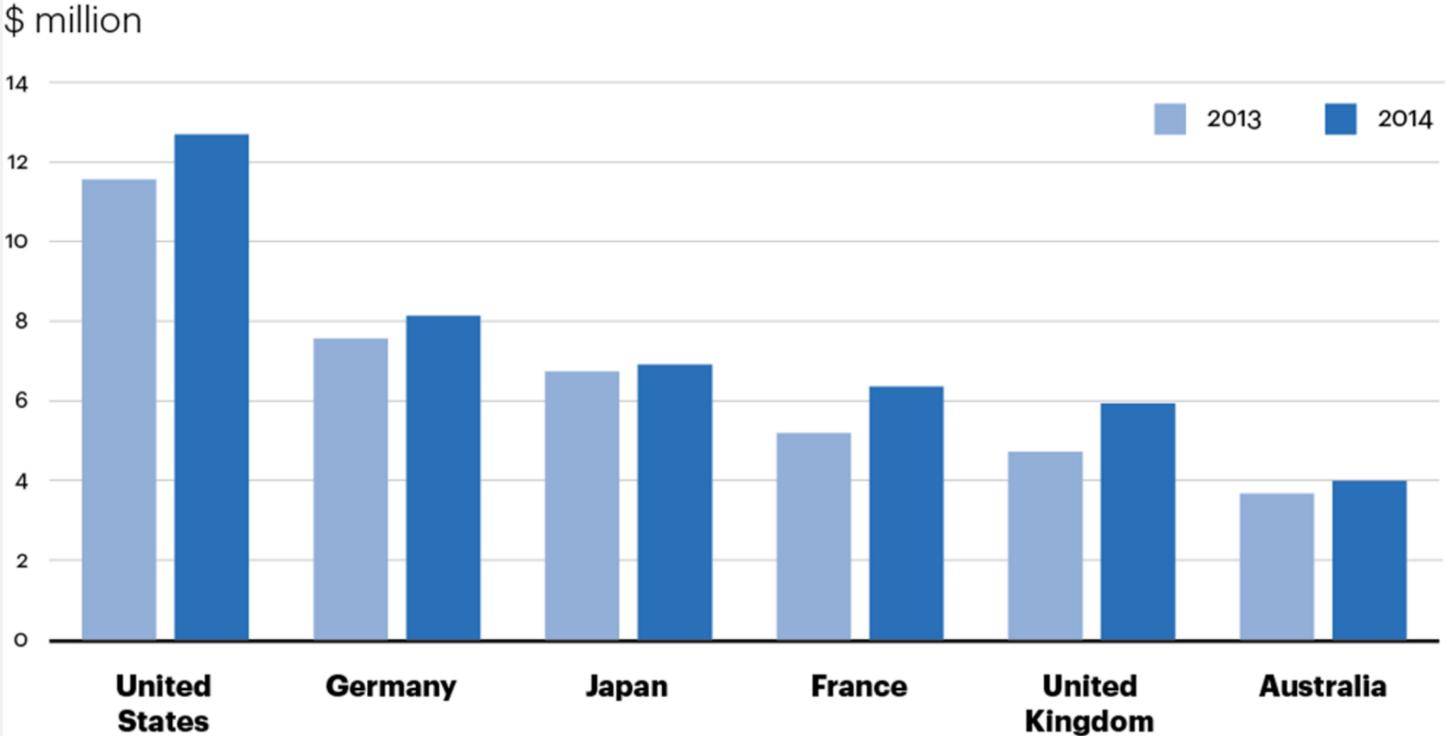


The average costs of cyber crime in seven countries (converted to U.S. dollars for comparison) show that U.S. companies average a significantly higher total cost than in other nations.

Source: The Ponemon Institute, surveying 257 companies

**EXPENSIVE**

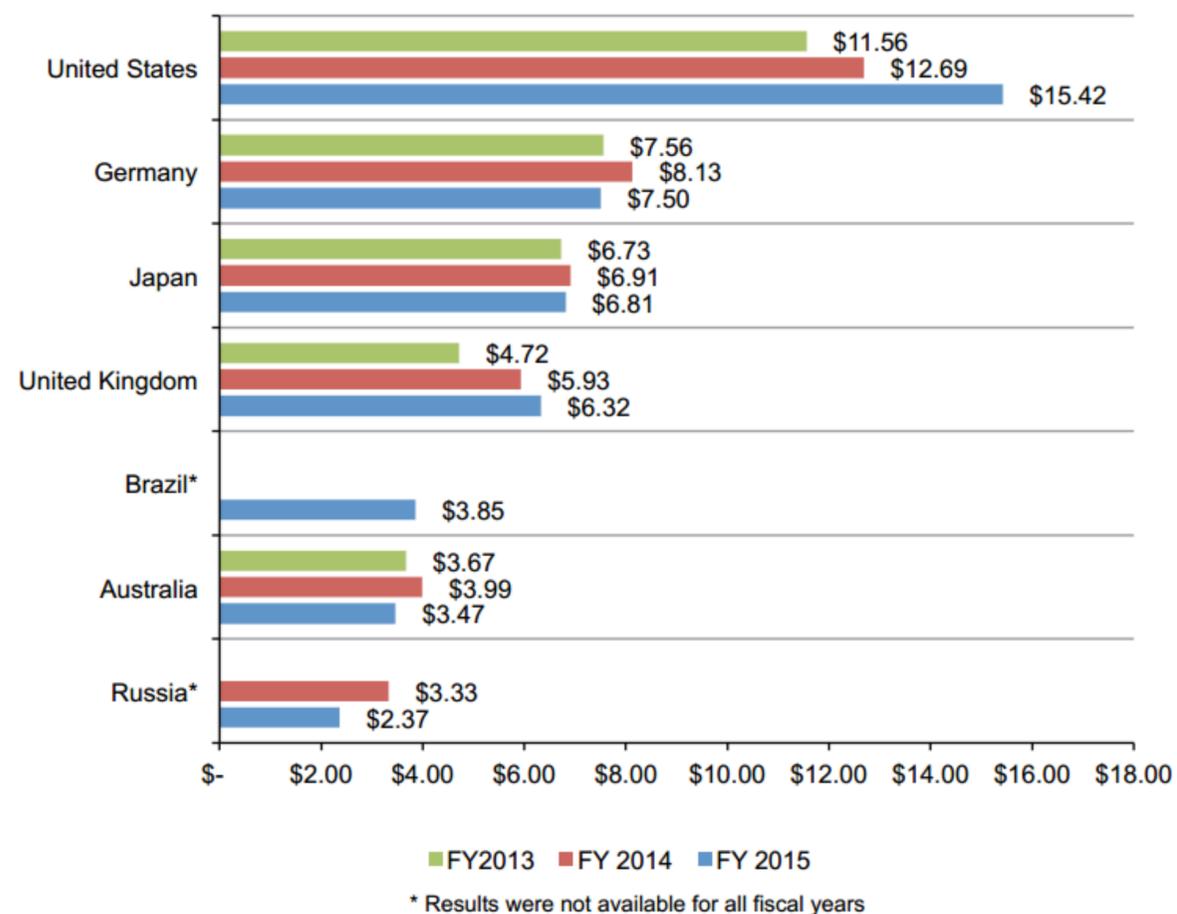
**Average cyber crime cost per company in key markets**



Sources: Ponemon Institute; A.T. Kearney analysis

**GROWING**

**Figure 1. Total cost of cyber crime in seven countries**  
 Cost expressed in US dollars (000,000), n = 252 separate companies



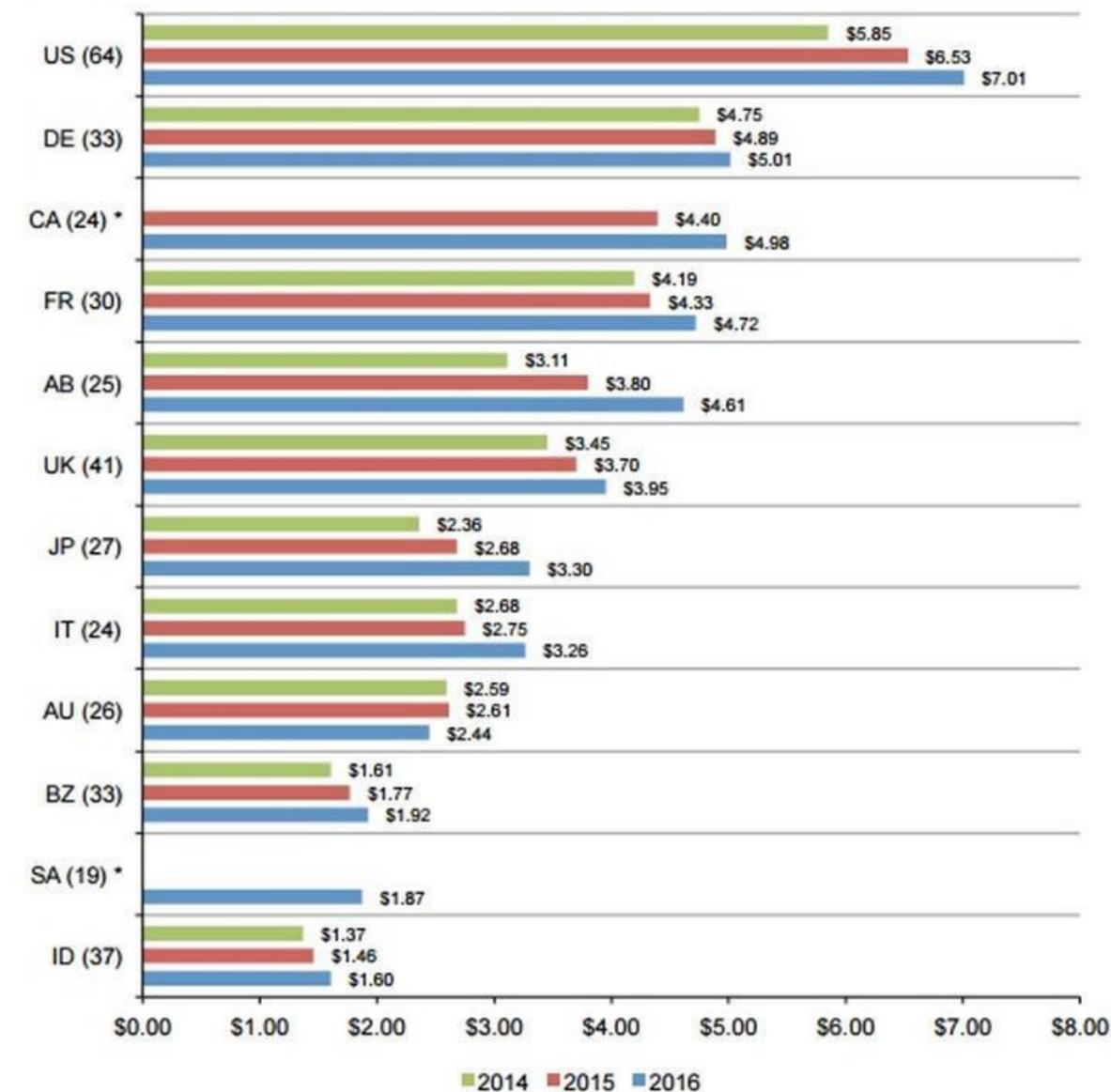
**EXPENSIVE**

**GROWING**

**Figure 2. The average total organizational cost of a data breach over three years**

Grand average for FY 2016=\$4.0, FY 2015=\$3.8, FY 2014=\$3.50

\*Historical data is not available in all years  
 (FY 2016=383, FY 2015=350, FY 2014=315)  
 Measured in US\$ (millions)



- **What is most important to you, your people, your organisation, your country?**
- **Do you know where your data is?**
- **Do you know what is being accessed, by whom, and how data moves on your network?**

## **1. If you have experienced a cyber attack:**

- How did you find out?**
- How much did it cost to remediate?**
- Were there have adequate response plans? Insurance?**

## **2. What is the average delay between breach and discovery?**

- 9 months**

## **3. Up to how much will the EU be able to fine companies for failure to report a serious breach within 72 hours?**

- 4 % of global turnover**

## **4. In your organisation, who is responsible for the cyber risk?**

## **5. Is cyber regularly on their board agenda?**

**UK GOV EXAMPLE**

# Common Cyber Attacks: Reducing The Impact

Most cyber attacks are composed of four stages: **Survey**, **Delivery**, **Breach** and **Affect**. The following security controls, applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

**81%**  
OF LARGE COMPANIES  
REPORTING BREACH

**£600K -  
£1.15m**  
AVERAGE COST OF  
SECURITY BREACH

Source: 2014 Information Security Breaches Survey sponsored by the Department for Business, Innovation and Skills.



**Who might be attacking you?**

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.



# WHAT MIGHT A BREACH MEAN?



Breach day: shares at 289.4p – market cap £2.7bn  
Today: 193.2p – market cap £1.83bn



**CEO accountability**  
**Political unacceptability**  
**Reputational damage**  
**Company value**

**£900m loss of shareholder value**  
**£60m write off 2015**  
**100,000 customers**

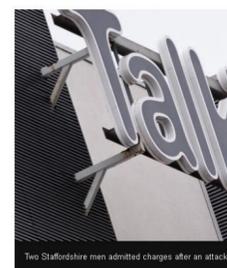
# WHO IS DOING THIS?



News navigation bar for BBC News, including links for Home, UK, World, Business, Politics, Tech, Science, Health, Education, Entertainment & Arts, Video & Audio, and More. Includes a search bar and 'Find local news' button.

## TalkTalk hack attack: Friends admit cyber crime charges

26 April 2017 Stoke & Staffordshire



Two friends have admitted their part in a £42r website.

Matthew Hanley, 22, and Connor Allsopp, 20, admitted massive data breach in October 2015.

News navigation bar for BBC News, including links for Home, UK, World, Business, Politics, Tech, Science, Health, Education, Entertainment & Arts, Video & Audio, and More. Includes a search bar and 'Find local news' button.

## Teenage cyber hacker Adam Mudd jailed for global attacks

25 April 2017 Beds, Herts & Bucks



A computer hacker has been jailed for two years online attacks as a teenager from his bedroom

Adam Mudd, now 20, admitted creating malware in 1.7 million cyber attacks.

Among the victims were gaming websites including fantasy game Runescape, the Old Bailey heard.

Judge Michael Topolski said Mudd "knew full well the

## Kenya Revenue Authority 'lost \$39m to hacker'

22 March 2017 Africa



An IT expert has been charged with hacking in and stealing \$39m (£31m).

Alex Mutungi Mutuku, 28, is accused of electronic fraud.

The prosecution says he is part of an international ring of several state bodies.

The government says there is a ring involving expats from other countries, along with police officers and civil servants.

MailOnline News navigation bar, including links for Home, News, U.S., Sport, TV & Showbiz, Australia, Femail, Health, Science, Money, Video, Travel, Fashion Finder, and more. Includes a search bar and 'Find local news' button.

## Chinese hackers 'tried to infiltrate a company linked to US-built THAAD missile system set up in South Korea'

- US cyber security expert said China regularly uses espionage to target missiles
- South Korean government spokesman said it had intervened to stop the hackers
- Chinese officials denied any involvement and asked for THAAD to be scaled back
- The anti-missile defence programme met with mixed opinions in South Korea

By GARETH DAVIES FOR MAILONLINE

PUBLISHED: 09:28, 27 April 2017 | UPDATED: 22:52, 27 April 2017

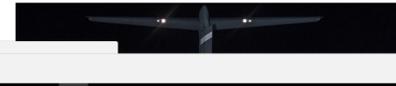
57 shares

An American security firm believes Chinese hackers tried to infiltrate a company linked to the US-built THAAD anti-missile defence system set up in South Korea.

Chinese officials, who have been calling for the programme aimed at protecting Seoul from North Korea's nuclear threat to be scaled back, denied any involvement.

But a US cyber expert said China regularly uses espionage and a South Korean government spokesman said it had blocked hackers from targeting their missiles system within the last month.

Scroll down for video



News navigation bar for BBC News, including links for Home, UK, World, Business, Politics, Tech, Science, Health, Education, Entertainment & Arts, Video & Audio, and More. Includes a search bar and 'Find local news' button.

## Router hacker suspect arrested at Luton Airport

23 February 2017 Technology



A British man suspected of being behind an attack on Deutsche Telekom routers has been arrested at Luton Airport.

The November attack hijacked about 900,000 routers and briefly stopped their owners getting online.

The UK's National Crime Agency said it arrested the man under a European Arrest Warrant on behalf of Germany's federal criminal police force (BKA).

The BKA said it wanted to extradite the 29-year-old to Germany to face charges of computer sabotage.

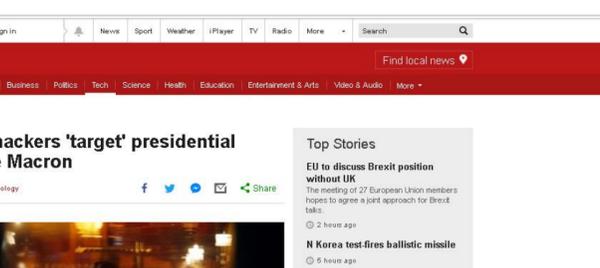
"He is accused of being the mastermind behind the attack," Cologne public prosecutor Dr Daniel Vollmert told the Press Association.

In a statement (in German), the BKA said the attack last year was "particularly serious" and was carried out in a bid to enroll the home routers in a botnet - a network of hijacked machines.

News navigation bar for BBC News, including links for Home, UK, World, Business, Politics, Tech, Science, Health, Education, Entertainment & Arts, Video & Audio, and More. Includes a search bar and 'Find local news' button.

## 'NSA malware' released by Shadow Brokers hacker group

10 April 2017 Technology



Key Macron staff into handing over login names

targeting the campaign of French presidential Macron, say security experts.

ire and fake net domains were all being used as attack

Hacquebard, from security company Trend Micro.

ved to be part of the same group that targeted the US

it is behind attacks aimed at Mr Macron.

abord said the group behind the "aggressive" attacks was a

ckers known widely as Fancy Bear, APT28 and Pawn

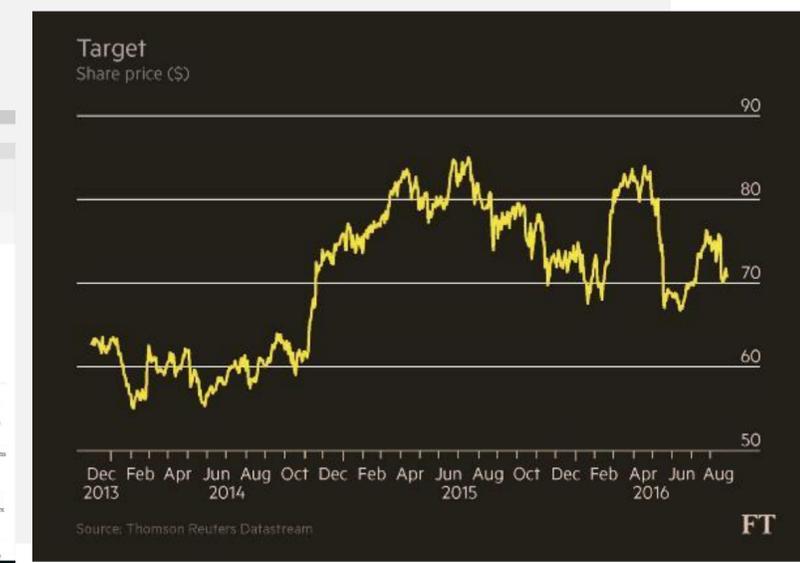
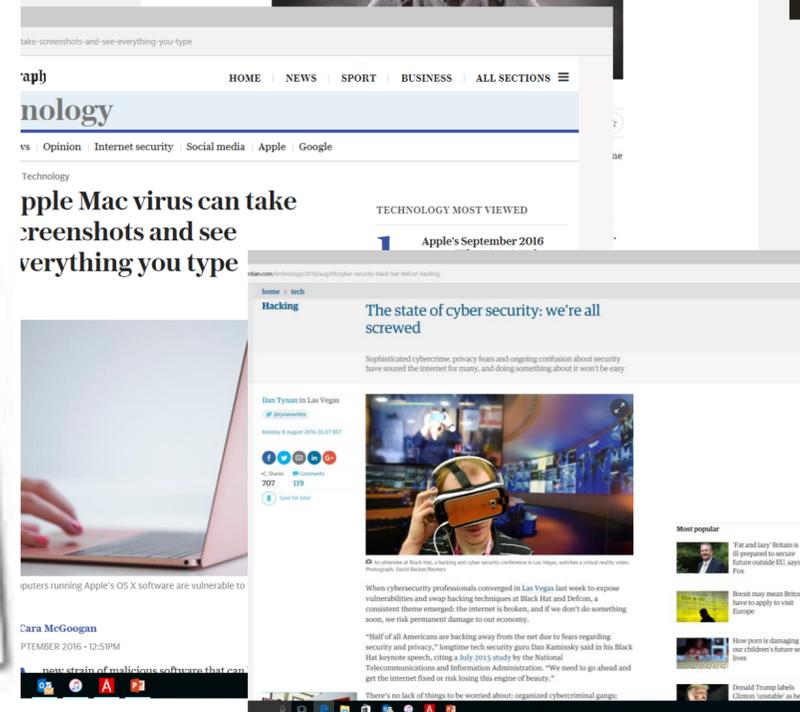
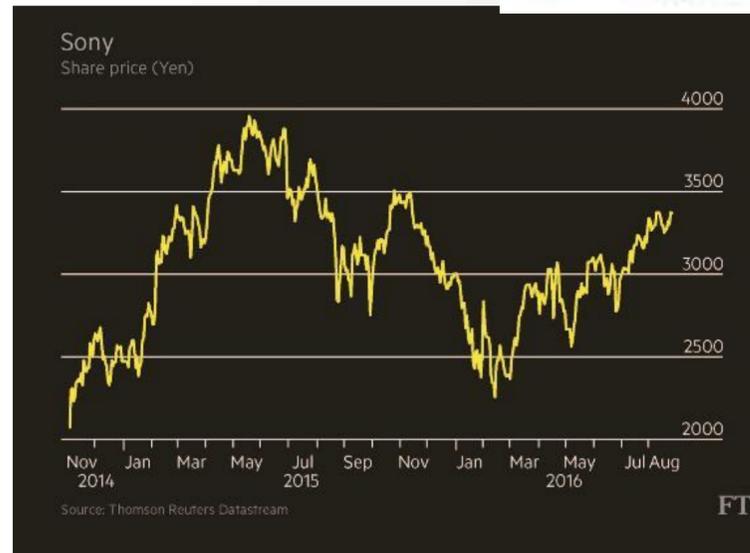
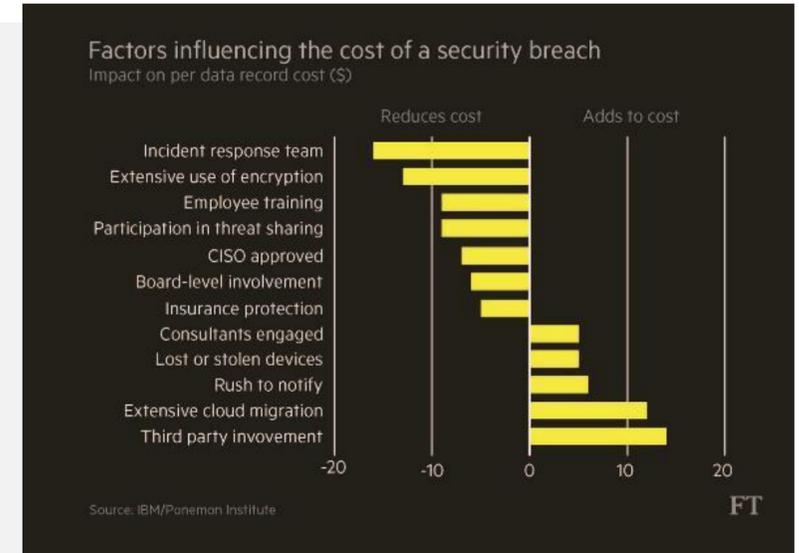
usion an extensive arsenal of hi-tech con tricks to crash

Top Stories sidebar for BBC News, including links for EU to discuss Brexit position without UK, N Korea test-fires ballistic missile, and Hundreds to lodge claims against surgeon.

Features sidebar for BBC News, including links for The women banished to a hut during their period and 10 things we didn't know last week.

Cybercrime article from The Guardian, titled 'Hackers attacked one in five UK firms last year, survey finds'. The article discusses a survey by the British Chamber of Commerce (BCC) showing that 24% of businesses were attacked by cybercriminals in the past year. It also mentions that larger companies were more susceptible to attacks and that the survey followed a series of high-profile attacks on company databases.

# A NEWS ITEM ALMOST EVERY DAY



- Experts claim that 80% of cyber vulnerabilities can be dealt with through 'normal' cyber hygiene
- Many organisations are spending too much or in the wrong areas, driven by fear, uncertainty, or the inability to quantify the risk and therefore prioritise

- **The 20% that is not normal is really very sophisticated**
- **Assume that most IT networks are already compromised: protect your data first**
- **Educate everyone - and make it matter personally to the Board and CEO**
- **Work out what is really important to the organisation- what are the Crown Jewels?**

- **Policies and Procedures**
- **State of your IT estate (Patching, Configuration)**
- **Educate and enforce – tough on breaches EVERYWHERE**
- **Mandate at Board level with budget**
- **Manage the risks dynamically**