
# Cybersecurity – (K)eine Chance gegen Internetspione

*Einführung/Introduction*

DAJV Jahrestagung 6. September 2014
Klaus Beucher, LL.M. (Wisconsin-Madison), Partner, Freshfields Bruckhaus Deringer LL.P.

Freshfields Bruckhaus Deringer

# Cyber-Agenda

1. **Cyber attacks**
   - Some figures and trends
   - Types and targets of cyber attacks
2. **Risk perception: US vs. Europe**
3. **Political awareness and activities**
4. **Regulatory topics**

# Cyber moments

# Cyber moments

September 2, 2014 9:36 am

## I'm not a celebrity – get me out of hacks

Last updated: September 2, 2014 9:07 pm

## Apple admits celebrity accounts hacked but denies iCloud breach

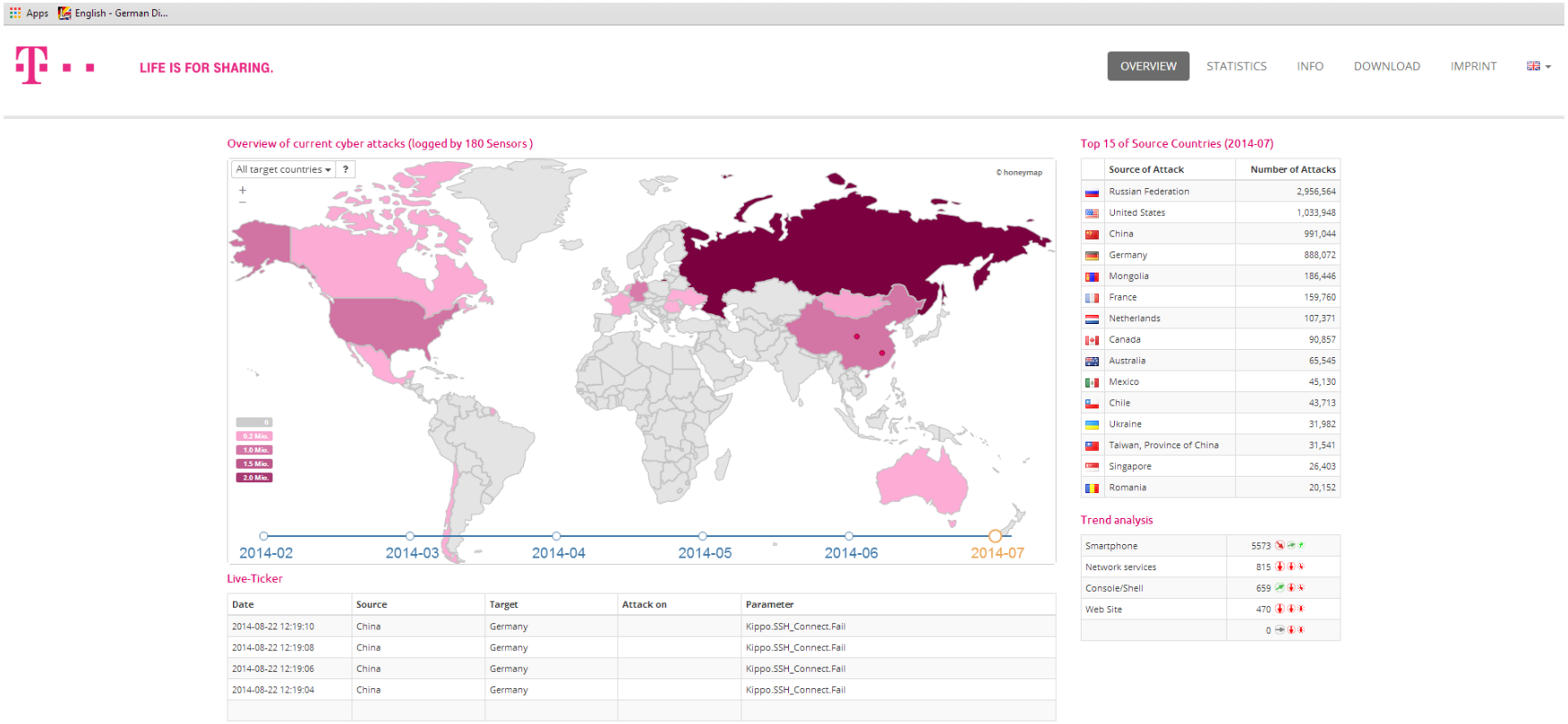
The New York Times

## *Path of Stolen Credit Cards Leads Back to Home Depot Stores*

By NICOLE PERLROTH SEPT. 3, 2014

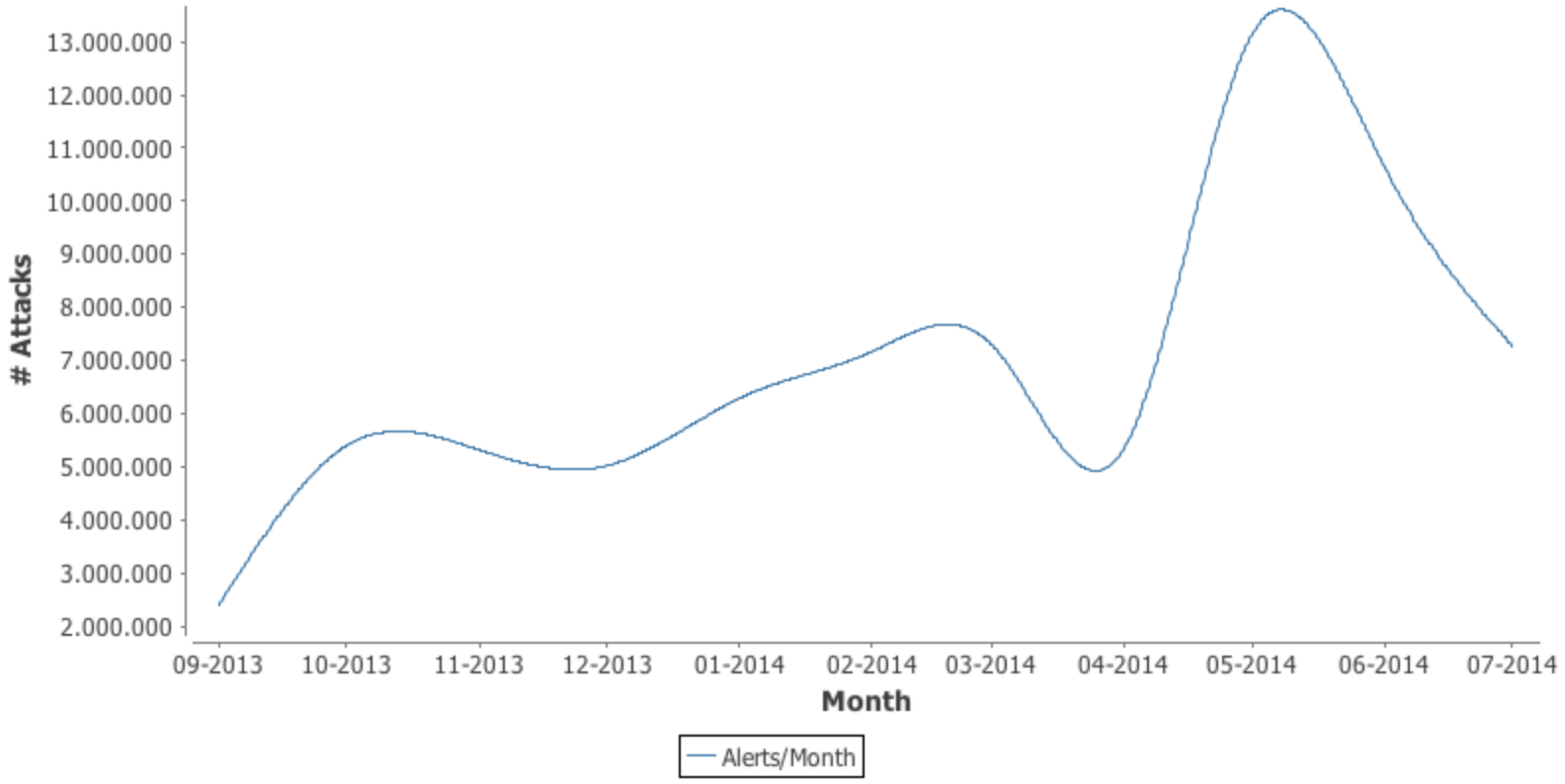
# Cyber attacks – a rising tide

http://www.sicherheitstacho.eu/?lang=de



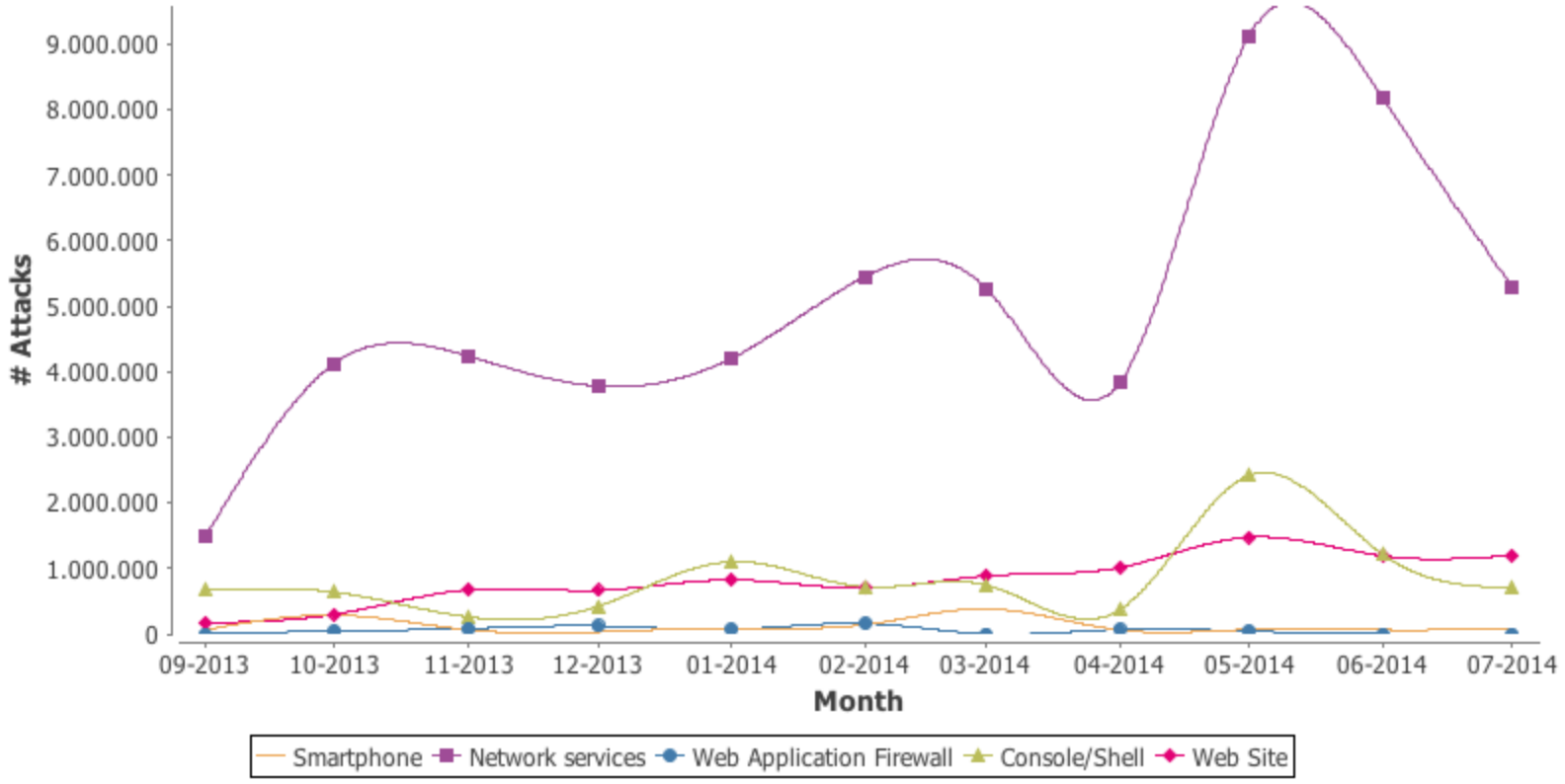

Source: Deutsche Telekom AG – www.sicherheitstacho.eu

# Overall numbers of attacks in major economies




Source: Deutsche Telekom AG – www.sicherheitstacho.eu

# Number of attack by infrastructure




Source: Deutsche Telekom AG – www.sicherheitstacho.eu

# 2013 Trends

- Number of targeted attacks increased by 91%
- Over 552 m identies were jeopardized by data attacks
- 23 zero-day security gaps were identified
- 38% of mobile users was a victim of mobil Internet crime during the last 12 months
- 1 out of 392 emails used to launch a phishing attack
- Web-based attacks increased by 23%
- 1 out of 8 legitimate websites has a critical security gap

Source: 2014 Symantec Internet Security Threat Report

# Different types of attacks

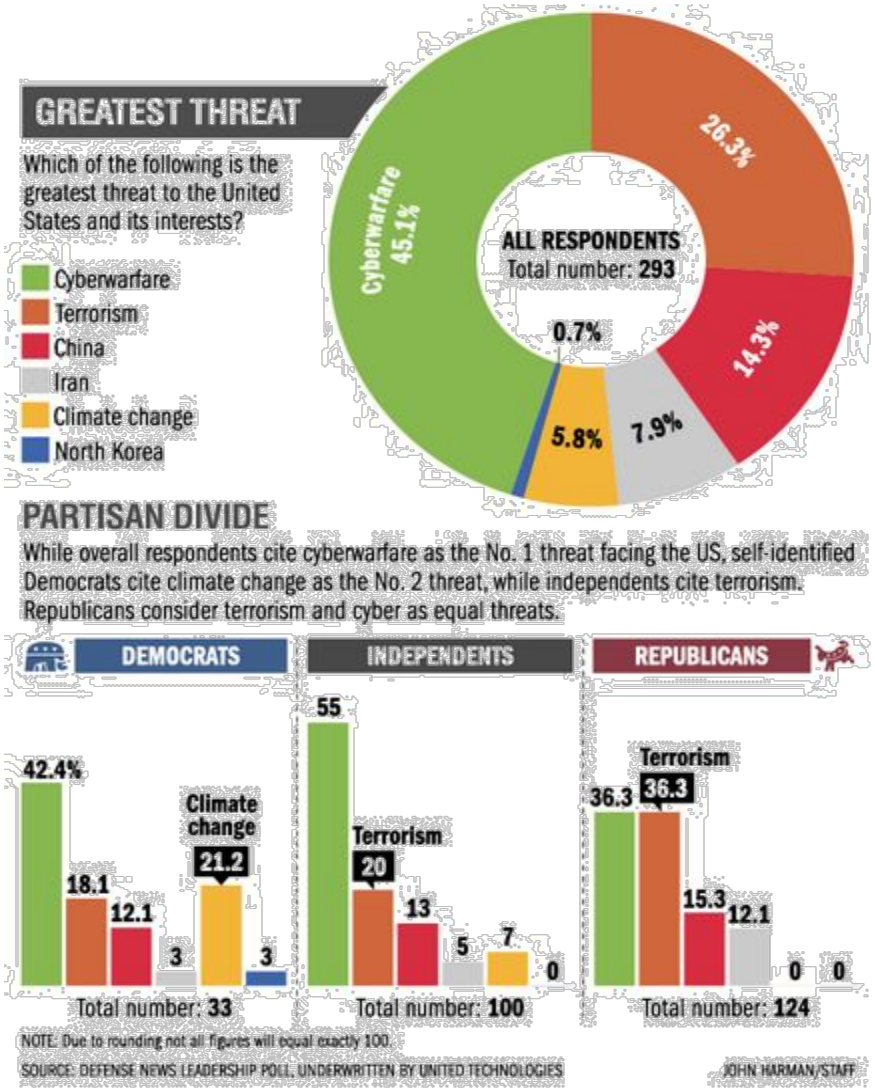
| | |
|---|---|
| **Criminal** | • **2013: Vodafone Germany: hacker captured data of 2 million customers**<br>• **2013: Barclays theft of £1.3m by computer added robbery; possible use of DoS to manipulate target's stock**<br>• **2013 Target Corp hacked, data theft of million costumers, substantial impact on share price, entire management sacked**<br>• **2014: European Central Bank hacked to get data of 20,000 customer** |
| **State sponsered** | • 2008 Russia-Georgia War: Russian hacker hit Georgian websites<br>• 2010 Stuxnet: computerworm designed to attack industrial plants, Iranian nuclear plants attacked in 2010, Russian nuclear plants attacked in 2013<br>• 2010 Pakistanian 'Cyber Army' attacks India´s Central Bureau of Investigation<br>• 2013 Snowden revelation<br>• 2014 Australian Foreign Minister targeted by suspected state-sponsored phone hackers |
| **Hacktivism** | • 1997 Worchester Airport: hacker shut down air/ground traffic communication sytems for 6 hours<br>• 2010 Visa & MasterCard websites attacked by Anonymous' hacker<br>• 2011 Goldman Sachs re Occupy Wall Street<br>• 2013 Hacker accessed the Guardians & Associated PressTwitter accounts<br>• 2013 Anonymous' threat to shut Goldman Sachs' social media pages |

# Targets, issues, reactions

| Targets | Issues | Reactions |
|---|---|---|
| **States** | • State communication systems corrupted<br>• Critical infrastructures<br>• Cyberwar attacks by other states | • Investment in system security<br>• Regulation; explanation, education<br>• NATO to amend Art. 5 NATO Treaty to include cyber attacks |
| **Companies** | • Loss of costumer data / IP<br>• Reputational issues / costumer trust<br>• Exposure to liability in relation to costumers and shareholdes<br>• Management liability | • Fortification of systems; data classification<br>• Cyber response / PR strategy<br>• Contractual protection from outsourcing providers; liability limitation<br>• Establish internal structures, external audits |
| **Individuals** | • Violation of data privacy<br>• Damages from criminal actions | • Choose trusted providers; security software updates<br>• Keep online banking safe; secure passwords |

# Risk perception - USA

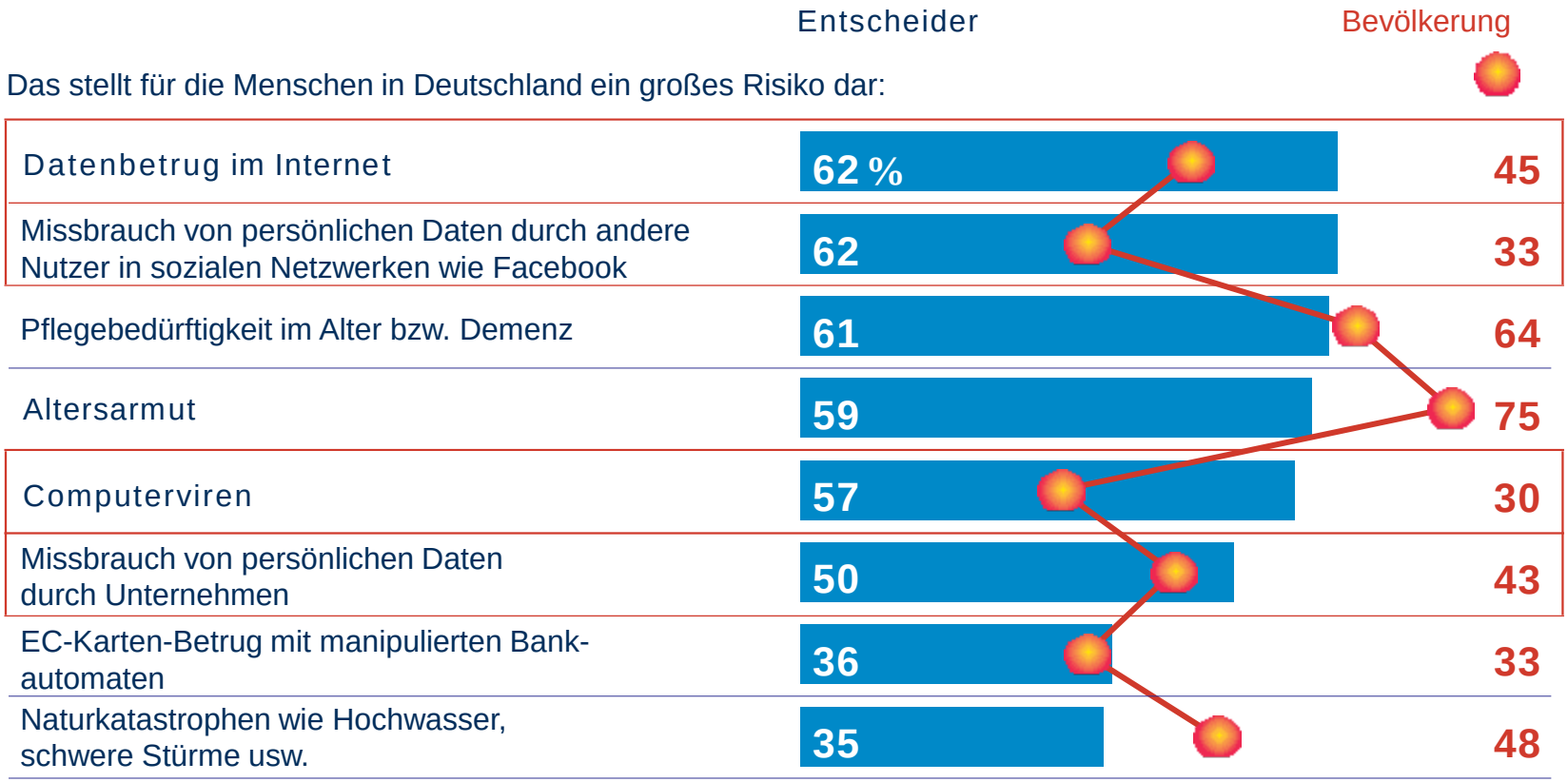
## Perception of cyberwarfare in US defence and society




Source: Defence news leadership poll, underwritten by United Technologies

# Risk perception - Germany

## Risk perception of German deciders (politics / industry) vs. General public




Source: Cyber Security Report 2013, Deutsche Telekom/T-Systems

# Political awareness

## USA - Early awareness of the threat from cyberspace since the early 2000s

**National Academy of Sciences, Computer Sciences and Telecommunications Board, 1990**

*"We are at risk. Increasingly, America depends on computers. […] Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."*

**The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998**

*"Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."*

*"It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."*

**Congress discussion in 2003/2005**

"Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress"

**SEC regulation 2011**

Cybersecurity Disclosure Guidelines

# Political awareness

## USA – Regulatory activities

**First Legislative attempts 2012**

‘Cyber Intelligence Sharing and Protection Act’ in 2012 which failed in Senate due to data privacy concerns, re-introduced in Senate in 2014

**US Executive Order 2013**

Strengthen cyber security through information sharing and developing a set of voluntary standards

**Cybersecurity Framework 2014 + Cyber Community C³**

National Institute of Standards and Technology (NIST) developed a set of voluntary cybersecurity standards, guidelines, and practices for critical infrastructures (Cybersecurity Framework 2014). Department of Homeland Security (DHS) has partnered with the critical infrastructure community to establish a voluntary program to encourage use of the Framework to strengthen critical infrastructure cybersecurity (Cyber Community C³).

**Draft Deter Cyber Theft Act 2014**

Bill proposed in Senate, currently in committee, that would empower the Treasury Department to impose sanctions on individuals and companies who benefit from cyber theft of IP.

# Political awareness

## Germany – Political awareness started later

**German Minister of Interior, Otto Schilly, 2000**

‘Security and IT are inseparable’

**UN World Summit on the Information Society 2003**

Germany sending ‘only’ Minister for Development Aid

**German Minster of Interior, Otto Schilly, 2005**

Publishes ‘National Plan for the Protection of IT Infrastructure‘

**BSI-Gesetz 2008**

Established with a focus on IT security for Federal institutions

# Political awareness

## Germany – Regulatory activities

### (Sector)-specific regulation

- **Data protection:** Reporting obligation in cases of a loss of sensitive personal data ( § 42 a German Data Protection Act introduced in 2009)
- **Financial Services:** Mandatory IT security plans and measures. The Banking Act refers to specific IT standards developed by the BSI (2009/2012: MaRisk, Grundschutzkatalog). April 2014: BaFin expects reporting if significant damage or critical IT security incidents have occurred due to the Heartbleed Bug or similar security flaws.
- **Energy:** Mandatory appropriate IT security measures (§ 11 para 1 a Energy Industry Law introduced 2011). German Federal Network Agency (BNetzA) has to develop an IT security catalogue for energy network operators, (draft published, final version expected in December 2014). Yearly reporting.
- **Telco Provider**: Mandatory state-of-the-art IT security measures to protect personal data and confidential information (§ 109 para 1 TKG). Reporting obligation for significant security incidents to BNetzA.

### German government presents draft German IT Security Act (Feb 2013)

First draft presented 2013. End of August 2014, updated draft, taking into account certain criticisms from the industry. German Government prioritises the adoption of the Act as part of the ‘Digital Agenda’. Likely to to be adopted end of 2014.

# Political awareness

**EU**

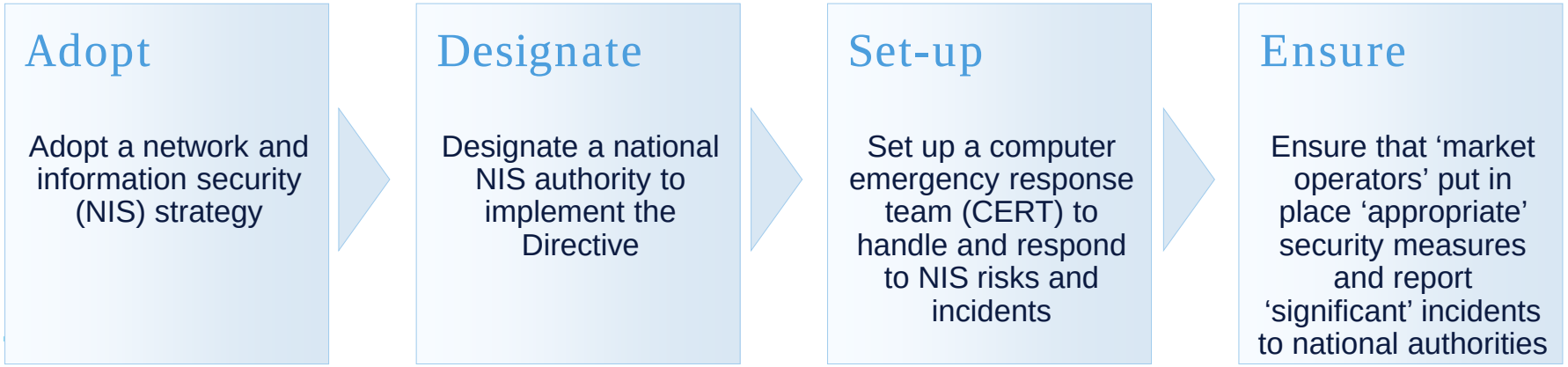
**European Convention on Cybercrime 2004**

First multinational agreement relating to cybercrime

**EU establishes European Network and Information Security Agency (ENISA), 2004**

**European Commission presents draft Cybersecurity Directive (Feb 2013)**

Draft is now under consideration by the EU Council and Parliament. EU Parliament's IMCO committee (Internal Market and Consumer) voted on various amendments in January 2014. Approved by full Parliament on 13 March. Final negotiations between Council, Parliament and Commission are likely to take place in late 2014.



# International activities

## OECD

**2002 ‘OECD Guidelines for the Security of Information System and Networks‘**

Important role for ‘culture of security‘ and great influence on ISO 27001 standard

OECD is currently revising its ‘2002 Guidelines‘ and will start reviewing its ‘Recommendation on the Protection of Critical Information Infrastructures‘ in Dec 2014

## UN

**Since 1998, the UN publishes annual reports on IT security.**

Report 2012/13 by the ‘Groups of Governmental Experts‘ (GEE) acknowledges the full aplicability of international law to state behaviour in cyberspace (by recommending to anchor ICT security in the existing framework of international law) and recommends confidence-building measures.

A new GGE is no westablished that had its first meeting in New York in July 2014, and elected Brazil as the Chair. The Group will have three more meetings and issue its report in 2015.

## NATO

**Ammendment of Art. 5 NATO Treaty to include cyber war**

# Topics of regulation

| Topic | EU | Germany | US |
|---|---|---|---|
| **Critical Infrastructure** | Operators of critical infrastructure that are essential for the maintenance of vital economic and social activities in the fields of energy, transport, financial institutions, healthcare<br>⇨ Key internet enablers still under discussion | 2 more sectors than EU (water + food) and adding telco + internet services providers to certain extent | Critical infrastructure: systems and assets of which the harm or destruction would 'have a debilitating impact on security, national economy security, national public health or safety.' |
| **Security standards** | Mandatory appropriate state-of-the-art measures. Specification of IT standards by industry associations. | Industry specific IT standards (almost implemented for energy sector) which can be submitted for approval to BSI | Cyber security framework developed. Implementation by companies on a voluntary basis. |

# Topics of regulation

| Topic | EU | Germany | US |
|---|---|---|---|
| **Reporting obligations** | Report significant cyber security incidents to national authorities having affected core services. | In addition to EU, German draft act includes also incidents that may affect the core services (but in this case, anonymized notification possible). | Not part of executive order |
| **Audit requirements** | no regular obligation | external audits on 2 year basis | Not part of executive order |

# Topics of regulation

| Topic | EU | Germany | US |
|---|---|---|---|
| **Obligations for telcos and ISPs** | no additional obligations to existing security and incident reporting requirements under the EU telecommunications regulatory regime | Telcos: Obligations to inform clients about 'easy to use' anti-virus software in case of attack, obligations re IT security standards extended to any form of unauthorized access and reporting about any IT incident that can lead to disruption or unauthorized access of systems. ISPs: mandatory appropriate state-of-the-art measures. | Not part of executive order |

# Thank you for listening!