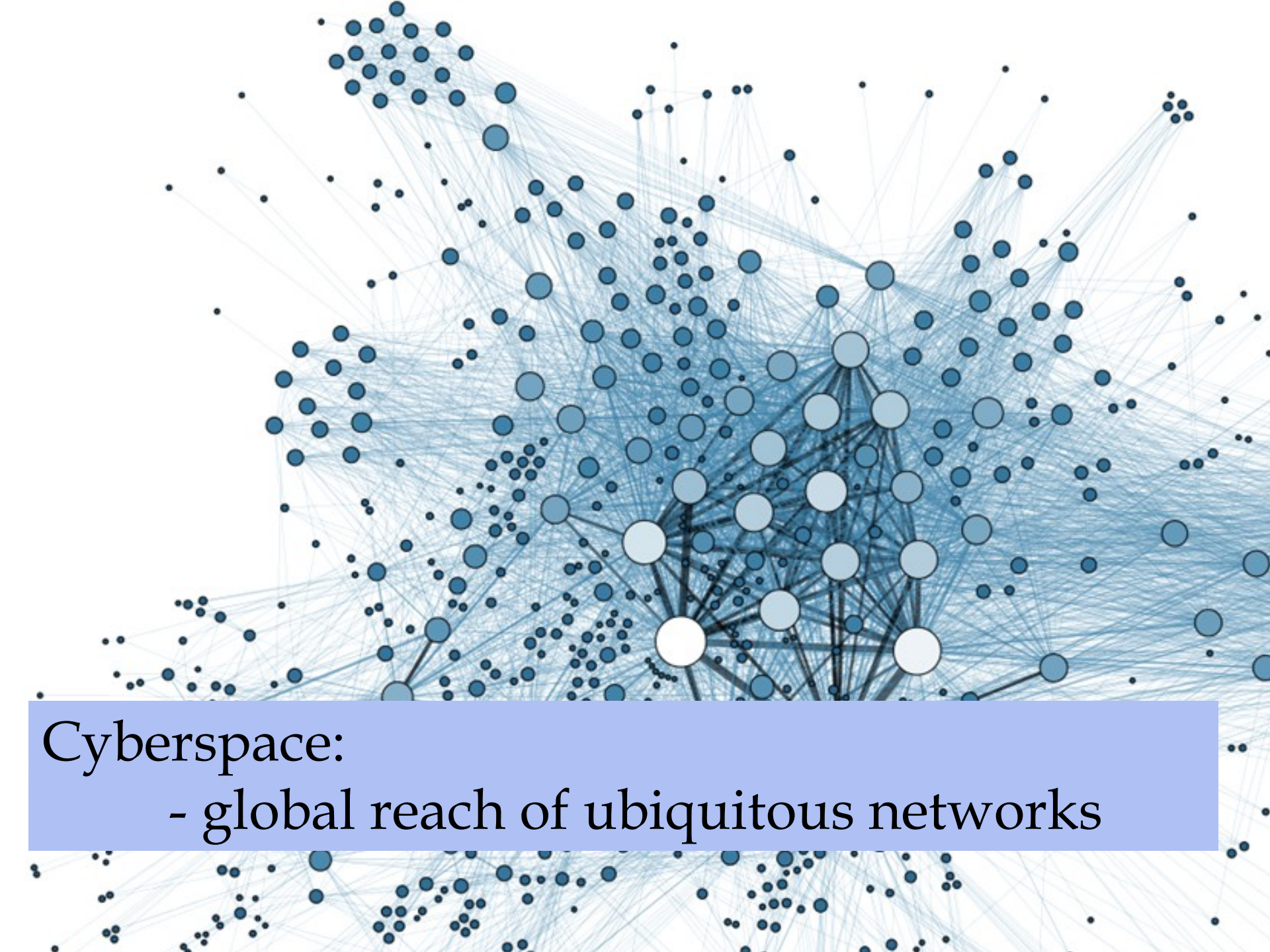


THE BITS TO KNOW ABOUT CYBERSECURITY

~~(Even Especially if you are a lawyer)~~

Anca Plovie



Cyberspace:
- global reach of ubiquitous networks



Cyberspace:
- fast connection speeds



Cyberspace:

- lack of largely accepted norms and principles

CYBERSECURITY?



measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster Dictionary)



CYBERSECURITY

aims to

attain and maintain

confidentiality



CYBERSECURITY

aims to

attain and maintain

integrity



CYBERSECURITY

aims to
attain and maintain

availability

CYBERSECURITY

aims to

attain and maintain

confidentiality

integrity

and

availability

CYBERSECURITY

works on

global threats

under

legal

uncertainty





Cybersecurity has to contend with an Internet architecture that makes it virtually **impossible** to attribute an attack to an actor



Traditional approach to security was to build and stand on a wall protecting the most valuable enterprise assets.

NEW SPACE, NEW PLAY RULES

- THE “INTERNET OF THINGS” AND THE “BIG DATA” WORLD

- Threats are rapidly multiplying, originating across enterprise walls and taking new forms
 - persistent probing,
 - malicious codes,
 - software vulnerability exploits,
 - denial of service attacks, etc

⇒ enforcing a perimeter and reacting to events no longer sufficient

⇒ harder to identify and
defend against new threats

-Organizations need to **analyze** and **correlate** all available streaming and historical **data** to continuously **identify threats** - and **act in real time** to **protect** all physical and cyber assets.

International New York Times

SECTION'S

SUBSCRIBE LOG IN

BUSINESS DAY

Millions of Anthem Customers Targeted in Cyberattack

Login | Registrierung

SPIEGEL ONLINE NETZWELT

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Reise | Auto | Stil

Nachrichten > Netzwelt > Netzpolitik > Computersicherheit > E-Mail-Passwörter gestohlen: 18 Millionen Datensätze

Cyberkriminalität: Fahnder entdecken 18 Millionen gestohlene E-Mail-Passwörter

Von Michael Fröhlingdorf, Hubert Gude und Jörg Schindler

the guardian

Winner of the Pulitzer prize

technology lifestyle fashion environment tech money travel

Company loses \$17m in email scam

technology

The Washington Post

Tech

Uber says database containing names and drivers was breached

By Associated Press February 27

NEW YORK — Uber says a database containing the names and drivers

Cartes SIM piratées : « une guerre froide au sein de l'Union européenne »

LE MONDE | 23.02.2015 à 19h41 • Mis à jour le 24.02.2015 à 08h17 |

Propos recueillis par Martin Untersinger

Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

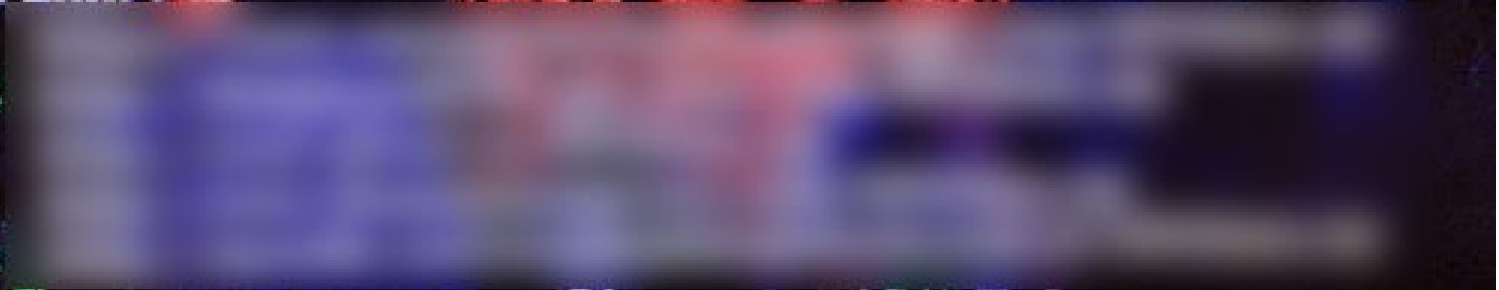
We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the **24th, 11:00 PM(GMT)**.

Data Link :



SWISS LEAKS

www.icij.org/project/swiss-leaks/explore-swiss-leaks-data

+ SWISS LEAKS COUNTRIES PEOPLE STORIES ABOUT



SWISS LEAKS

The leaked HSBC files offer a rare glimpse inside one of the world's most private banking systems.

More than \$100 billion from 106,000 clients of 203 countries.

Explore [countries](#), [people](#) and [stories](#).

Most client & account data from 1988-2007; amounts from 2006-07. [Learn more.](#)

swiss-leaks/

SEND A TIP RECEIVE NEWS DONATE SHARE

ADOBE BREACH

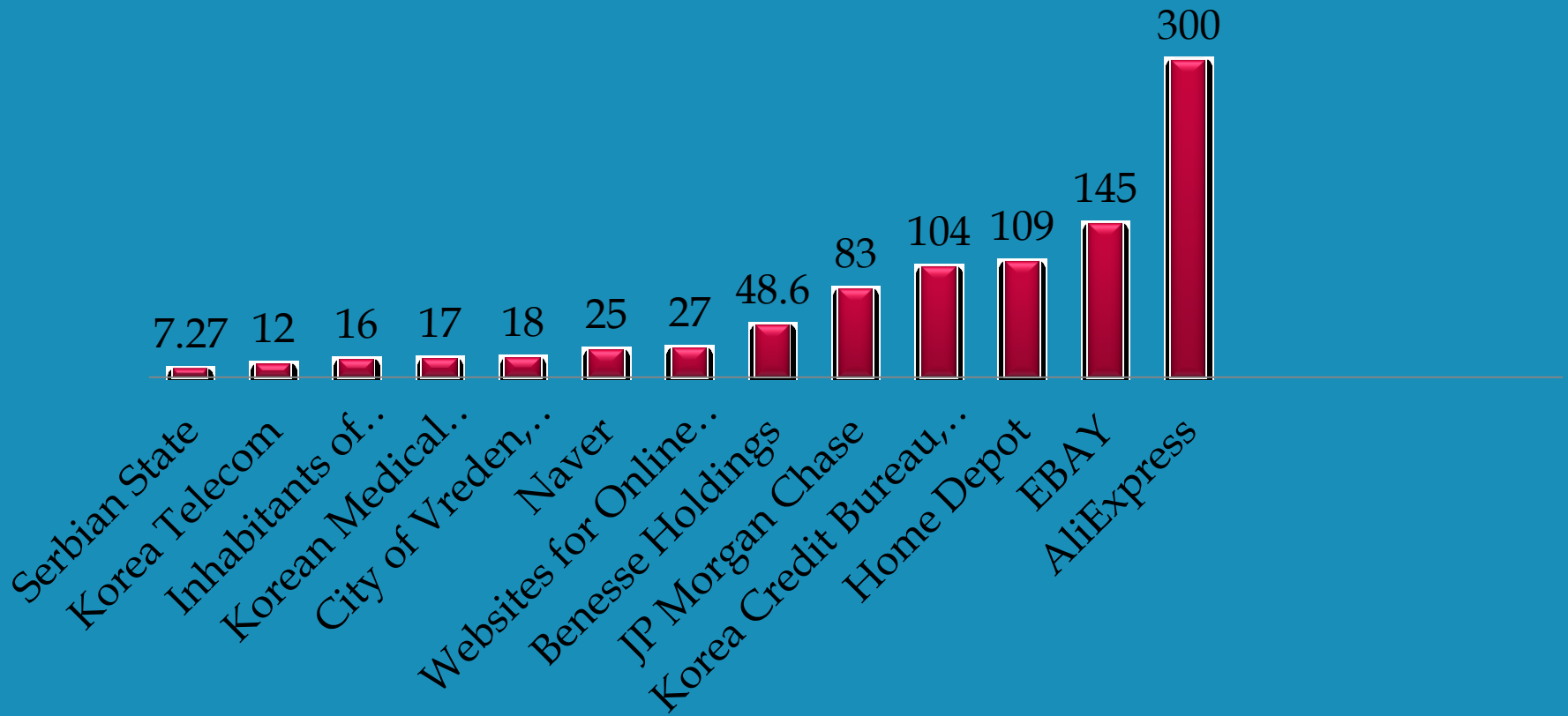
HACKERS RECENTLY LEAKED **153 MILLION** ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS. ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER	PASSWORD	HINT
4e18acc1ab27a2d6		WEATHER VANE SWORD
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1
8bab6299e06eb6d		DUH
8bab6299e06eb6d	a0a2876eb1ea1fca	
8bab6299e06eb6d	85e9da81a8a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86da6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b	e0dec1e6ab797397	SEXY EARLOBES
a1f9b2b6299e7a2b	617ab0277727ad85	BEST TOS EPISODE
3973867adb0b8af7	617ab0277727ad85	SUGARLAND
1ab29ae86da6e5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279cadeb44	9dca1d79d4dec6d5	
38a7c9279cadeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279cadeb44		PURLAINED
a8ae5745a717af7a	9dca1d79d4dec6d5	FAV. WATER-3 POKEMON

THE GREATEST CROSSWORD PUZZLE
IN THE HISTORY OF THE WORLD

TOP BREACHES OF 2014

Million records exposed in data breaches



Source: 2014 Breach Level Index Gemalto NV, 2015, www.gemalto.com

MOTIVATION



Financial gains

W. D. MIDDLEBROOK.

MACHINE FOR MAKING WIRE PAPER CLIPS.

(Application filed Apr. 27, 1899.)

(No Model.)

2 Sheets—Sheet 2.

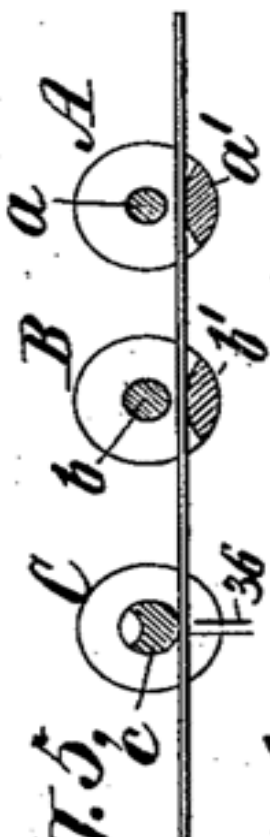
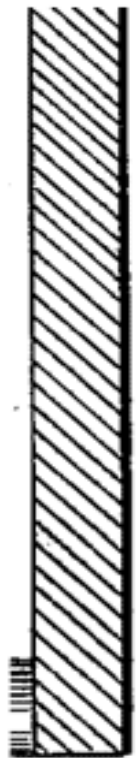


Fig. 5.

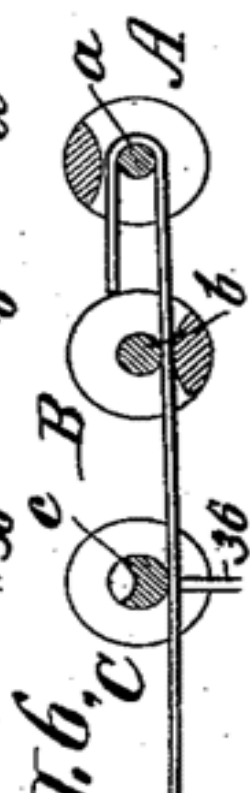


Fig. 6.

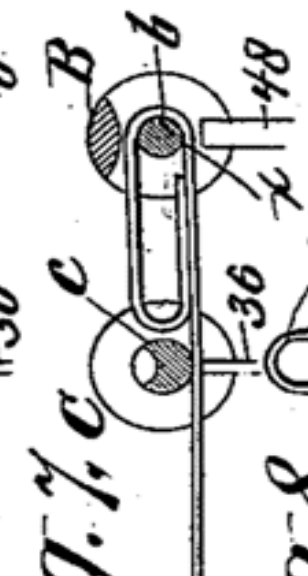


Fig. 7.

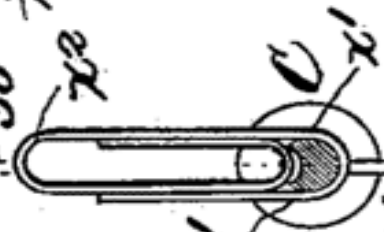


Fig. 8.

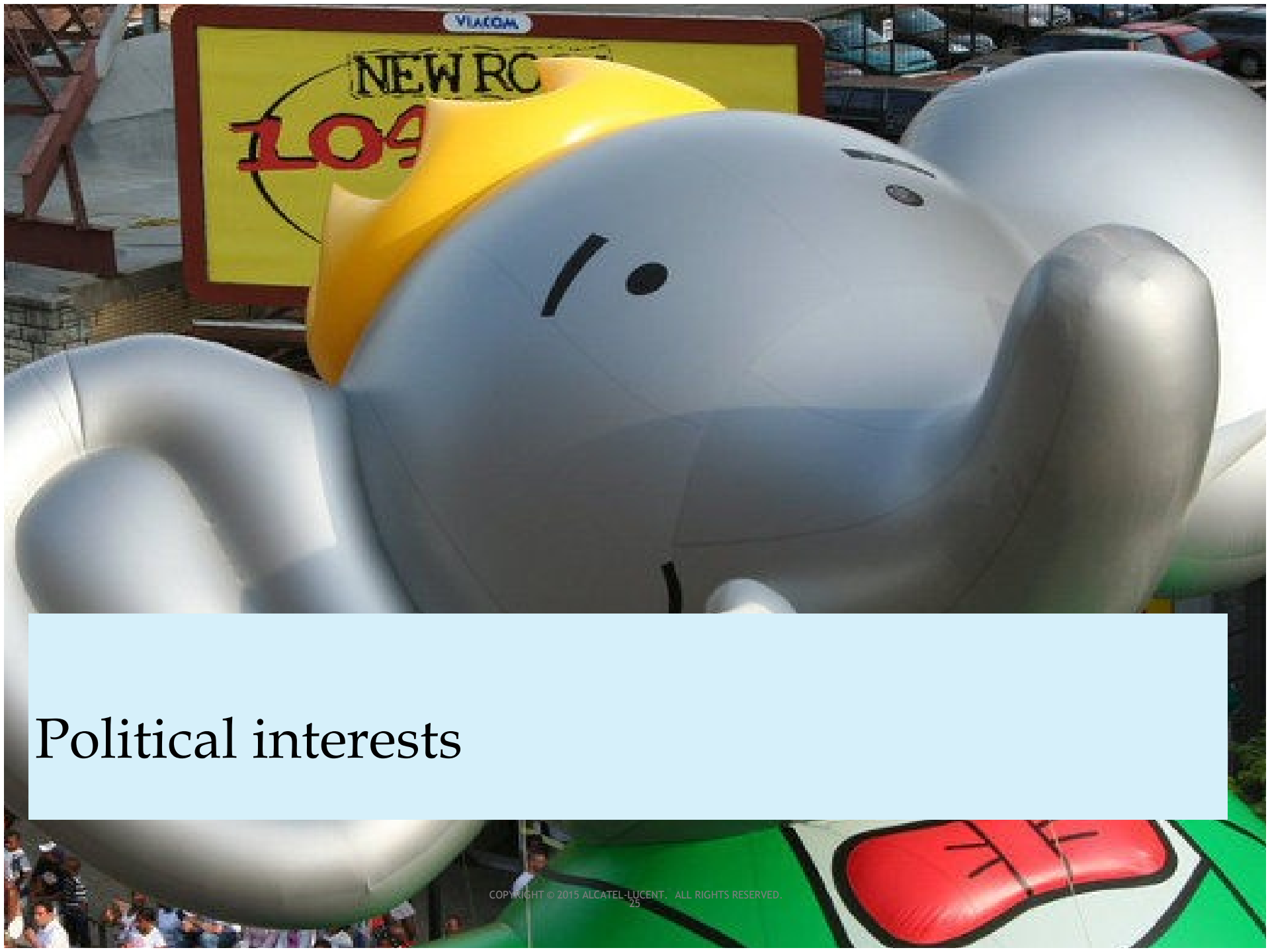
Corporate interests

INVENTOR

BY Wm D. Middlebrook

Baldwin, Davidson & Wight

ATTORNEYS



Political interests



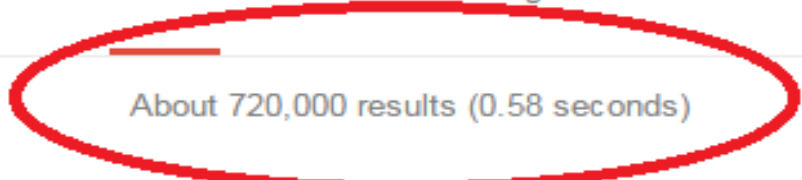
Hacktivism



Narcissism



Revenge and punishment



About 720,000 results (0.58 seconds)

For fun...

Remote Computer Software - screenconnect.com

Ad www.screenconnect.com/

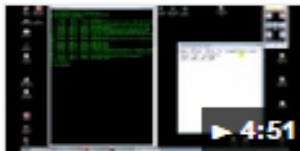
Support and Access Remote Computers - Start Your Free Trial Now

How to hack remote computer using IP Address | HackTweaks

www.hacktweaks.com/how-to-hack-remote-computer-using-ip-address/

Again this is IP based and this is possible only when your friend's computer is online. If it is off or not connected to internet then remote IP hacking is totally ...

How to remotely Hacking into Another Computer Without ...



www.youtube.com/watch?v=JUFdFkas-tA

Oct 31, 2012 - Uploaded by W4RCRYzeeH4CK3R

Hello everyone, in this video i'll be teaching you how to Trace someone and a remote access trick that is ...

3 Ways to Hack a Computer - wikiHow

www.wikihow.com > ... > Internet > Internet Security

Hacking a computer is a useful and, at times, an important skill to pick up. Below are ... Three Methods:Hacking Log-InsRemote HacksHacking WiFi. Hacking a ...





Find professional hackers for hire

People need professional hackers for hire. So, we connect people who need professional hackers to professional hackers for hire around the world. Safe, fast and secure Learn how it works.

[Browse](#) OR

[Start Project](#)

WHY WOULD THEY ATTACK US?





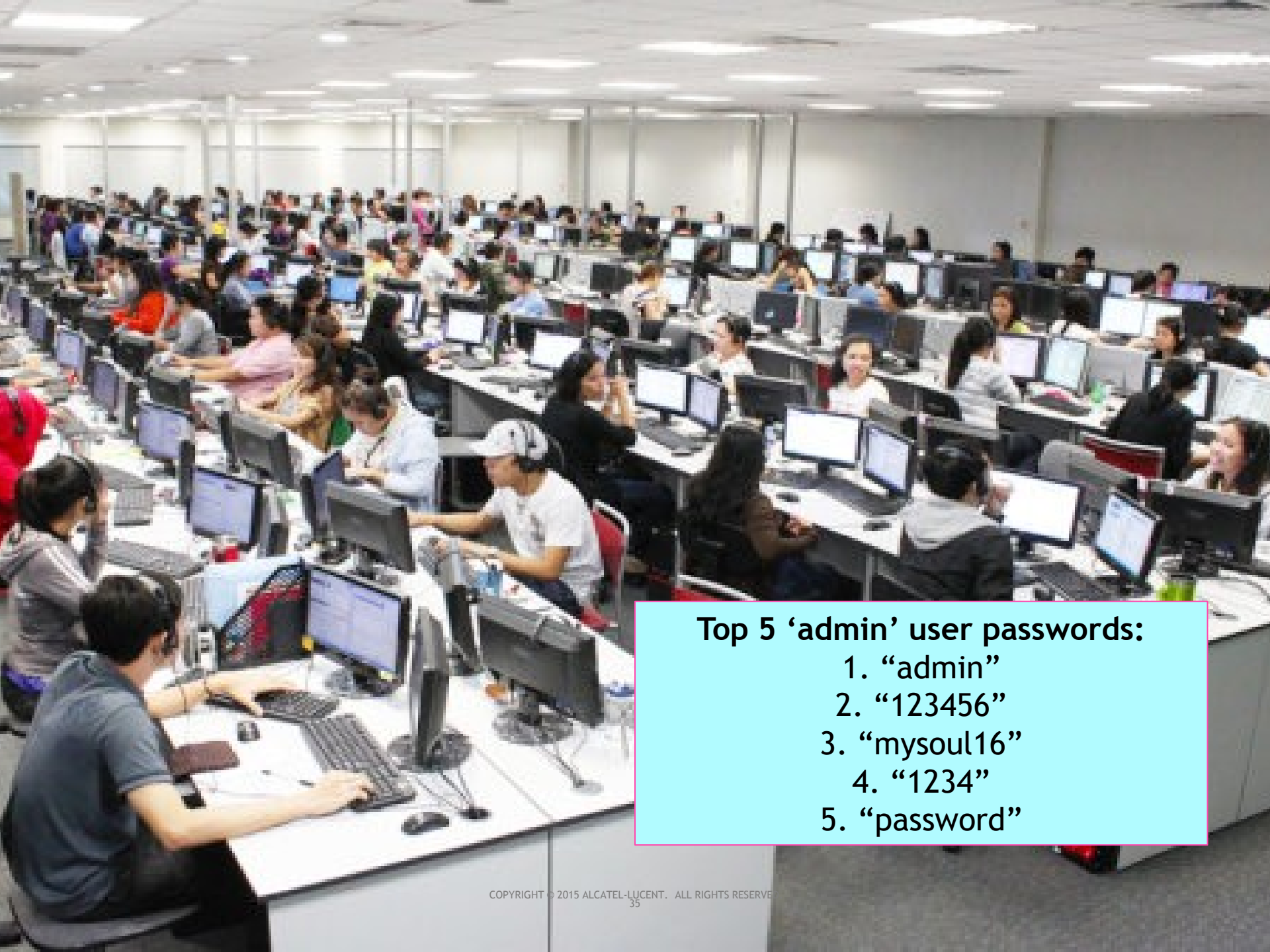
- Business plans, including merger or acquisition strategies, bids, etc.
- Trading algorithms
- Contracts with customers, suppliers, distributors, joint venture partners, etc.
- Employee log-in credentials
- Information about company facilities, including plant and equipment designs, maps, and future plans
- Product designs
- Information about key business processes
- Source code
- Lists of employees, customers, contractors, and suppliers
- Client data

CYBERSECURITY RISKS

INTERNAL THREATS (INCLUDING AUTHORIZED THIRD PARTIES)

“The majority of our analysis of data breach investigations -- 76% -- revealed that the third party responsible for system support, development and/or maintenance introduced the security deficiencies exploited by attackers.”

- Trustware Global Security Report



Top 5 'admin' user passwords:

1. "admin"
2. "123456"
3. "mysoul16"
4. "1234"
5. "password"

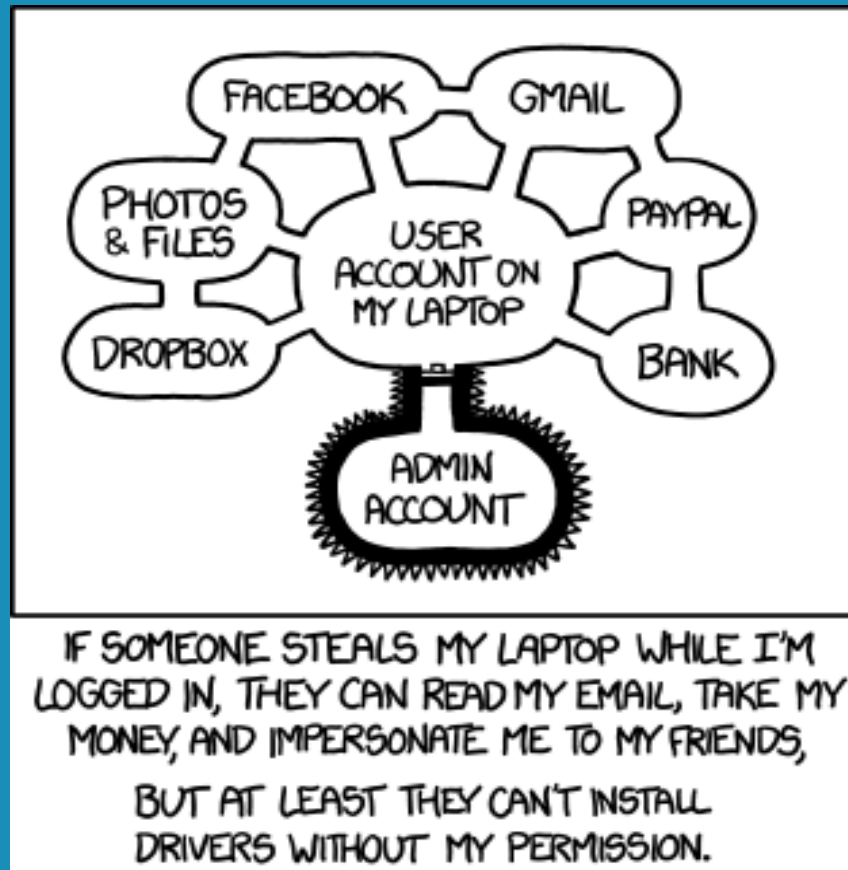


PASSWORD FATIGUE

Top 25 most hacked passwords:

1. 123456 (*Unchanged*)
2. password (*Unchanged*)
3. 12345 (*Up 17*)
4. 12345678 (*Down 1*)
5. qwerty (*Down 1*)
6. 123456789 (*Unchanged*)
7. 1234 (*Up 9*)
8. baseball (*New*)
9. dragon (*New*)
10. football (*New*)
11. 1234567 (*Down 4*)
12. monkey (*Up 5*)
13. letmein (*Up 1*)
14. abc123 (*Down 9*)
15. 111111 (*Down 8*)
16. mustang (*New*)
17. access (*New*)
18. Shadow (*Unchanged*)
19. master (*New*)
20. michael (*New*)
21. superman (*New*)
22. 696969 (*New*)
23. 123123 (*Down 12*)
24. batman (*New*)
25. trustno1 (*Down 1*)

PASSWORD RE-USE



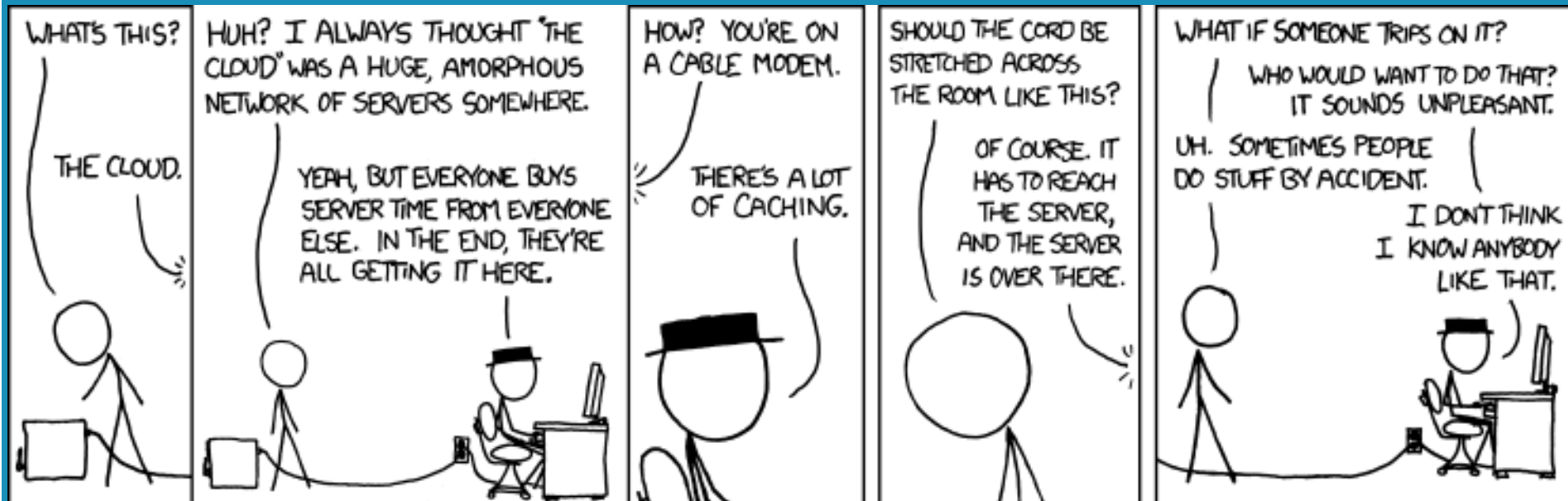
SOCIAL ENGINEERING



key factor in 92% of industrial espionage attacks

CLOUD SECURITY

“a super computer in your pocket”



Vendor and Supply chain

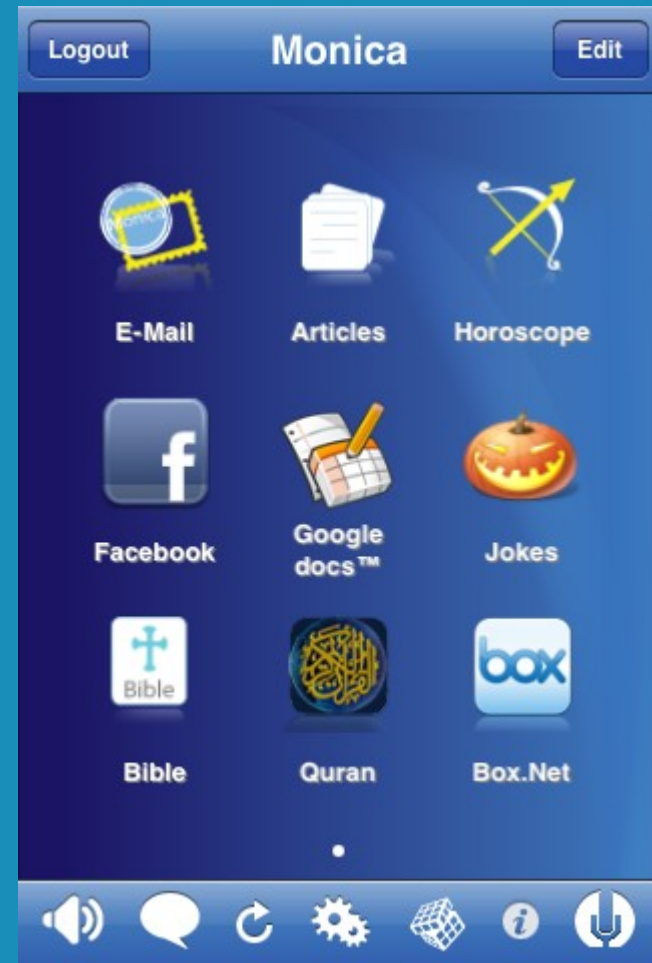


**BRING
YOUR OWN
DEVICE**
(or better: PLEASE DON'T!)



MOBILE APPLICATIONS

“There’s an app for that!”



USE OF WI-FI



Londoners agree to give up first-born child in exchange for free internet

Experiment with 'Herod clause' exposed lax security with open wi-fi networks

Lizzie Dearden

Tuesday, 30 September 2014

Londoners agreed to give away their first-born child in exchange for free wi-fi in an experiment exposing an "utter disregard" for security by smartphone users.

REGULATORY CHALLENGES

SETTING THE STAGE:

- 1992 – **OECD**: “Guidelines for the Security of Information Systems”, revised in 2002 & December 2014
- **2001 – Council of Europe – Convention on Cybercrime (“Budapest Convention”)**
- 2008 – **OECD**: “Recommendation on the Protection of Critical Information Infrastructures”, revised in 2013
- **UN through ITU (193 member states):**
 - 2010 Global Security Agenda
 - 2011 ITU National Cybersecurity Guide
 - 2014 Global Cyber Security Index

CYBERSECURITY LEGISLATION

Typically covers five main areas:

- Legal Measures
- Technical Measures
- Organizational Measures
- Capacity Building
- National and International Cooperation

EUROPEAN UNION

EU Commission February 7, 2013:

1. EU Cybersecurity Strategy
2. Draft EU Network and Information Security (NIS) Directive

DRAFT NIS DIRECTIVE AIMS:

- achieve European cyber resilience
- drastically reduce European cybercrime
- develop **common** European cyber defense **policies and resources**
- establish a coherent European cyberspace policy and promote core EU values
- EU competent authorities to cooperate, share information, and coordinate responses
- **18 months implementation period** through national laws (if adopted)

DRAFT NIS DIRECTIVE KEY POINTS

- companies in “critical” sectors to adopt strict network security standards and report “significant” cybersecurity incidents
- broad section of industry sectors, including “non-essential” services (e.g. YouTube)
- no clear distinction between targeted cybersecurity incidents and other types of breaches
- **Red Flag:** breach reporting requirements are **not harmonized** with existing and anticipated breach reporting requirements under the **EU E-Privacy Directive and the proposed EU General Data Protection Regulation!**

DRAFT NIS DIRECTIVE APPROACH IS PRESCRIPTIVE:

- Market operators are to improve cybersecurity frameworks
- Tougher sanctions
- Scrutiny from a cybersecurity watchdog

UNITED STATES

February 12, 2013, Executive Order 13636

“to enhance the cybersecurity of critical infrastructure in the US”

UNITED STATES

February 12, 2014, National Institute of Standards and Technology:

Framework for Improving Critical Infrastructure Cybersecurity

(“NIST Framework”)

- **voluntary**
- based on existing standards, guidelines, and practices
- provides guidance for reducing cybersecurity risk
- for organizations within **critical infrastructure** sectors

USA - THE OTHER ACTORS ON THE SCENE

- Federal Trade Commission
- Securities Exchange Commission
- Department of Justice
- US Congress
- State Attorneys General

ASIA PACIFIC POLICY DEVELOPMENTS

Legislation introduced but not yet adopted:

- India
- Japan
- Singapore
- Thailand

ASIA PACIFIC POLICY DEVELOPMENTS

PR China

- Intention to legislate on cybersecurity announced in March 2015 but no draft is available yet.
- Cybersecurity implications of the draft antiterrorism law and new banking rules: **technology suppliers required to hand over sensitive information such as encryption keys or source code to Chinese regulators.**

NEWEST REGULATORY CHALLENGE

Data sovereignty and data localization

- Brazil
- Russia

CONSEQUENCES OF A DATA BREACH

COST ISSUES

Average total organizational cost of a data breach (in USD):

- US:	\$5,850,000
- Germany:	\$4,740,000
- France:	\$4,190,000
- UK:	\$3,680,000
- Italy:	\$2,690,000

(Source: Ponemon Institute, 2014)

TYPES OF COSTS ASSOCIATED WITH A DATA BREACH

- Business continuity costs
- Investigation costs
- Contractual liability to business partners and to customers
- Notification costs
- Credit-monitoring services
- Identity restoration services
- Identity-theft insurance
- Regulatory costs
- Legal assistance
- Litigation costs

Some estimates predict that between

\$9 and \$21 trillion of global economic value creation

could be at risk if companies and governments are unable to successfully combat cyber threats.



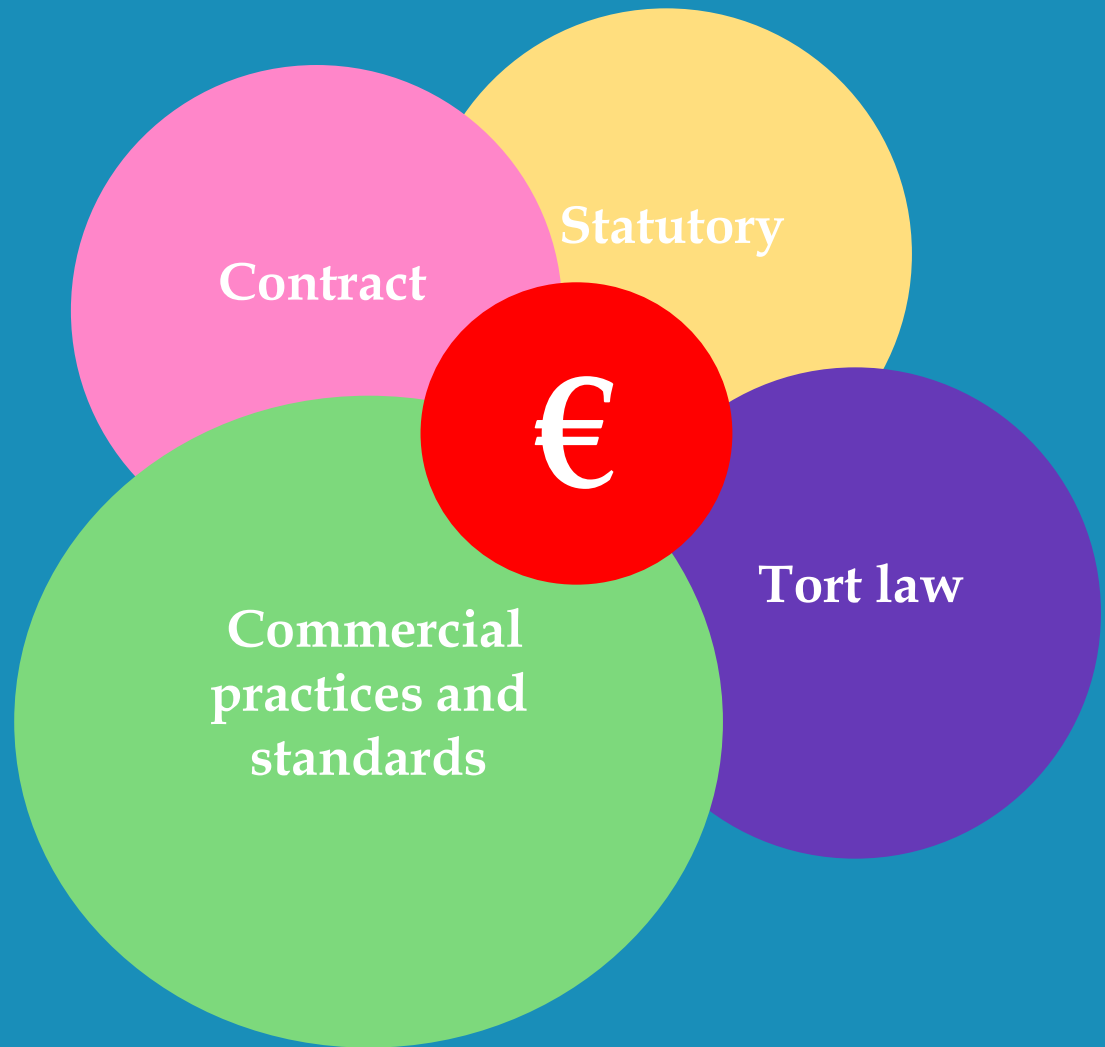
OTHER CONSEQUENCES

- Competitive disadvantage
- Loss of business
- Loss of business
- Reputational issues
- Loss containment



Red Flags in Contracts

Sources of liability



PRIVACY AND CYBERSECURITY - SOME RED FLAGS IN CONTRACTS

Compliance with Privacy Laws

Define term “Privacy Laws” based on:

- data subjects
- type of personal data
- extra-territorial application of laws
- specific sectoral laws applicable

PRIVACY AND CYBERSECURITY – SOME RED FLAGS IN CONTRACTS

Obligation to protect data

Determining factors:

- **Where** personal data will be processed
- **Who** will process personal data
- **What** personal data will be processed
- **How** personal data will be processed

Security obligations

- **Categories** of data
- **Location** of data
- **Measures** taken to protect data while at rest or in motion
- Compliance to security **standards**

Monitoring and audit rights for the customer

“More tears are shed over answered prayers than unanswered ones.”

- Mother Teresa

Notification and cooperation obligations

- required by law or not
- deadlines for notifications
- co-operation post breach

Duty to appropriately manage or eliminate security/cyber risks

Know your definitions:

Risk vs. vulnerability vs. event vs. threat vs. incident

- Full elimination of risk is often undesirable

Liability of Board and Management

- Intense focus by regulators
- Personal liability may be engaged
- Need to:
 - get the **right team** in place
 - **prepare** proactively
 - know what is **valuable** and needs protection
 - allocate **time** at board meetings

Cyber Insurance:

- 32% of companies have it**
- essentials: coverage, exclusions, retentions/franchises, prerequisites, annual review**



IS IT REALLY THAT COMPLICATED TO PREPARE?

Proactive incident response planning

- inventory databases with sensitive personal information and other critical data
- understand how personal information flows through the organization
- conduct ongoing risk assessments for internal and external risk to the data
- involve the Board
- inventory of third party relationships
- inventory of compliance requirements
- develop a breach response procedure
- cyber insurance

Minimal technical measures

- Restricting user installation of applications (“whitelisting” as opposed to “blacklisting”)
- Ensuring that the operating system is patched with current updates
- Ensuring that software applications have current updates
- Restricting administrative privileges
- Boundary firewalls and internet gateways

>< PRIVACY?

Be cybersafe!

MY RESOURCES:

Cyber Security Skills – A Guide for Businesses:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/385009/bis-14-1277-cyber-security-balancing-risk-and-reward-with-confidence-guidance-for-non-executive-directors.pdf

Safe checking if my details been compromised in any recent data breaches:

<https://haveibeenpwned.com/>

Chronology of Data Breaches from 2005 to present:

<https://www.privacyrights.org/data-breach>

First 24 hours after breach checklist:

<http://www.experian.com/data-breach/24-hour-checklist.html>

Various CISO checklists:

<http://www.cisopatform.com/profiles/blog/list?tag=Checklists>

MY RESOURCES:

Cybercrime Convention (Budapest Convention)

<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

Glossaries of Security Terms:

<http://www.sans.org/security-resources/glossary-of-terms/>

<http://niccs.us-cert.gov/glossary>

Examples of data breach procedures:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

https://www.exeter.ac.uk/media/level1/academicserviceswebsite/it/recordsmanagement/service/20130322_Data_Breach_Procedure_1.0.pdf

https://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.pdf

Articles and Papers:

The rule of law on the Internet and in the wider digital world:

<https://wcd.coe.int/ViewDoc.jsp?id=2268589>

Nice trivia:

What hacking reveals about a person:

<http://pando.com/2013/10/26/i-challenged-hackers-to-investigate-me-and-what-they-found-out-is-chilling/>

Consequences of data breaches:

<http://thinkprogress.org/economy/2015/01/12/3610424/charlize-theron-pay-gap/>

Photo attribution:

Image of the Internet: <http://bitcast-a.bitgravity.com/blyon/opte/maps/static/1105841711.LGL.2D.1024x1024.png>, via Wikipedia

How to Live in Peace: <http://www.wikihow.com/Image:How-to-Live-in-Peace---10.jpg>, Wikiphoto

The Great Wall of China: By Severin Stalder

http://commons.wikimedia.org/wiki/File%3AThe_Great_Wall_of_China_at_Jinshanling.jpg (Own work) [CC BY-SA 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)], via Wikimedia Commons from Wikimedia Commons

Carton of eggs: By Gisela Francisco (Own work) [CC BY 3.0 (<http://creativecommons.org/licenses/by/3.0/>)], via Wikimedia Commons

Dubai - 7 Star luxury: by Chris Hopkins, <https://flic.kr/p/dLR13b>

Babar: <http://www.aheliotech.com/blog/beware-of-babar-the-spyware-created-by-the-french-secret-service/>

Anonymous: By Vincent Diamante, http://commons.wikimedia.org/wiki/File%3AAnonymous_at_Scientology_in_Los_Angeles.jpg, [CC BY-SA 2.0 (<http://creativecommons.org/licenses/by-sa/2.0/>)], via Wikimedia Commons from Wikimedia Commons

Butterfly: By Ezhuttukari (Own work) [CC BY-SA 3.0 (<http://creativecommons.org/licenses/by-sa/3.0/>)], via Wikimedia Commons

"Vengeance populaire après la prise de la Bastille-Landon-IMG 2365" - Photograph by Rama, Wikimedia Commons, Cc-by-sa-2.0-fr. Licensed under CC BY-SA 2.0 fr via Wikimedia Commons -

http://commons.wikimedia.org/wiki/File:Vengeance_populaire_apr%C3%A8s_la_prise_de_la_Bastille-Landon-IMG_2365.JPG#/media/File:Vengeance_populaire_apr%C3%A8s_la_prise_de_la_Bastille-Landon-IMG_2365.JPG

Head in the sand: By tropical.pete, <https://flic.kr/p/5q67Vu>, [<https://creativecommons.org/licenses/by-sa/2.0/>]

Ostrich: by Ignacio García, https://www.flickr.com/photos/bichologo_errante/7881219424/in/photostream/, via <http://free-images.gatag.net/en/tag/ostrich>

Chain close-up: By Toni Lozano, <http://www.flickr.com/photos/quiero-un-pantano/176909201>, via Wikimedia Commons

All cartoons from: <https://xkcd.com/>

Alcatel·Lucent 