Introduction to Information Security in Healthcare for BelRai Information Security Administrators

J.G.E. (Hans) Wierts
Informatieveiligheidsconsulent eHealth-platform
Sint Pieterssteenweg 375
1040 Brussel
E: hans.wierts@ehealth.fgov.be
W: https://www.ehealth.fgov.be
T: +32 2 74 18 394
F: +32 2 74 18 300

Goals of the eHealth-platform

- What?
  - Optimize the quality and continuity of healthcare.
  - Optimize patient safety
  - Simplify administrative formalities for all healthcare actors.
  - Thorough healthcare policies.
- How?
  - A well organized set of mutual electronic services and exchange of information between all healthcare actors.
  - Several guaranties regarding information security, protection of privacy and professional secrecy.

High level Flow

Impossible d'afficher l'image.

Base services

- To raise information security levels and protection of privacy.
  - User and Access Management (UAM)
  - End To End Encryption (ETEE)
  - Coding and anonymisation.
  - eHealth Box
  - Logging
- To support evidential / probative value
  - Time Stamping
    - Electronic prescription
- Trustworthy authentic sources like
  - Databases with Therapeutic relations
  - Database with capacities of caretakers
  - Meta Hub

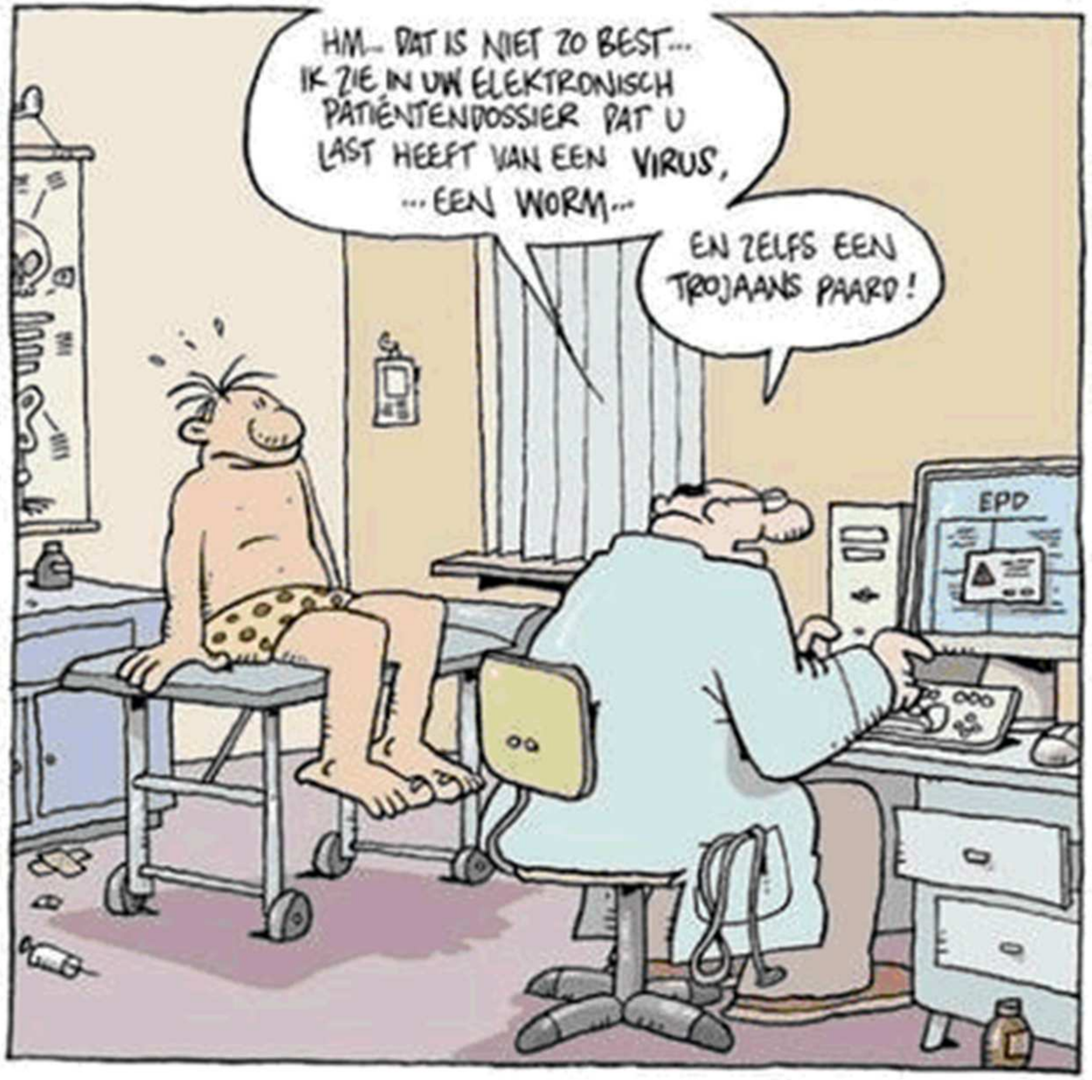
Legal Warranties

- eHealth law
- Specific laws initiated by eHealth (ex. E-Prescription)
- Authorized and permanently checked by Sectoral Committee
- Checked by management committee composed by representatives of all stakeholders.
- Upfront assurance of the legality of exchange of personal information and possible constraints.
- Service Level Agreements assure:
  - Availability
  - Performance

Base Service UAM

Impossible d'afficher l'image.

Information Security


HM... DAT IS NIET ZO BEST... IK ZIE IN UW ELEKTRONISCH PATIËNTENDOSSIER DAT U LAST HEEFT VAN EEN VIRUS, ...EEN WORM...
EN ZELFS EEN TROJAANS PAARD!
EPD

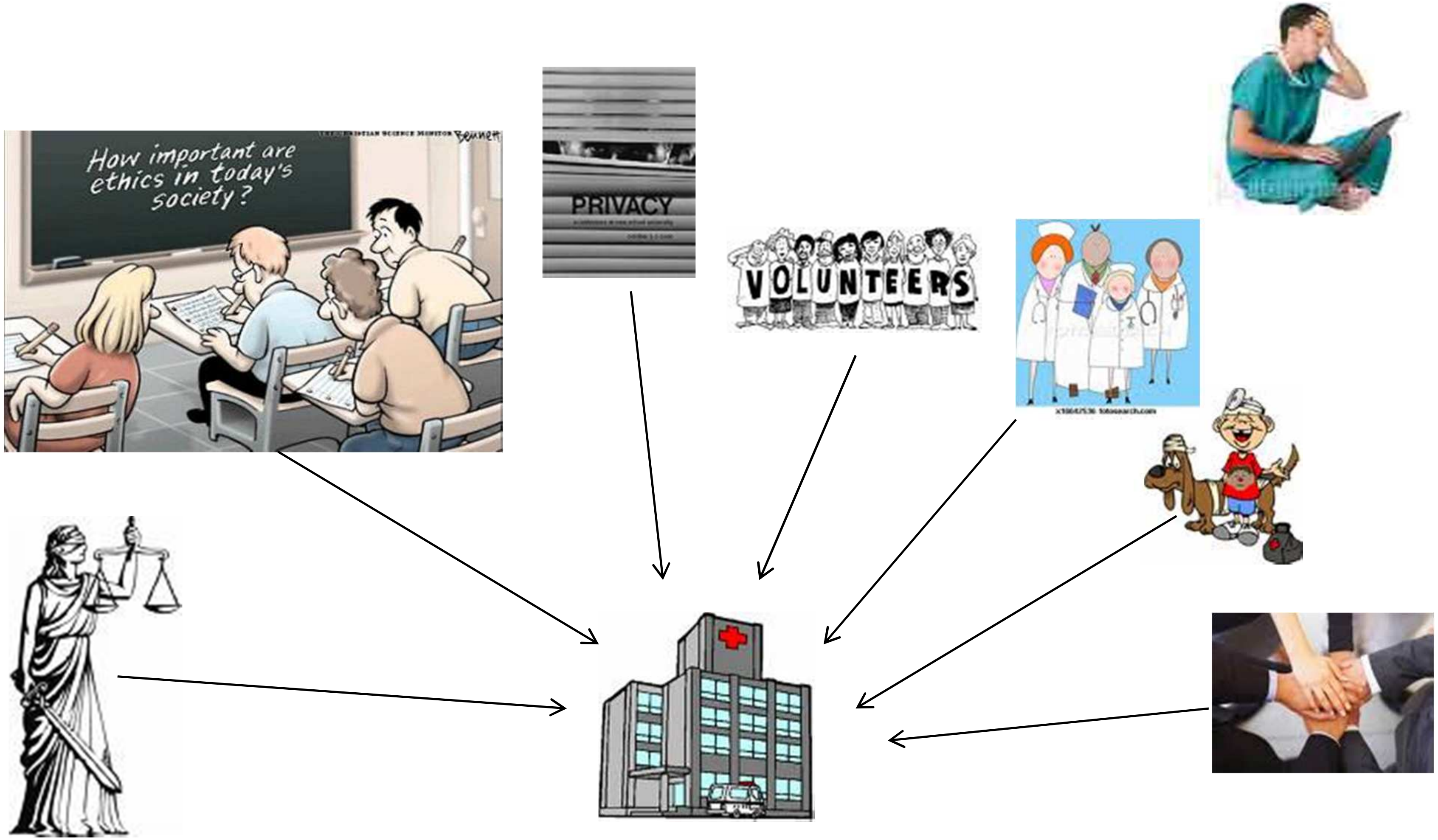
Reference

- http://www.privacycommission.be/en/in_practice/information-security/index.html
- http://www.iso.org/iso/search.htm?qt=information+security&searchSubmit=Search&sort=rel&type=simple&published=true
- http://www.staatsbladclip.be

Health information security goals

- Maintaining information confidentiality, availability, and integrity (including authenticity, accountability and audit-ability)
- In healthcare, privacy of subjects of care depends upon maintaining the confidentiality of personal health information.
- Maintain the integrity of data using secured audit trails, and other system data in ways that allow breaches in confidentiality to be noticed.
- Patient safety depends upon maintaining the integrity of personal health information, failure to do this can also result in illness, injury or even death.
- A high level of availability is an especially important attribute of health systems, where treatment is often time-critical.
- Disasters that could lead to outages in other non-health-related IT systems may be the very times when the information contained in health systems is most critically needed.

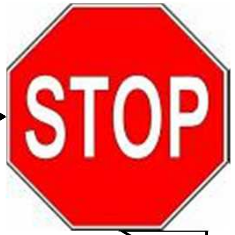
Influencers



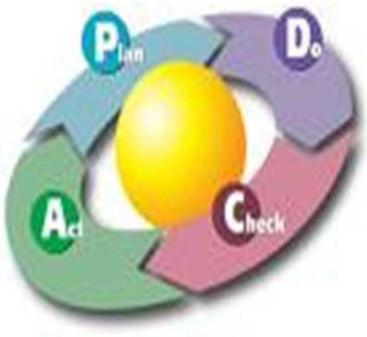
How it works, a little exercise

For example: Your hospital signed a contract stating it will comply with conditions imposed by sectoral committee to get access to the National Register

Check om strategic level if conditions above have a impact on global (security) policy. If yes analyze risks and update policy.



On tactical level analyze risks and define / maintain measures (controls) to enforce the policy, maintain accountability and audit-ability.



On operational level enforce and
evaluate controls.

Informationstores

http://www.youtube.com/watch?v=GAuiXr8mwOE

http://www.youtube.com/watch?v=XlTEIYGk3Ro

Why informationsecurity measures?

Sample threats for information security :

- Errors and mistakes
- Theft
- Fraud
- Failure of systems (Physical infrastructure, third parties, …)
- Attackers (internal - external) with bad intentions
- Threats to privacy

Increased Threat

http://www.waarschuwingsdienst.nl/movies/botnetfilm_en.mp
g

http://gocsi.com/forms/csi_survey.jhtml

2008

CSI Computer Crime & Security Survey

General conclusions CSI report

- This year’s survey results are based on the responses of 522 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions anduniversities. This is the 13th year of the survey.
- The most expensive computer security incidents were those involving financial fraud…with an average reported cost of close to $500,000 (for those who experienced financial fraud). The second-most expensive, on average, was dealing with “bot” computers within the organization’s network, reported to cost an average of nearly $350,000 per respondent. The overall average annual loss reported was just under $300,000.
- Virus incidents occurred most frequently…occurring at almost half (49 percent) of the respondents’ organizations. Insider abuse of networks was second-most frequently occurring, at 44 percent, followed by theft of laptops and other mobile devices (42 percent).

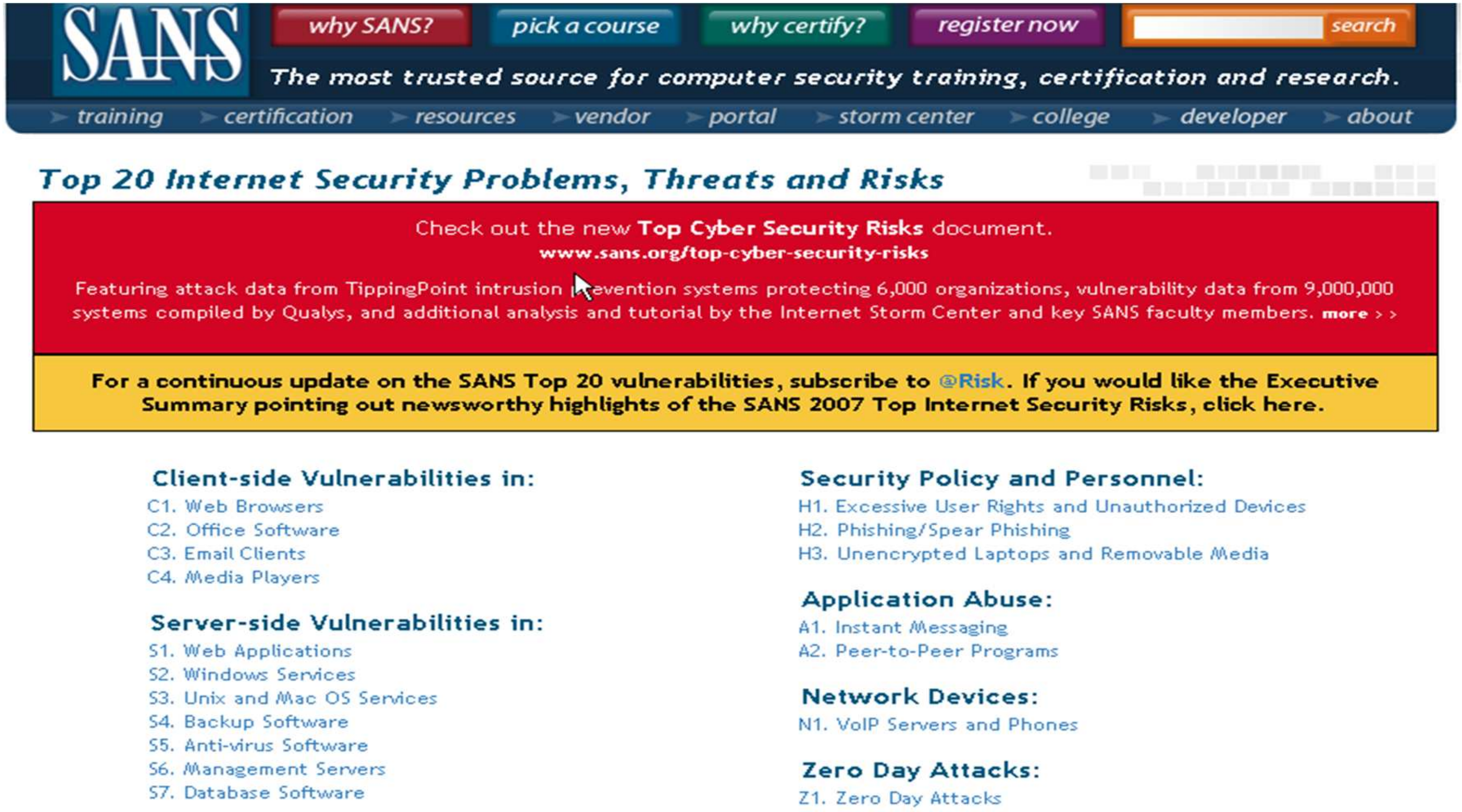
General conclusions CSI report

- Almost one in ten organizations reported they'd had a Domain Name System incident…up 2 percent from last year, and noteworthy, given the current focus on vulnerabilities in DNS.
- Twenty-seven percent of those responding to a question regarding "targeted attacks"… said they had detected at least one such attack, where "targeted attack" was defined as a malware attack aimed exclusively at the respondent's organization or at organizations within a small subset of the general business population.
- The vast majority of respondents said their organizations either had (68 percent)…or were developing (18 percent) a formal information security policy. Only 1 percent said they had no security policy.

Some important weaknesses

Sans research results Internet – Top 20

http://www.sans.org/top-cyber-security-risks/



Top 20 Internet Security Problems, Threats and Risks

Check out the new **Top Cyber Security Risks** document.
www.sans.org/top-cyber-security-risks

Featuring attack data from TippingPoint intrusion prevention systems protecting 6,000 organizations, vulnerability data from 9,000,000 systems compiled by Qualys, and additional analysis and tutorial by the Internet Storm Center and key SANS faculty members. **more** > >

For a continuous update on the SANS Top 20 vulnerabilities, subscribe to @Risk. If you would like the Executive Summary pointing out newsworthy highlights of the SANS 2007 Top Internet Security Risks, click here.

Client-side Vulnerabilities in:

C1. Web Browsers
C2. Office Software
C3. Email Clients
C4. Media Players

Server-side Vulnerabilities in:

S1. Web Applications
S2. Windows Services
S3. Unix and Mac OS Services
S4. Backup Software
S5. Anti-virus Software
S6. Management Servers
S7. Database Software

Security Policy and Personnel:

H1. Excessive User Rights and Unauthorized Devices
H2. Phishing/Spear Phishing
H3. Unencrypted Laptops and Removable Media

Application Abuse:

A1. Instant Messaging
A2. Peer-to-Peer Programs

Network Devices:

N1. VoIP Servers and Phones

Zero Day Attacks:

Z1. Zero Day Attacks

Some important weaknesses

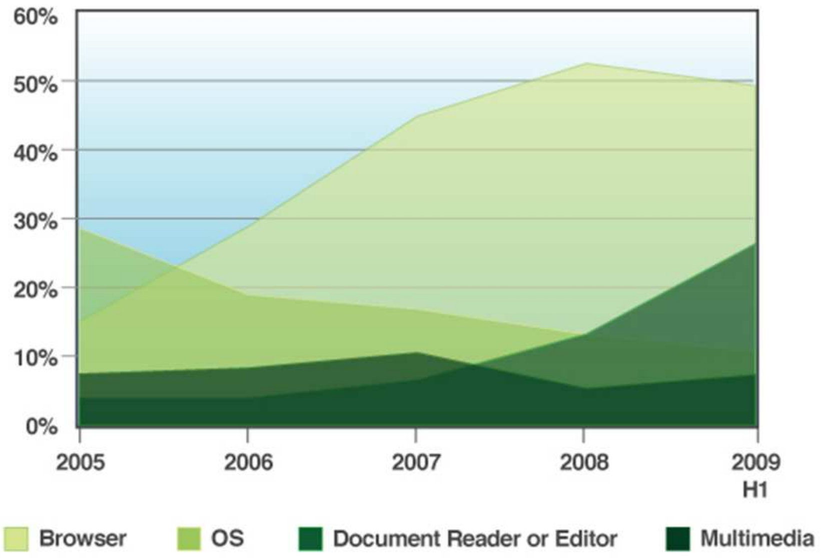
Sans research results

Some highlights:

- Client-side software that remains unpatched.
- Internet-facing web sites that are vulnerable.
- Rising numbers of zero-day vulnerabilities

Prevalent Client-Side Software

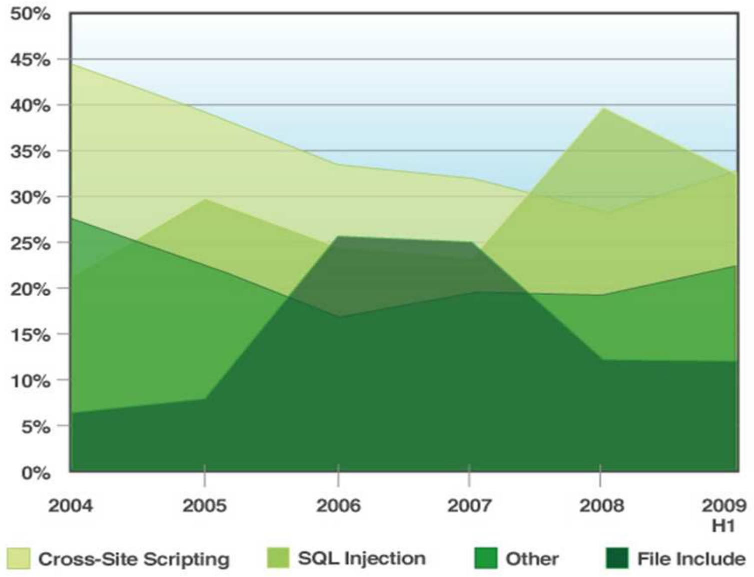
Percent of Critical and High Vulnerability Disclosures



source: IBM X-Force®

Web Application Vulnerability Disclosures

2004-2009 H1

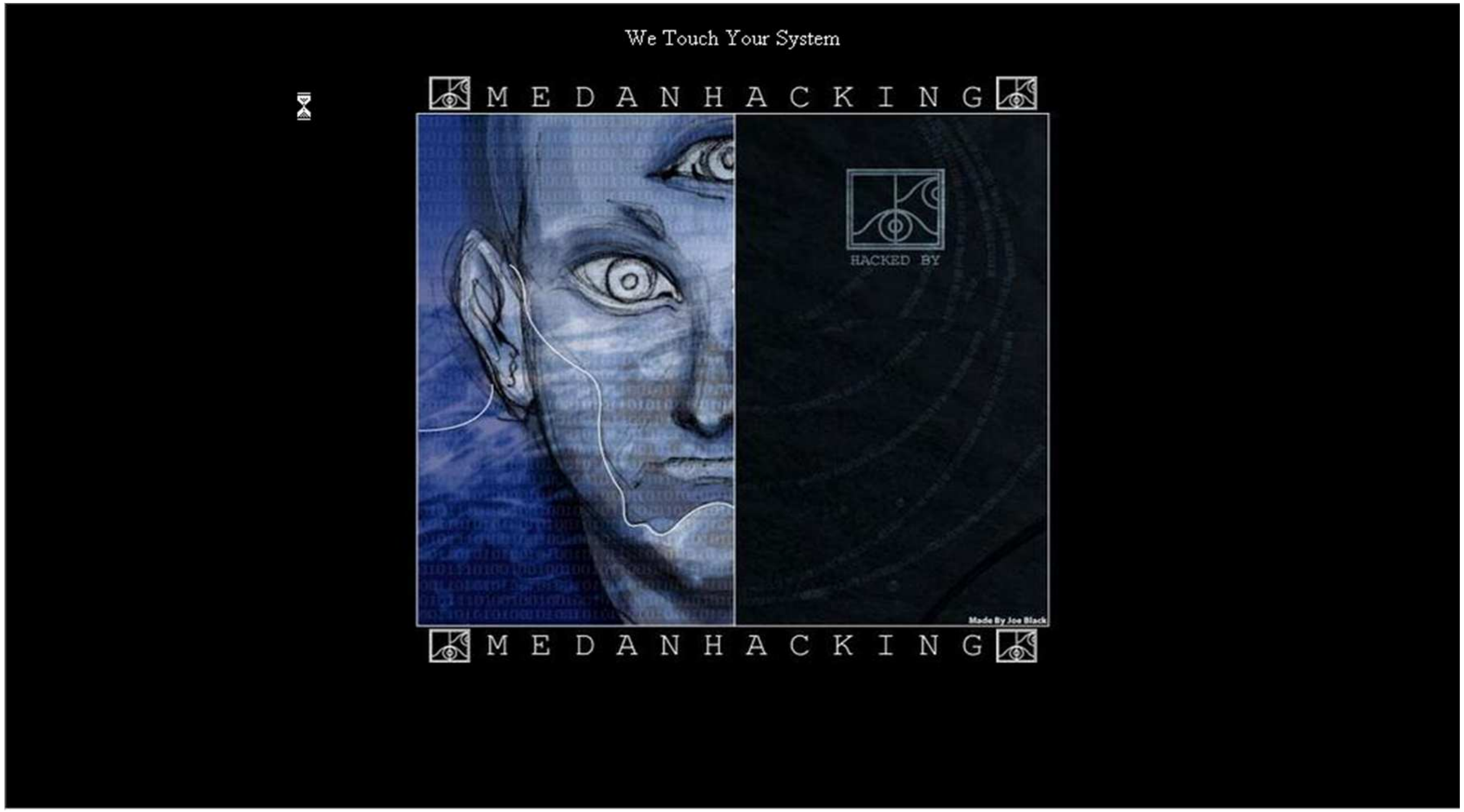


source: IBM X-Force®

Possible consequences

- Financial loss
  - direct
  - indirect: “assurance against hacking”
- Liability
  - Medical errors (switched patients, wrong medication)
  - Death
- Reduced public trust.
- Breached professional standards and ethics.
- Lowered interoperability among health systems

Illustratie : Defaced websites



We Touch Your System

MEDANHACKING

HACKED BY

Made By Joe Black

MEDANHACKING

The attackers

- Script kiddies
  - The usual stereotypes: children or bored employees etc.....
  - Scripts and tools are available available :
    - free on the Internet (nmap, nessus, backtrack etc.)
    - payed on the Internet, (backorfrice, botnetmanager etc)
    - exploit recently discovered weakspots.
- Internet security community:
  - Informationsecurity professionals
  - White-Hat
    - Focused on improvement of general security levels
    - Actively search for exploitable weaknesses
    - Openly share information about found weaknesses
    - Report found weaknesses to those responsible to fix.
  - Black-hat & Organized Crime
    - Aimed on personal (financial) profit.
    - Exploit unpatched weaknesses
- Former employees:
  - Act out of fun or revenge
  - Dangerous because of inside knowledge

Attack vectors

Technical

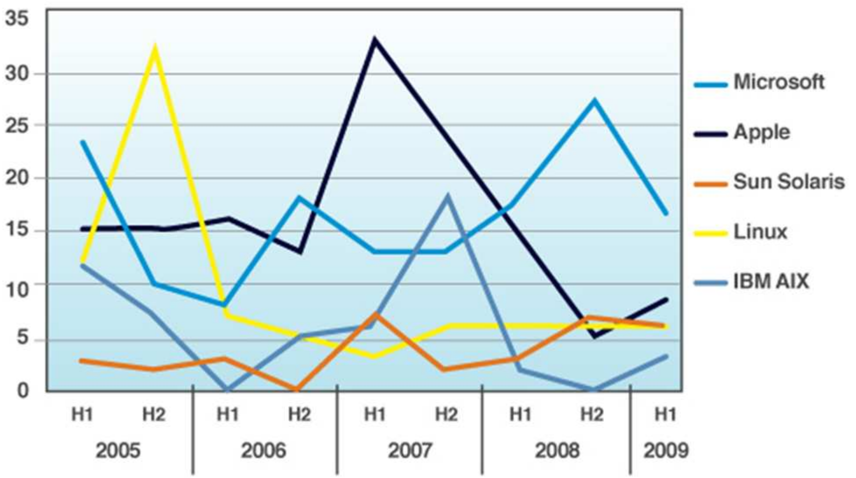
- Network
  - snif traffic,
  - re-route traffic (DNS spoofing),
  - mask (IP spoofing, piggy backing),
  - sabotage,
- Operating system
  - rootkits,
  - infected drivers,
  - default setup and passwords,
  - faulty design (one fits all design),
  - huge number of codelines (one major error per 4000 lines),
- Application
  - puchased programms,
  - downloaded programms,
  - own developped programs,

} http://cwe.mitre.org/top25/index.html

- Radsomware, Crimeware, Spyware, Worms, Virusses etc (Malware)
- Scripting options in harmless looking files like pdf, doc and lately pictures

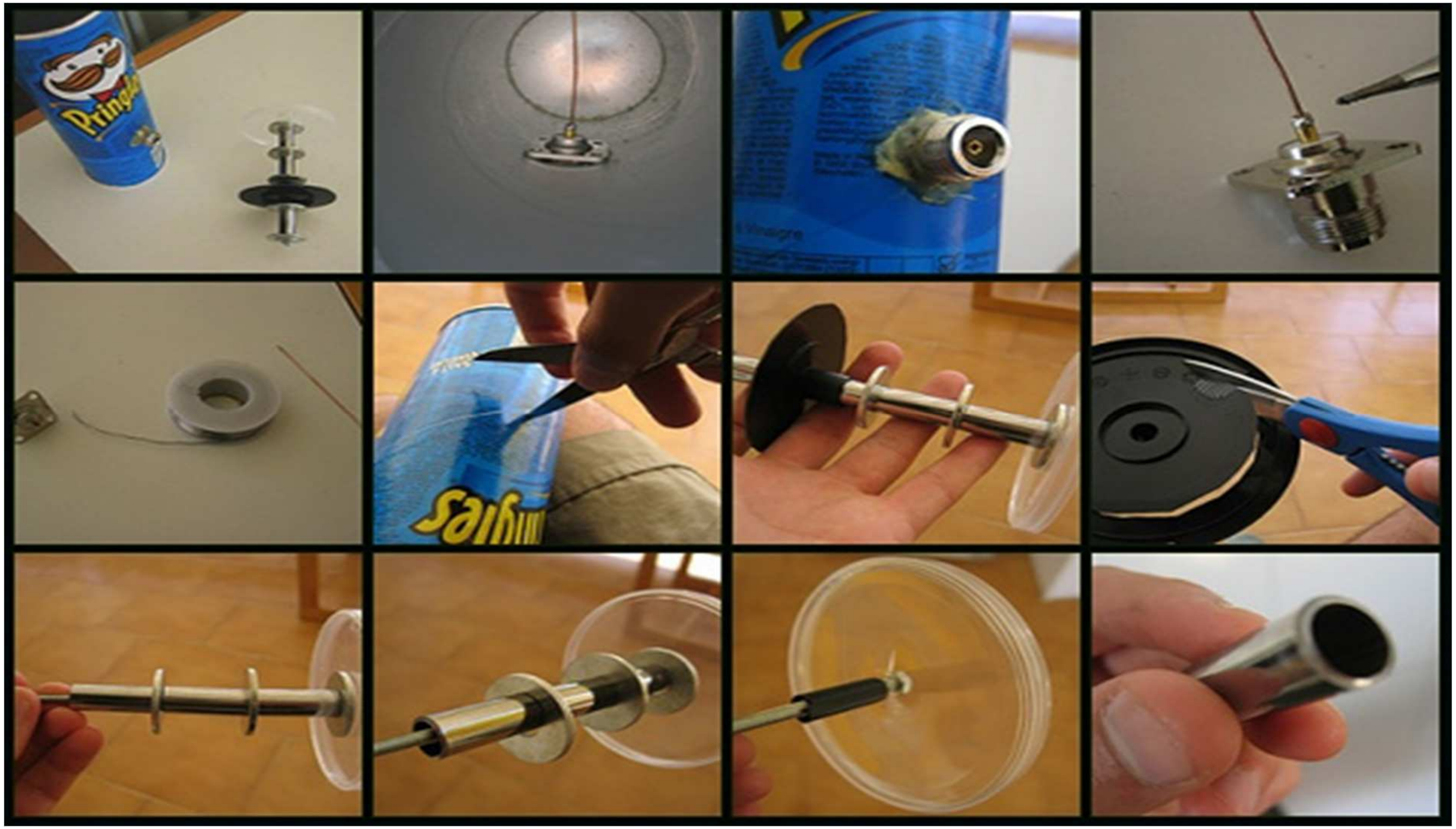
The attack is often masked using for example encryption.

Critical and High Operating System Vulnerability Disclosures



source: IBM X-Force®

Pringles Cantenna



http://flakey.info/antenna/waveguide/

Attack vectors

Phases:

- Zero Day, proof-of-concept available but kept secret, no work-a-round or patch available,
- Vulnerability, proof-of-concept published, no work-a-round or patch available,
- Exploit, proof-of-concept on how to exploit the underlaying vulnerability has been issued, no work-a-round nor patch available,

Register of exploits:

- Common Vulnerabilities and Exposures List (CVE) (http://cve.mitre.org/about/)
- Open Vulnerability Assessment Language (OVAL) (http://oval.mitre.org/)
- Propriatry for example IBM/ISS (http://xforce.iss.net/)

Conclusions:

- In order to mitigate damage patch asap. Time between Zero Day and patch should be as short as possible.
- All systems are vulerable to Vulnerabilities matching their OS or Application while unpatched.
- Time between Zero Day and Exploit is critical
- Broad access to source code provides a large auditing community

Attack vectors

Physical

- Accidential
  - Earth Quake
  - Flood
  - Storm / Tornado
  - Fire
- Intentional
  - Terrorist attack
  - Burglary
  - Vandalism
  - Skimming
  - Spying (swift affair)
  - War

Attack vectors

Human

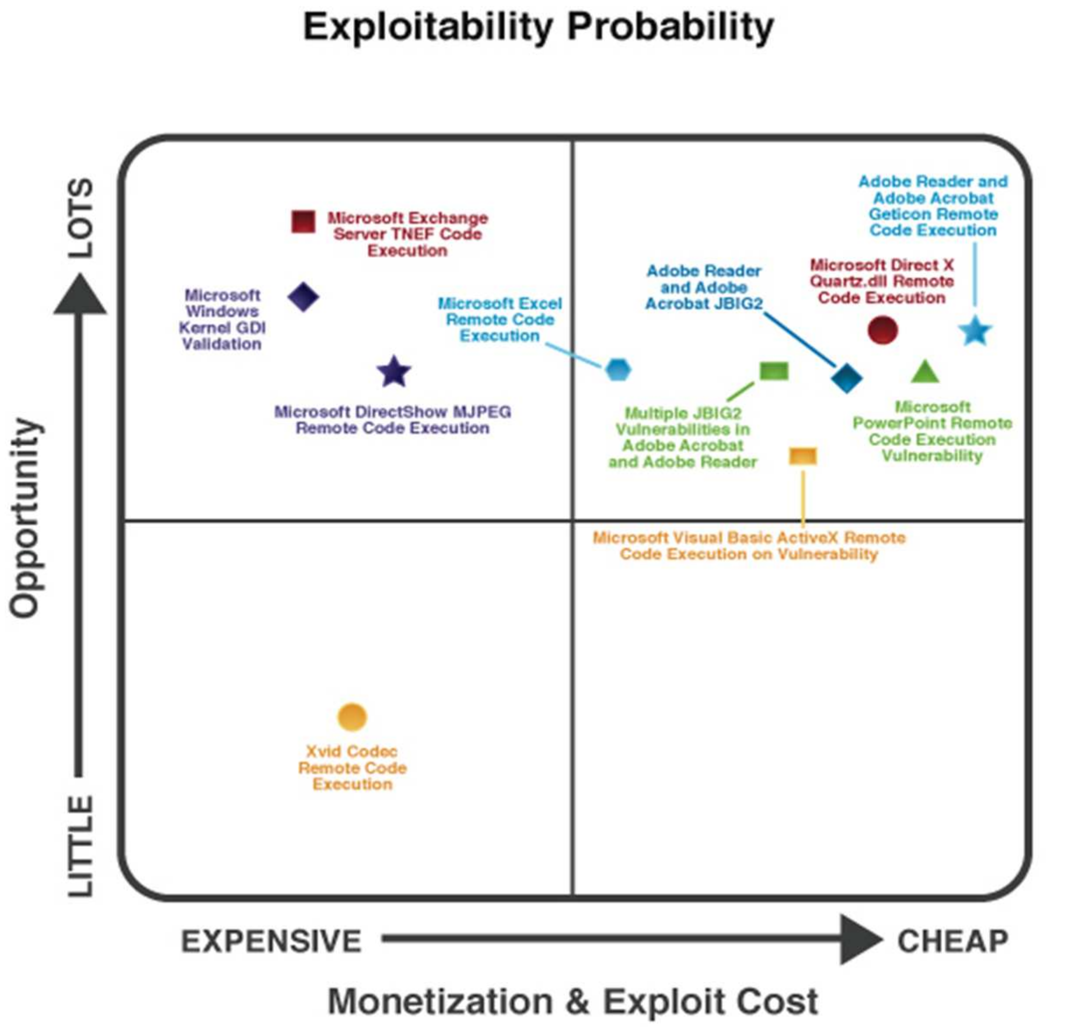
- Social hacking
  - (Chinese) USB Sticks
    - http://www.hln.be/hln/nl/4125/Internet/article/detail/1061587/2010/02/01/Chinezen-hacken-zakenlui-met-geschonken-USB-sticks.dhtml
  - Pretend to be helpdesk, boss etc.
  - Trade password for a choco bar.
    - http://www.ad.nl/ad/nl/1005/Digitaal/article/detail/458150/2010/01/21/Computergebruikers-ruilen-wachtwoord-voor-chocoreep.dhtml
  - Professional blindness / non awareness
  - Identity theft
- Complex policies and controls
- Bribe
- Fraud
  - Antwerp credit card issue
- Forgery
  - Dutch chamber of commerce issue

Attackscenario

- Collect information
  - Public sources
    - IP registries, DNS information
    - public websites, search engines
    - Job ads (security officer 😉)
    - phone lists
    - (Official) Registers (https://www.erin911.com, facebook, twitter etc.)
    - Company annual reports (http://bcc.nbb.be/BCCIA0101/WEB/actions/startbcc?lang=N)
    - newsgroups (google.com: historical trace)
  - Other sources
    - email header
    - port scanner to find hosts, ip addresses and open ports
    - vulnerability scanner to find types of systems and known vulnerabilities
- Actively exploit known vulnerabilities
- Wipe possible traces

BLOOVER DEMO

Attackscenario



source: IBM X-Force®

Legal context

Hacking is illegal!!

- Government (war in Afgenistan)
  - http://www.security.nl/artikel/32347/1/Het_speelkwartier_is_over_.html
- Political
  - http://sniggle.net/hacktivism.php
- Organized crime
  - http://www.hbvl.be/nieuws/buitenland/hackers-plunderen-braziliaans-regenwoud.aspx
- For the kick
  - http://www.hbvl.be/nieuws/media-en-cultuur/aid887545/pesten-professionele-hackers-jim-met-storingen.aspx

Width vs Depth

- Width
  - Services
    - SLA
    - UPC
  - Procedures
    - HRM Security controls (NDA, Contract, Pre-employment scanning)
    - Split responsabilities
    - Security management
  - Organization
  - Technical
    - IT Technical
    - Infrastructural

act
plan
PDCA-Cycle
check
do

- Depth
  - Strategical level
  - Tactical level
  - Operational level

Discussion: general situation

Everyone knows but..

- No budget
- No time
- Difficult
- Complex
- Digital illiterate

Governance

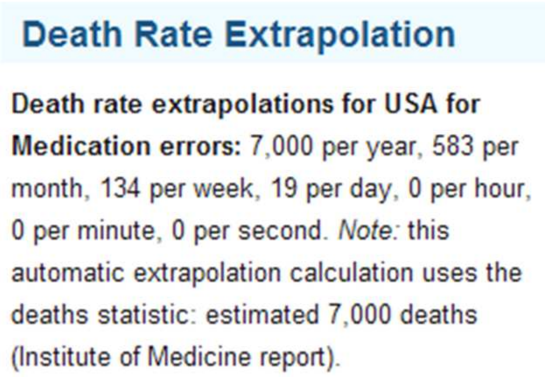
- Many areas of information management, such as accreditation and data protection, can be considered to fall within the scope of information governance. It is vitally important that the scope of information governance embrace and aid the ongoing deployment of information security so that due attention is always paid to confidentiality, integrity and availability. Information security is clearly a critical component enabling the broader aspects of information governance.
- All countries and jurisdictions will undoubtedly have case studies where breaches have led to misdiagnoses, deaths or protracted recoveries. Clinical governance frameworks therefore need to treat effective information security risk management as equal in importance to care treatment plans, infection management strategies and other “core” clinical management matters.

Information whose CIA to protect

- personal health information
- pseudonymized data derived from personal health information via some methodology for pseudonymous identification
- statistical and research data, including anonymized data derived from personal health information by removal of personally identifying data
- clinical/medical knowledge not related to any specific subjects of care, including clinical decision support data (e.g. data on adverse drug reactions)
- data on health professionals, staff and volunteers
- information related to public health surveillance
- audit trail data, produced by health information systems that contain personal health information, or pseudonymous data derived from personal health information, or that contain data about the actions of users with regard to personal health information
- system security data for health information systems, including access control data and other security related system configuration data for health information systems.

Typical things to consider

- A lot of people walking around: staff, volunteers, visitors subcontractors
- Some health organizations are underfunded, staff works under significant stress
- People are dedicated to health not to IT or security (lack of interest)
- Integrity of information is most important. If things go wrong you have something to prove.



Death Rate Extrapolation

Death rate extrapolations for USA for Medication errors: 7,000 per year, 583 per month, 134 per week, 19 per day, 0 per hour, 0 per minute, 0 per second. *Note:* this automatic extrapolation calculation uses the deaths statistic: estimated 7,000 deaths (Institute of Medicine report).

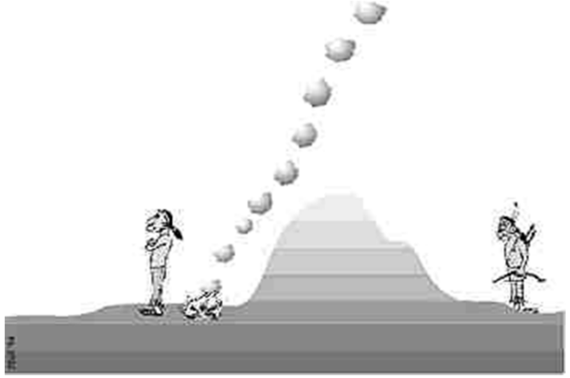
ISMS

Http://www.verinice.org

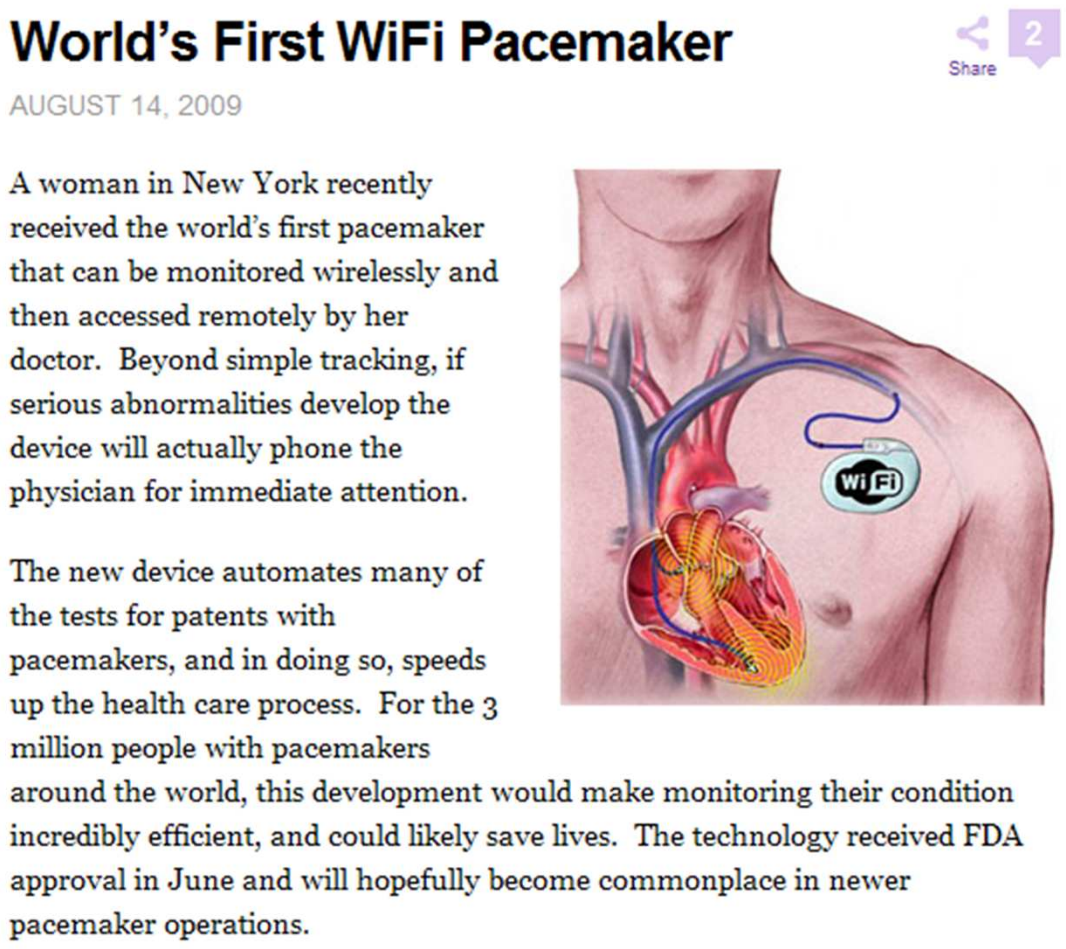
Threats to health information security

Annex A of ISO27799

- Masquerade of insiders, service providers or outsiders
- Unauthorized use
- Introduction of malware
- Misuse of system resources
- Communications infiltration, jamming or interception
- Repudiation
- Misrouting
- Errors
- Staff shortage
- Theft
- Vandalism
- Terrorism



Lose or gain?



World's First WiFi Pacemaker

Share 2

AUGUST 14, 2009

A woman in New York recently received the world's first pacemaker that can be monitored wirelessly and then accessed remotely by her doctor. Beyond simple tracking, if serious abnormalities develop the device will actually phone the physician for immediate attention.

The new device automates many of the tests for patents with pacemakers, and in doing so, speeds up the health care process. For the 3 million people with pacemakers around the world, this development would make monitoring their condition incredibly efficient, and could likely save lives. The technology received FDA approval in June and will hopefully become commonplace in newer pacemaker operations.

http://www.psfk.com/2009/08/worlds-first-wifi-pacemaker.html

Future developments

CONCEPTS FOR HEALTH
PSFK presents
FUTURE OF HEALTH
unicef
BODYlanguage
Your lungs say: "Don't even think about smoking. It's been 8 hours since your last cigarette – carbon monoxide in your blood has already dropped by half. Look, I'm already getting pinker!"
Dr. Cube
cpr
12
abc
UNICEF BRM
ID #: U7847382
NAME: Moussa
Lilou
SEX: M
Options
Clear
93
Before Meal
Reminder
Notes
the tent
Angola Region

http://www.psfk.com/future-of-health

Th@nk you !
Questions ?

https://www.ehealth.fgov.be