



# Cybersecurity:

## awareness, awareness, awareness

# Introduction

René Ritzen

Corporate Information Security Officer  
Utrecht University



**Utrecht University**

Jean Popma

Corporate Information Security Officer  
Radboud University

**Radboud University**



# Today's menu

- Why bother?
- What, Why, How & Who?
- The weakest link
- Who? Me?
- Message in a bottle: One size fits no-one
- The Prophet and the mountain
- The personal approach
- Do's and Dont's
- Where do we go?



# Why bother?

- Information Security & Privacy is expensive
- Return on investment is low
- Risks seem to be acceptable
- Better invest in primary objectives education and research





# Breach of Confidentiality

**Hogeschool versprekt**  
9 maart 2016  
Hogeschool Van Hall Lare  
doorgestuurd naar alle stud  
BSN-nummer van studenten

**Gegevens bijna 800 kankerpatiënten gestolen**  
3 maart 2016 om 16:42 door Astrid Ottens

**NKI-AVL**  
Het Nederlands Kanker Instituut  
Antoni van Leeuwenhoek Ziekenhuis

**studenten**  
SERVICE  
in per ongeluk  
s, -mailadressen en het

Dit meldt **Omroep Gelderland**.  
**Publeaks**, waar mensen anoniem

**Studenten van de Radboud**  
interne netwerk kampte met een beveiligingsprobleem  
salarissen van medewerkers op straat  
van personeel en studenten.

Dieven hebben een onbeveiligde harde schijf gestolen met de gegevens van 781 kankerpatiënten van het Antoni van Leeuwenhoek Ziekenhuis. De schijf is in december uit de kofferbak van de auto van een onderzoeker gestolen. Dat maakte het Amsterdamse ziekenhuis donderdag bekend.

Het Antoni van Leeuwenhoek. Foto: ANP



# Identity Fraud

ORGANISATIE - 22 APRIL 2014 Foto: ANP

## Een op de vijf WUR'ers trapt in phishing mail

tekst: Rob Ramaker

Nieuws

Een op de vijf medewerkers en studenten is in een test met phishing mails getrapt. Zij gaven afgelopen week vrijwillig hun login én wachtwoord prijs. De IT-afdeling is geschrokken van het resultaat en wil meer gaan voorlichten.

RUG-med  
nep-phis

Gepubliceerd: 1  
Laatste update

Duizend werknemers van de Rijksuniversiteit Wageningen (WUR) zijn in een test met nep-phishingmail getrapt en hebben hun e-mailadres, personeelsnummer en wachtwoord ingevoerd.

Dat meldt Webwereld. Van de 6000 werknemers die de e-mail ontvingen, hebben 3000 medewerkers het bericht ook daadwerkelijk gelezen. Hierna klikten 2800 werknemers op de verdachte link en voerden uiteindelijk 1000 werknemers gevoelige informatie in.



# Data Manipulation

## Tentamenfraude HHS



07-02-2014 | 16:27



Op de Haagse Hogeschool wordt waarschijnlijk flink gesjoemeld met tentamens. Studenten weten van tevoren de hand te leggen op tentamenvragen en hoeven alleen nog maar de antwoorden uit hun hoofd te leren, zo blijkt uit informatie van Omroep West. De directie van de Haagse Hogeschool laat nu onafhankelijk onderzoek doen naar mogelijke tentamenfraude.



# Espionage



## Nederlands-Duits defensiebedrijf gehackt door Chinezen

Het Nederlands-Duitse bedrijf Rheinmetall Defence is vanaf 2012 aangevallen door een groep Chinese hackers. Die hebben daarbij 'zeker' toegang gekregen tot technologische informatie van het bedrijf en hadden waarschijnlijk tot voor kort controle over het bedrijfsnetwerk. De hackers kwamen binnen door een aanval op het Duitse bedrijf, waardoor ook Nederlandse informatie binnen handbereik kwam. Dat bevestigen bronnen in de inlichtingenwereld aan de Volkskrant.

Door: Huib Modderkolk 15 juni 2016, 02:00

NEWS

## University of Virginia will spend millions on new security after Chinese hack

present in University server since Spring 2014

Pin.it

ah Hall | Sep 16 2015 | 09/16/15 10:23pm

for its information  
lune data  
more




# Abuse of ICT-facilities

Is uw pc besmet door Pobelka?

donderdag 14 feb 2013, 17:00 (Update: 15-02-13, 07:17)

## Microsoft 'blacklists' Oxford University in accidental 'spam' overload

Oxford University managed to accidentally overflow Windows Live services, triggering Microsoft's anti-spam technologies, resulting in the university being 'blacklisted'.



In totaal is 750 Gb aan data onttreemd via een zogeheten botnet

NOS

Van duizenden Nederlandse bedrijven, ziekenhuizen, universiteiten, overheidsinstellingen en mediabedrijven zijn gevoelige gegevens in handen gekomen van cybercriminelen.

In totaal is 750 Gb aan data onttreemd via een zogeheten botnet, een netwerk van computers, waarmee ze doordrongen in zo'n 150.000 computers in Nederland.

# Disruption of Infrastructure

## Websites Universiteit Leiden door ddos-aanval

Gepubliceerd: 06 oktober 2015 14:17  
Laatste update: 06 oktober 2015 21:33

De websites van Universiteit Leiden was o  
ddos-aanval.

Dat meldde de universiteit dinsdag.

De ddos-aanval werd dinsdagmiddag geconstateer  
avond waren opgelost. Er wordt nog onderzocht of  
met de dreiging van dinsdag.

## Vrije Universiteit Amsterdam getroffen door cryptolocker-virus

Door Joost Schellevis, maandag 9 maart 2015 14:32, 101 reacties, 13.069 views • [Feedback](#)

In de afgelopen week zijn circa 200 computers van de Vrije Universiteit Amsterdam getroffen door Cryptolocker, malware die bestanden versleutelt en tegen betaling weer ontsleutelt. Volgens de VU zijn nog geen bestanden verloren gegaan als gevolg van de infectie.

Woordvoester Aukje Schep bevestigde de infectie, nadat beveiligingsonderzoeker Rickey Gevers een screenshot van een mededeling van de VU [postte](#) op Twitter. De waarschuwing roept studenten en medewerkers op om niet zomaar bijlagen in e-mails te openen. Ook op linkjes mag niet zomaar worden geklikt, waarschuwt de Vrije Universiteit.

Volgens woordvoester Schep begon de relatief grootschalige infectie een week geleden en zijn er in die periode 'om en nabij' tweehonderd computers geïnfecteerd. "De malware waart al wel een tijdje rond, de afgelopen maanden werden af en toe al pc's geïnfecteerd", zegt Schep. Waardoor het aantal aanvallen zo is toegenomen, weet Schep niet. "We hebben nog geen idee in welke hoek we dit moeten zoeken."

De zogeheten ransomware versleutelt bestanden en eist dat gebruikers betalen voordat ze weer worden ontsleuteld. "Maar wij betalen natuurlijk niet", aldus Schep. De universiteit stelt dat er voor zover bekend bovendien nog geen bestanden verloren zijn gegaan door de malware-infectie.

# Main threats for HEI

- Breach of confidentiality
- Identity fraud
- Data manipulation
- Espionage
- Disruption of ICT infrastructure
- Abuse of ICT-facilities
- Intentional reputation damage



# Risks

- Reputation damage
- Loss of intellectual property
- Disruption of primary process
- Substantial cost of repair
- Non-compliance
- Personal damages



# More to come....

## 'Cybercrime kost Nederland jaarlijks 10 miljard'

© MA 4 APRIL, 00:13 BINNENLAND, ECONOMIE, TECH



N nieuwsuur

## 'Over vijf jaar helft misdaad door cybercriminelen'

© WOENSDAG, 16:46 BINNENLAND



NOS

Nieuws

Sport

Uitzendingen

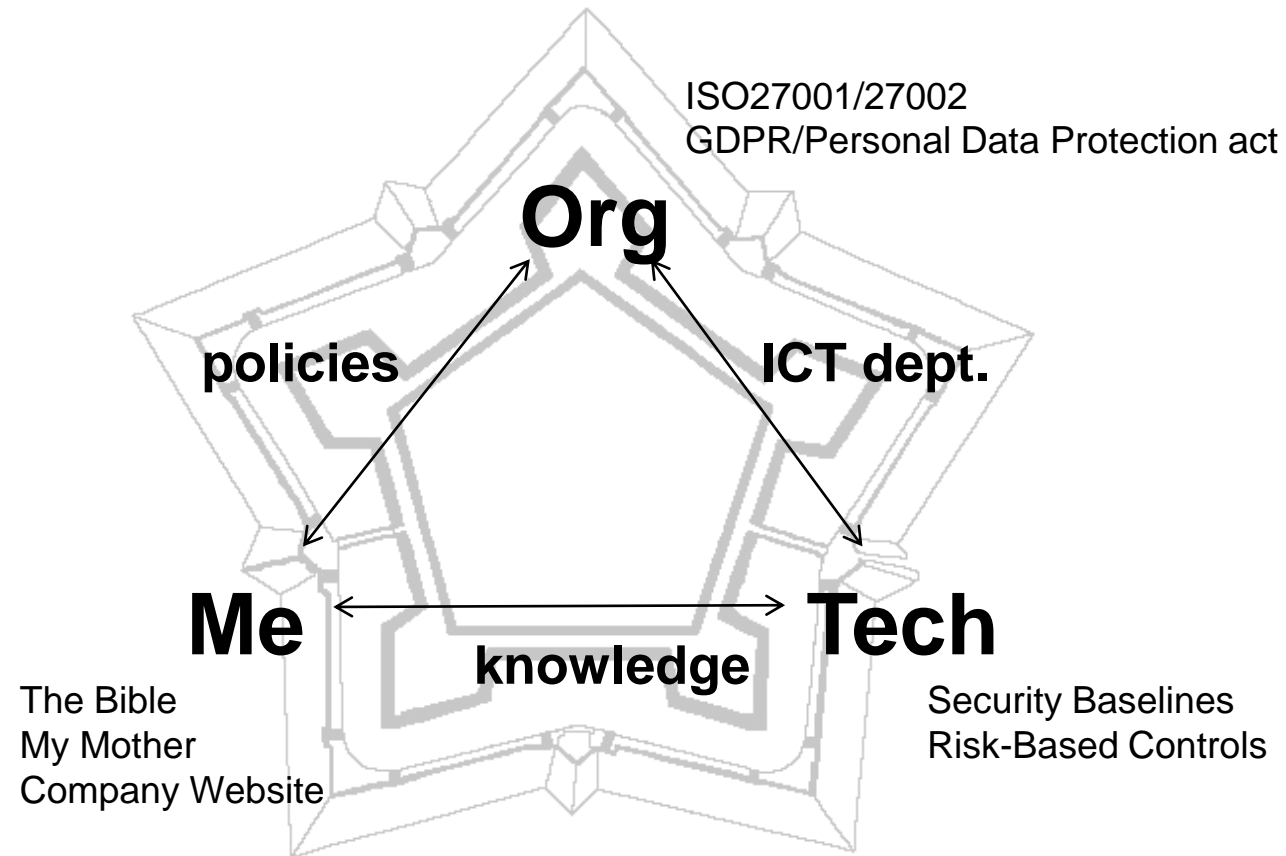
2 GERELATEERDE ARTIKELN

## Dijkhoff: cybercrime begint economie te raken

© 11-04-2015, 11:04 POLITIEK



# How to deal with that?







<https://www.youtube.com/watch?v=opRMrEfAlil>





# The weakest link

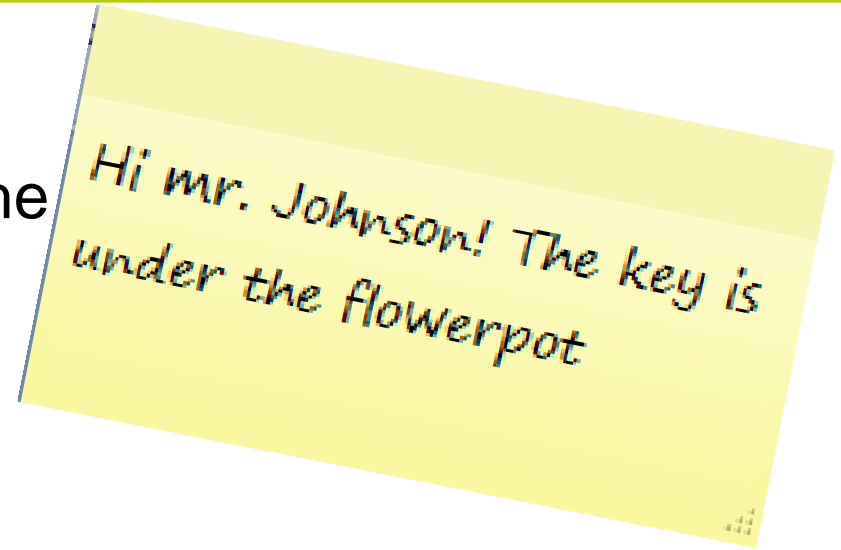
## The General Picture:

- Lack of risk awareness
- Lack of responsibility awareness
- Lack of empowerment
- Failing personal judgement
- The inevitable mistake will be made



# Who? Me?

- Who closes the door after leaving home in the
- The same for the backdoor?
- Who leaves valuables in plain sight?
- Who puts a key under the flowerpot or doormat?
- Who puts a note next to the doorbell ?



# Burglary

2012	Households	
# in NL	8.000.000	
# of burglaries	92.000	
Probability	1,2%	
Average damage	€ 1.800	
Total damage NL	€ 165.600.000	
Average detection in	10 minuten	
Probability someone is breaking in right now	0,00001%	

# Burglary

2012	Households	Computers
# in NL	8.000.000	10.000.000
# of burglaries	92.000	1.000.000
Probaility	1,2%	10%
Average damage	€ 1.800	€ 300
Total damage NL	€ 165.600.000	€ 300.000.000
Average detection in	10 minuten	36 days
Probability someone is breaking in right now	0,00001%	1%

source: Prof. Eric Verheul, Inaugural address, January 2014

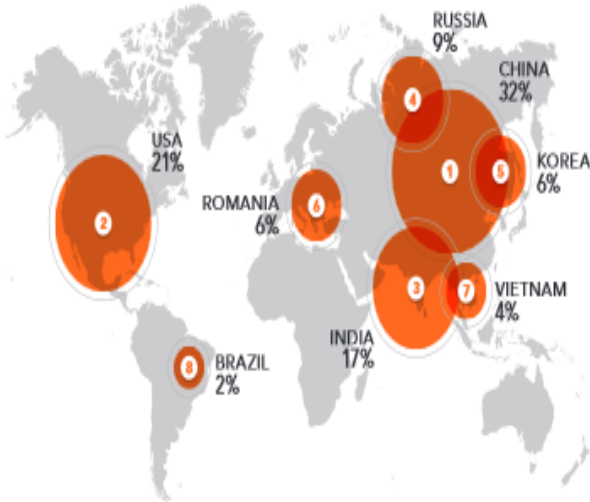


# Recognizing the villain

## » USA

### Origin of Attack

Attacks on US targets most frequently come from China, the US, India and Russia.



### Type of Malware

94% of malware observed was credential-stealing malware.



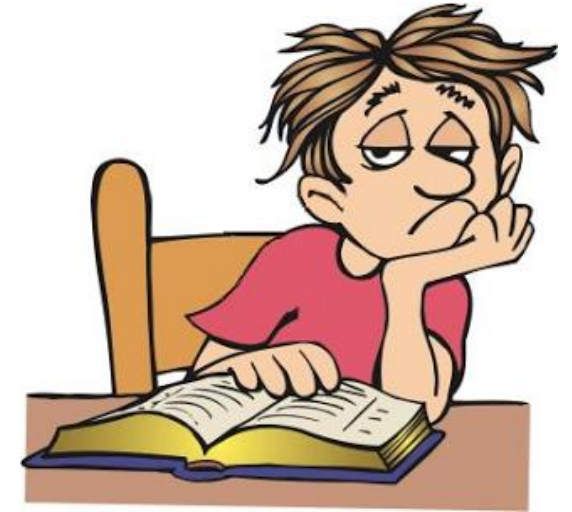
### # accounts compromised

MySpace:	360 miljoen
VK.com:	171 miljoen
LinkedIn:	117 miljoen
Tumblr:	65 miljoen
Mail.ru:	57 miljoen
iMesh:	51 miljoen
Yahoo Mail:	40 miljoen
Hotmail:	33 miljoen
Twitter:	32 miljoen
Mate1:	27 miljoen

Source: Volkskrant June 14 2016

# The general answer

- Rules and policies are declared
- A website! That'll teach 'em!
- Newsletters and more Newsletters
- Campaigns with nice little gadgets
- Posters!



# Who has?

- Rules and policies
- A website
- Newsletters
- Campaigns
- Posters

# Effectiveness

- Who remembers the last security awareness campaign in your own organisation?
- What was it about?
- What was the result ?
  - Worked very good
  - Well....
  - Did not have the intended effect

# The general result

- Rules and policies are unknown, hard to find, way to extensive and incomprehensible
- A website: Less than 5% makes use of company website
- Newsletters: Less than 5% reads articles about information security topics

Campaigns: Not now please, I am busy

- Awareness game: less than 5% participation
- Posters: Last no longer than a week.



# The prophet and the mountain

*“If the mountain will not come to the prophet,  
the prophet must go to the mountain”*

- The communication means to enhance awareness are indispensable, but on their own ineffective
- We cannot expect users to do this by themselves.
- If broadcasting does not work, we have to switch to narrowcasting.

# There is no such thing as THE user

- Recognize differences: management, teachers, researchers, support staff, IT-staff, guinea pigs, students etc. and address them in their own context.
- Learn from their problems and daily practice
- Discuss risks based on actual cases, how to recognize and avoid them
- Create alliances, not adversaries

# Do's and Dont's

DO	DON'T
Operate in context	<i>On size fits all</i> advice
Focus on a user's perspective	Enterprise-wide campaigns
Promote good practices, develop them where necessary.	Focus on 'not allowed here'
Reward responsible behaviour	Focus on what's going wrong
Suboptimal behaviour is much better than avoiding behaviour	Rules are rules
Stimulate self-regulation and local protocols, related to the actual work	
Learn fom mistakes and incidents and be transparant	
Use actuality as a hook to hang your hat on	
Forge coalitions with stakeholders	



# The Dutch Approach: CAAS: Community as a Service

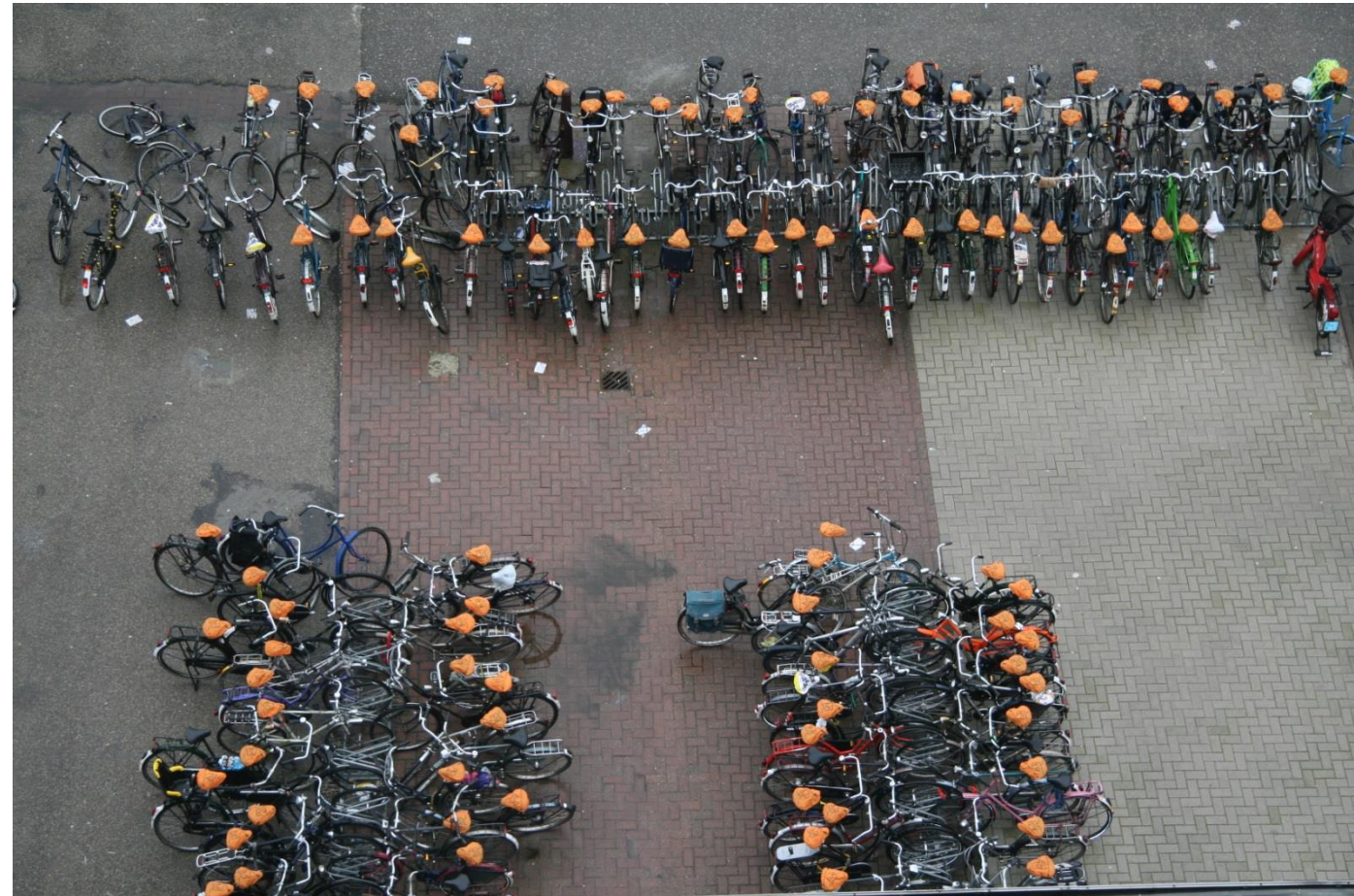
- Intensive community collaboration based on trust
- Cyber Save Yourself
  - As a source of materials : the toolkit
  - As a source of information: the knowledgebase
- Joint development of new materials and approaches (games, e-learning modules)
- Exchange of succes and failure



# Example: Game Smart Secure Yourself



# Example: Cyber Save Yourself



**CSY** CYBERSAVE YOURSELF





# Example: Your babies



**your bytes  
are  
your babies**

protect what's precious  
keep  safe



# Example: Wie zoet is ...



**ELF CSY CYBERSAVE YOURSELF CSY**  
**SAVE YOURSELF CSY CYBERSAVE YOU**

- Houd je wachtwoord voor jezelf!
- Helpdesksmedewerkers zullen nooit naar je wachtwoord vragen
- Type niet zomaar op een website je wachtwoord in
- Klik niet op links in mails en vul al helemaal niet daar je wachtwoord in

**Als je wachtwoord gestolen wordt, kan iemand jouw digitale identiteit overnemen!**

[www.ru.nl/cybersaveyourself](http://www.ru.nl/cybersaveyourself) SURF NET Radboud Universiteit Nijmegen



# Example: encryption week





# In search of new strategy

- In an open and pluriform HEI we cannot rely on company policies and technical means
- Users must be able to make personal judgements, based on risk-awareness in their own context. This is a personal responsibility for anyone in the organisation.



[https://youtu.be/AJKGrEI\\_omA](https://youtu.be/AJKGrEI_omA)





# In search of new strategy

- In an open and pluriform HEI we cannot rely on company policies and technical means
- Users must be able to make personal judgements, based on risk-awareness in their own context. This is a personal responsibility for anyone in the organisation
- Where strict rules or policies are required: Explain! Acceptance starts with understanding
- Management at all levels should have a focus on privacy and security:
  - Lead by example and implement good practices.
  - Show leadership in accomplishing behavioural and cultural changes.
  - Show that security and privacy are boardroom concerns

# Where do we go?

- Information technology will become even more pervasive
- Threats and risks for individuals and organisations will evolve
- Technological controls help but they are not the answer
- Key is individual and organizational awareness (responsibility of users and management)
- Substantial changes in culture and behaviour are required

# Cybersecurity: awareness, awareness, awareness

