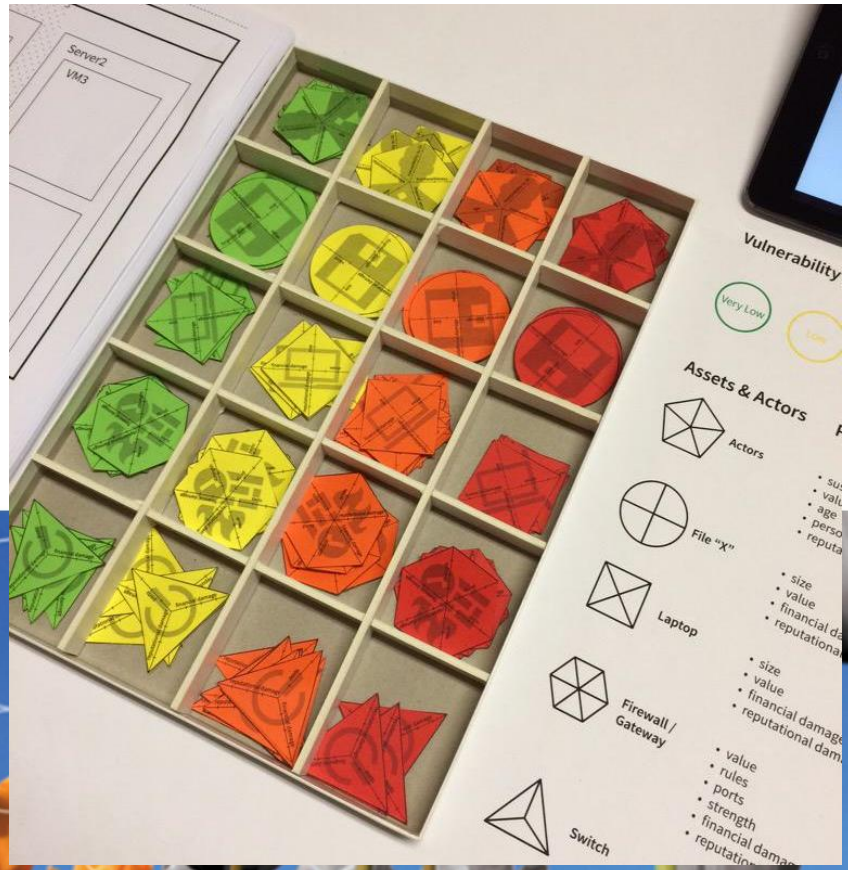
4TU.CybSec

Cyber security = cyber risk management

Wolter Pieters &
Jan van den Berg (TUD)

3TU cyber security
specialisation kickoff



TU Delft Delft University of Technology

TU/e Technische Universiteit Eindhoven University of Technology

UNIVERSITY OF TWENTE.

WAGENINGEN UR For quality of life

Problem: voting machine chip replacement

Proposed solution: seals & non-reprogrammable chips

Source: Teletekst / Wij Vertrouwen Stemcomputers Niet

Problem: Facebook invades users' privacy

Proposed solution: more privacy settings

- Hides users' personal data from each other
- But not from Facebook itself
- Encryption? But what about the business case?

Problem: vulnerability in OV-chipkaart

Proposed solution: replace in 2 years time

- "Limited gain for attacker" because fraud can be detected and stopped within 2 days
- Individual fraud vs. business case for criminals

Back in 2001 (New Security Paradigms Workshop):

Information Security is Information Risk Management

Bob Blakley
Tivoli Systems, Inc.
blakley@us.ibm.com

Ellen McDermott
J.P. MorganChase

Dan Geer
@Stake

ABSTRACT

Information security is important in proportion to an organization's dependence on information technology. When an organization's information is exposed to risk, the use of information security technology is obviously appropriate. Current information security technology, however, deals with only a small fraction of the problem of information risk. In fact, the evidence increasingly suggests that information security technology does not reduce information risk very effectively.This paper argues that we must reconsider our approach to information security from the ground up if we are to deal effectively with the problem of information risk, and proposes a new model inspired by the history of medicine.

1. INFORMATION RISK

consequence of an event is the dollar amount of the reduction in business value which the event will cause if it occurs [Har]

1.2 Measuring Risk

A common measure of the cost of risk is "Annualized Loss Expectation," or ALE. ALE is the expected cumulative cost of risk over a period of one year as estimated in advance. For example, a chemical company estimates the probability of an explosion at one of its plants during the year 2001 as one in a million. If an explosion occurs, it will cost the company 150 million dollars in direct and indirect expenses, (for example, repair costs, legal costs, or lost business).

The ALE created by the risk of a plant explosion for the year 2001 is simply:

ALE= $15,000,000 x (1/1,000,000) = $150

The big question

- How do we evaluate which cyber security controls we should implement?
- Preventive, detective, responsive

Risk mitigation

- Wait until something happens
- Checklists
- Theoretical models
- Evidence-based models

Return on security investment: effectiveness & cost

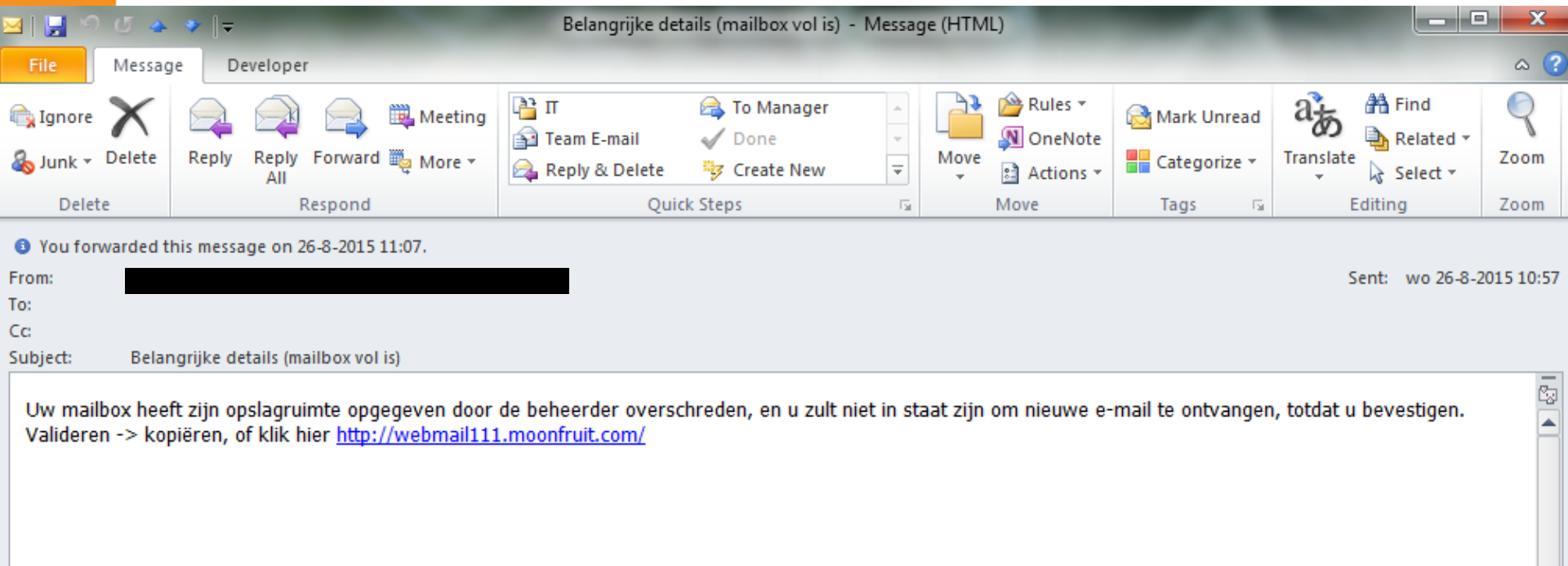
Traditional risk vs. adversarial risk

Attackers

- Cryptographic assumptions: attacker cannot perform prime factorisation efficiently
- Dolev-Yao: attacker controls the network, but cannot break crypto
- Game theory: attacker maximises his utility
- Goals, skills, resources, …

Scenarios / vulnerabilities

- Exploiting digital weaknesses
- Social engineering (e.g. phishing)
- Physical access



Possible controls

- More crypto
- Hardening / patching
- Locks / cards / biometrics
- Training

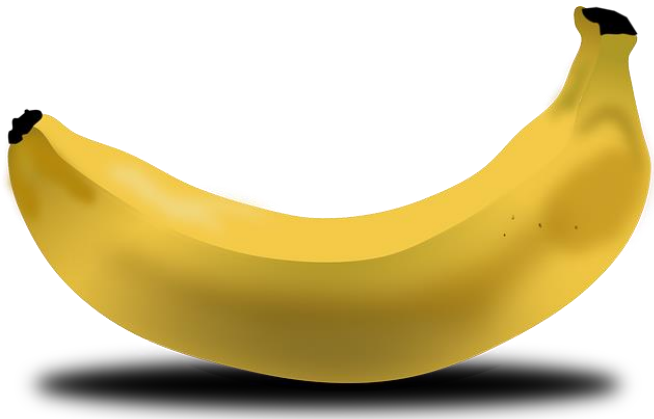
Factors

- How to combine system, attackers and possible controls in making security decisions?
- Can there be “evidence-based security” as there is evidence-based medicine?

Would you eat bananas?

"If you don't eat bananas, you might be robbed"

(Herley & Pieters 2015)



Key takeaways

- It’s not only about theoretical effectiveness of controls, but about their contribution to the system as a whole
- Interesting achievements and challenges in measuring and predicting such contribution
- See the upcoming courses!
- CRM course: http://homepage.tudelft.nl/e7x9k/CRM/