Markus Riek, Carlos Ganan

universität innsbruck

The Economic Impacts of Cyber Crime

D8.1 Cyber Risk Management

Framework and a sector-specific case study

Agenda

A. **Cyber risk management framework**

B. **Sector-specific remarks**

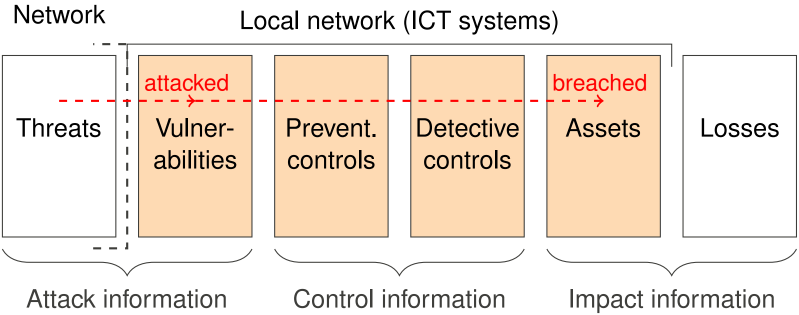
C. **Case study: Credit card fraud**

   A. **Motivation**

   B. **Research design**

   C. **(Preliminary) results**

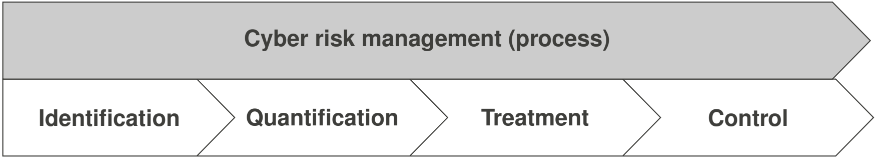
Cascade model of cyber risk arrival



- For a comprehensive risk management all information is required.
- Each risk factor (e. g. Threats) comprises a vector of risks.
- Risk factors are only partially under the control of the firm.

cf. Böhme et al. 2016. *A Fundamental Approach to Cyber Risk Analysis*, based on [Ransbotham and Mitra, 2009].

Risk management



Cyber risk management (process)

Identification

Quantification

Treatment

Control

- Checklists
- Attacktrees
- . . .

- Scenario analyses
- Monte Carlo Simulations
- . . .

- Risk avoidance
- Risk mitigation
- Risk transfer
- Risk acceptance

- Evaluation of decisions
- Documentation
- Reporting

Risk management frameworks

Top-down: structure the risk management process

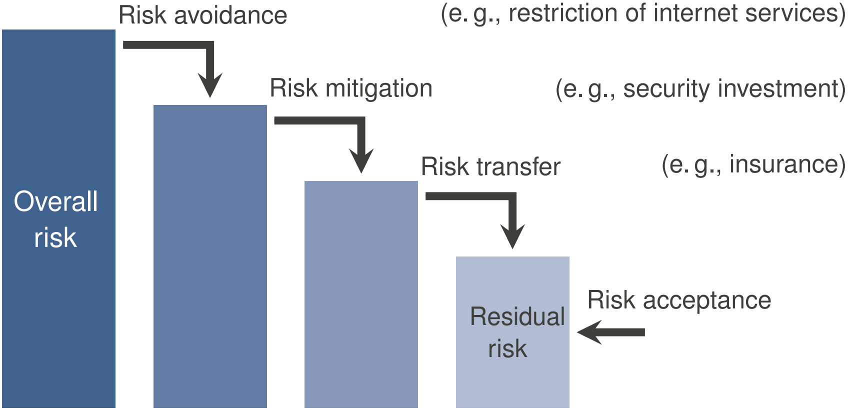
- ISO/IEC 27000-series of information security standards: ISO/IEC 27005 —-*Information security risk management*.
- NIST SP 800-30 – *Risk Management Guide for Information Technology Systems*

Bottom-up: identify risk factors

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) framework
- Factor analysis of information risk (FAIR) classification
- Vocabulary for Event Recording and Incident Sharing (VERIS)

[ISO/IEC, 2014, Stoneburner et al., 2002, Cebula et al., 2010, ISACA, 2009, Veris, 2016]

Cyber risk treatment



Cyber risk treatment highly depends on characteristics of each organization.

Cyber insurance as a tool for risk transfer

Problems preventing the growth of a cyber insurance market:

- **Lack of historic data** to calculate premiums
- **Information asymmetries:** inhibit the monitoring of policy holders
  - Adverse selection
  - Moral hazard
  - Insurance fraud
- **Dependent risks:** potentially causing catastrophic events
  - Interdependent security
  - Risk correlation

Increasing interest by insurers to develop the market.

Agenda

A. **Cyber risk management framework**

B. **Sector-specific remarks**

C. **Case study: Credit card fraud**

    A. **Motivation**

    B. **Research design**

    C. **(Preliminary) results**

E-CRIME sectors

- Financial
- Retail
- Transport
- Energy
- Health

Financial and Retail sectors

Selected key risks	Risk treatments
Loss, theft, or alteration of customer data, e.g. through hacking	*Risk mitigation*: hardened infrastructure, back ups; *Risk transfer*: outsourcing services.
Business interuption, through hacking, DDoS attacks or ransomware	*Risk mitigation*: employee trainings
Consumer-facing fraud, e.g. phishing, identity theft, or payment card fraud	*Risk mitigation*: fraud departments; *Risk avoidance*: avoiding market segments; *Risk acceptance*: e.g. for customer convenience

Customer interaction via the Internet imposes **inevitable risks** with various treatment alternatives.

Transport and Energy sectors

Transport:

Selected key risks	Risk treatments
Business interruption due to unavailable IT systems	*Risk mitigation*: network segmentation, code reviews
E-ticket fraud	*Risk avoidance*: avoid e-tickets;

Energy:

Selected key risks	Risk treatments
Business interuption and physical damage to systems	*Risk mitigation*: network segmentation, “air-gaps”, BYOD regulation

Business interruption is the major risk in both sectors.

Healthcare sector

Selected key risks	Risk treatments
Liabilities after data breaches	*Risk mitigation*: basic controls; *Risk transfer*: high demand for cyber insurance.
Interruption of health care systems	*Risk mitigation*: employee trainings; *Risk acceptance*: to not interfere with work processes.

Liabilities are an emerging problem, cyber insurance might be a viable treatment option.

Summary sector-specific risk assessment

Findings across sectors:

- Businesses in all non-ICT sectors rely increasingly on their ICT systems. **Business interruption** is a key risk across sectors.
- **Cyber insurance** as a means for cyber risk transfer is not widely adopted yet. The health sector is promising.

Limitations of sector-specific risk assessment:

- Organizations in a single sector are still very heterogeneous and face a large variety of risks.
- Organizations use all risk treatment alternatives in different contexts.

Identifying key risks and suggesting treatment options on the sector level is difficult.

Agenda

A. **Cyber risk management framework**

B. **Sector-specific remarks**

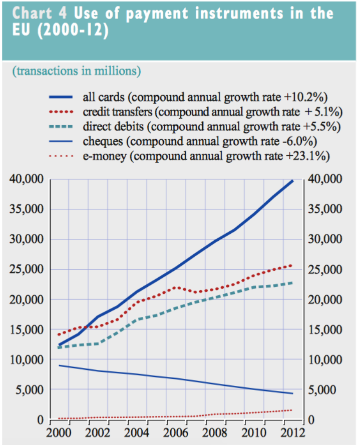
C. **Case study: Credit card fraud**

   A. **Motivation**

   B. **Research design**

   C. **(Preliminary) results**

Credit cards as a target for criminals

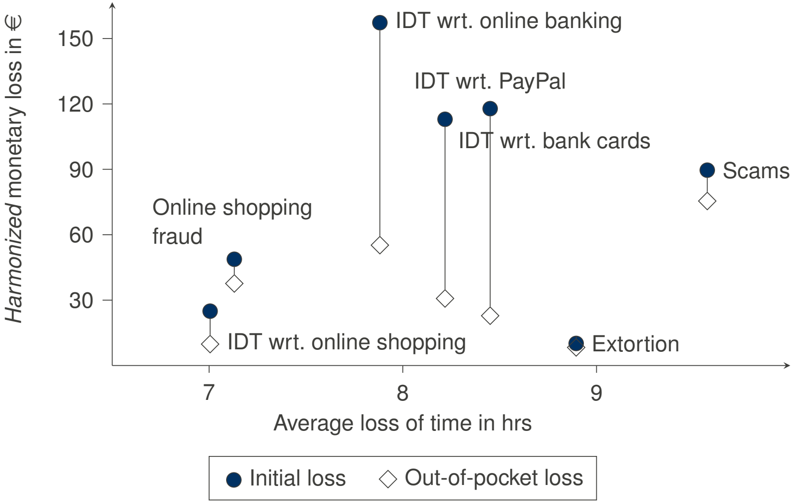


[ECB, 2014]

Observations of credit card (cc) fraud:

- **Public data breaches**, e. g. 56m. cc numbers stolen at Home Depot. Such breaches are likely to occur [Edwards et al., 2016].
- **Trading on black markets**: 100 490 unique cc numbers by monitoring IRC chats for 7-month [Franklin et al., 2007].
- **Victimization surveys**: 4.8% of UK Internet users (3.5% in Germany, 2.7% in Italy, . . .) [Riek et al., 2016].

Costs for the victims



High compensation payments by financial service providers.

E-CRIME WP4 & WP6, [Riek et al., 2016]

Direct costs for the credit card issuer

+ Charge-backs (which cannot be transferred to the merchant)

+ Issuing a new credit card

+ Communication with the customer

+ Opportunity costs (if victims do not use the new credit card)

= Total costs for the issuer

Potential opportunity costs:

- Victims do not use their new credit card
- Victims change to other payments methods

Risk management requires quantification of the costs of a fraud incident.

Related work

Cross-sectional surveys:

- 8% of Home Depot customers (8% Target) reported to have stopped using their credit card after the data breaches [Stanton, 2015].
- $>$50% of German credit card owners reported to use other payment methods after experiencing credit card fraud [Inscoe, 2012, 2014].
- In 2014, 22% of victims reported, that they do not use the replacement card (36% in 2012; [Inscoe, 2012, 2014]).

Academic studies:

- Cybercrime experience and perceived risk of cybercrime lead to avoidance of online services [Riek et al., 2015].
- Costs of automatically reissuing cards seems to be higher than waiting until fraud is attempted [Graves et al., 2014].

Missing pieces: Actual behavior of victims in a clearly defined context.

Agenda

A. **Cyber risk management framework**

B. **Sector-specific remarks**

C. **Case study: Credit card fraud**

   A. **Motivation**

   B. **Research design**

   C. **(Preliminary) results**

Study

PLUS CARD

Menschen. Karten. Strategien.

ecrime

The Economic Impacts of Cyber Crime

Cooperation with **PLUSCARD**:

- German credit card processor
- E-CRIME stakeholder

- **Victims of credit card fraud** are approached immediately after an incident and asked to participate.
- Data is collected with standardized **telephone interviews** and monitoring of **financial transactions**.
- Fieldwork started in December 2016 and is still on-going (preparations since late 2015).

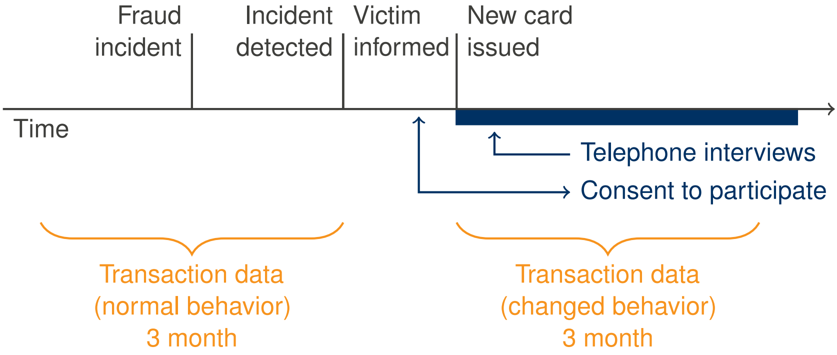
Contribution

Empirical studies of victim behavior after fraud incidents:

Use of . . . after incident	**Self-reported**	**Actual behavior**
Online shopping	Riek et al. [2015]	(✓)
Credit card online	Inscoe [2014]	✓
Credit card offline	Stanton [2015]	✓
Other payments online	Inscoe [2014]	
Other payments offline	Stanton [2015]	
Use of . . . before incident		
Online shopping	✓	(✓)
Credit card online	✓	✓
Credit card offline	✓	✓
Other payments online	✓	
Other payments offline	✓	

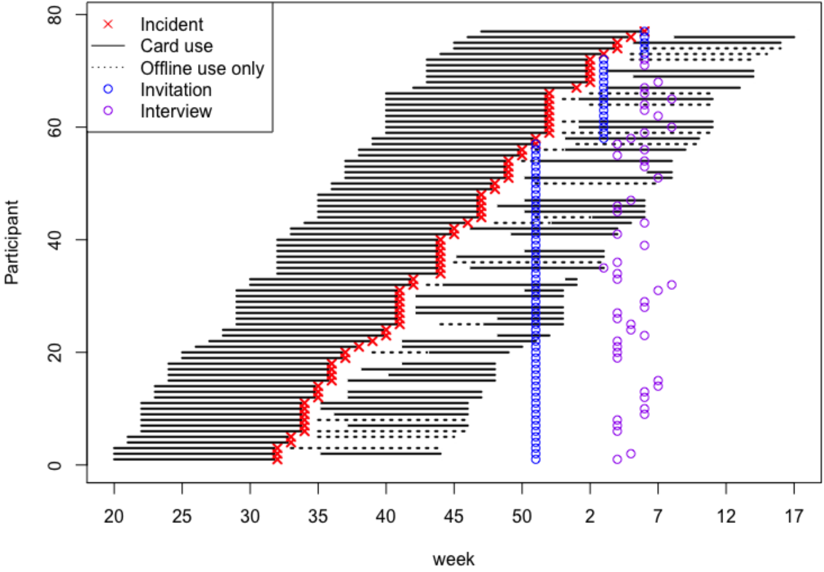
Research design

Natural experiment integrated into each fraud case:

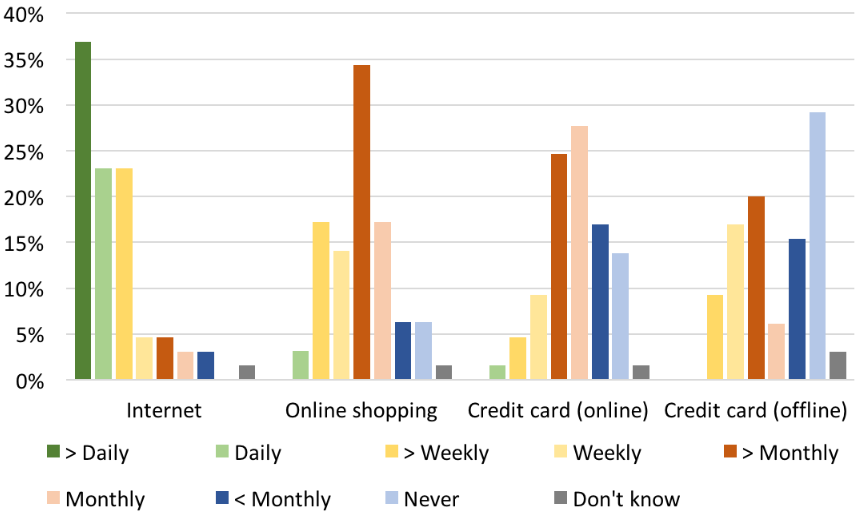


- **Telephone interviews**: self-reported behavior, perceptions
- **Actual behavior**: aggregated transactions before & after the incident

Time line of the (on-going) field work

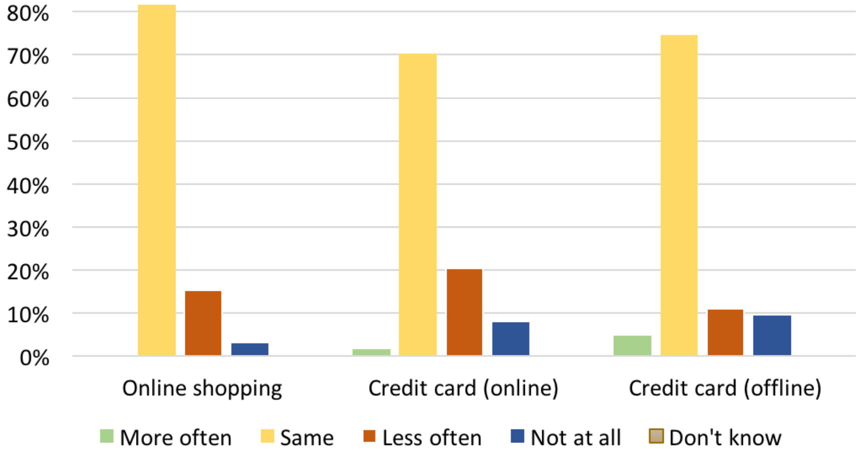


Self-reported use statistics



Base: 65 interviewed victims.

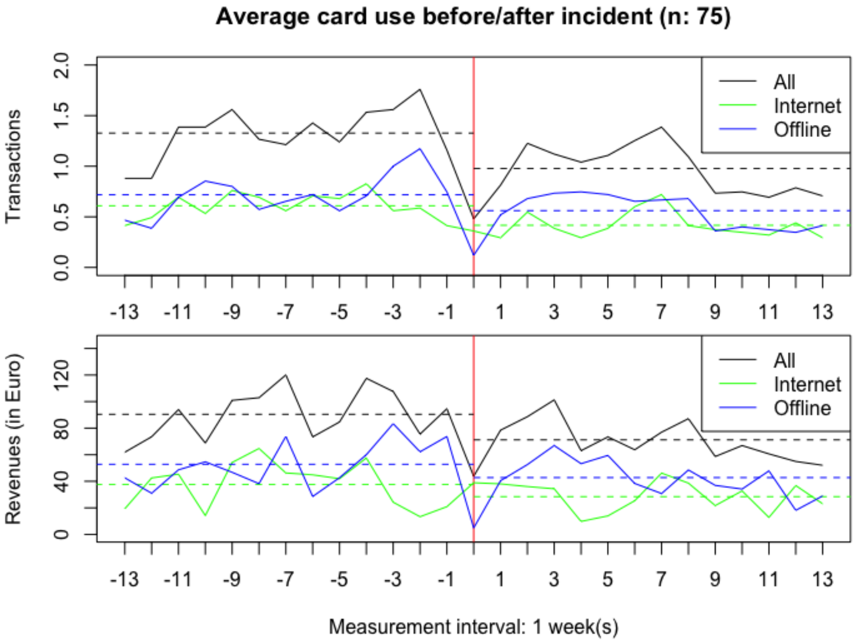
Use intention in the future



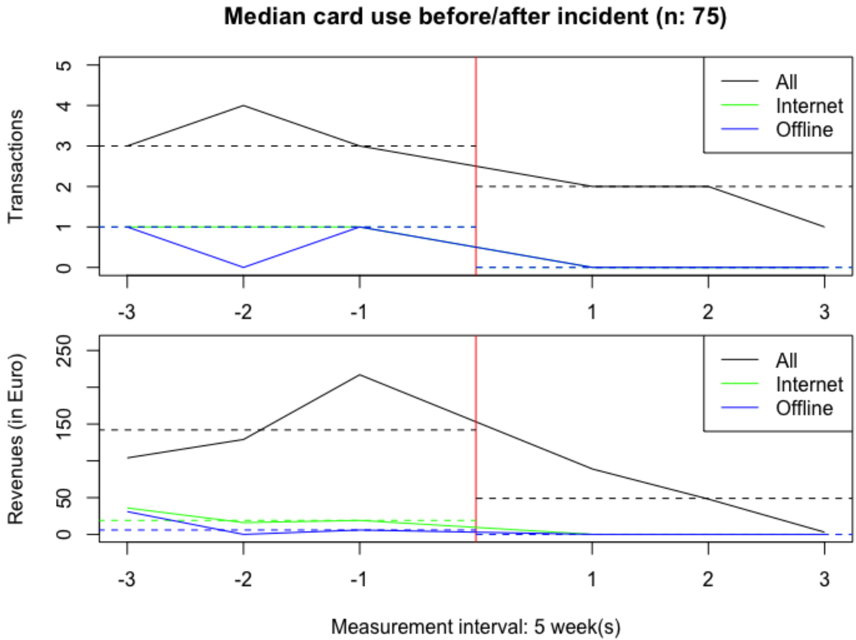
28% of victims intend to use their credit card less online (21% offline)

Base: 65 interviewed victims.

Visual analysis of the interrupted time series (1)



Visual analysis of the interrupted time series (3)



Summary of (preliminary) results

Use of . . . after incident	**Self-reported**	**Actual behavior**
Online shopping	18% intend less	(Av.m.R.: 115€)
Credit card online	28% intend less	Av.m.T.: 1.7
Credit card offline	21% intend less	Av.m.T.: 2.3
Other payments online	30% switched	
Other payments offline	10% switched	
Use of . . . before incident		
Online shopping	34% weekly	(Av.m.R.: 157€)
Credit card online	15% weekly	Av.m.T.: 2.5
Credit card offline	26% weekly	Av.m.T.: 3
Other payments online	40% prefer PayPal	
Other payments offline	57% mostly cash	

Av.m.T.: Average **m**onthly **t**ransactions, **Av.m.R.: Av**erage **m**onthly **r**evenue

Additional insights

From the complete data set:

- Sophisticated interrupted time-series models, e. g. ARMA.
- Quantification of opportunity costs.
- User group analysis comparing *frequent* with *non-frequent* or *primarily online* with *primarily offline* users.

From the telephone interviews:

- Direct and indirect costs for the victims, including time.
- Victim’s attitudes towards different payment methods.
- Indirect security costs through new 2-factor auth. methods.

Results will be made available when the data collection is complete.

Sources I

J. J. Cebula, M. E. Popeck, and L. R. Young. A taxonomy of operational cyber security risks. Technical report, Software Engineering Institute, 2010.

ECB. Card payments in europe ? a renewed focus on sepa for cards. Technical report, European Central Bank (ECB), 2014. URL `https://www.ecb.europa.eu/pub/pdf/other/cardpaymineu_renfoconsepaforcards201404en.pdf`.

B. Edwards, S. Hofmeyr, and S. Forrest. Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, page tyw003, 2016.

J. Franklin, A. Perrig, V. Paxson, and S. Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pages 375–388, New York, NY, USA, 2007. ACM. doi: 10.1145/1315245.1315292.

J. Graves, N. Christin, and A. Acquisti. Should payment card issuers reissue cards in response to a data breach? In *WEIS: Workshop on the Economics of Information Security, 2014*, WEIS '14, 2014.

Sources II

S. W. Inscoe. Global consumers react to rising fraud: Beware back of wallet. Technical report, Aite Group, 2012. URL `https://www.aciworldwide.com/-/media/files/collateral/trends/aci-aite-global-consumers-react-to-rising-fraud-1012.pdf`.

S. W. Inscoe. Global consumers: Losing confidence in the battle against fraud. Technical report, Aite Group, 2014. URL `https://www.aciworldwide.com/-/media/files/collateral/trends/2014-global-consumer-fraud-survey---part-1and-2.pdf`.

ISACA. The risk IT framework excerpt. Technical report, Information Systems Audit and Control Association (ISACA), 2009.

ISO/IEC. ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary. Standard, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), 2014.

Sources III

S. Ransbotham and S. Mitra. Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, 20(1):121–139, 2009.

M. Riek, R. Böhme, and T. Moore. Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 2015.

M. Riek, R. Böhme, M. Ciere, C. Gañán, and M. J. G. van Eeten. Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries. In *Workshop on Economics of Information Security (WEIS)*, University of California, Berkeley, CA, USA, 2016.

J. Stanton. Payment card data breaches: How does the consumer respond? Technical report, 2015.

G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical report, National Institute of Standards and Technology (NIST), 2002.

Veris. Vocabulary for Event Recording and Incident Sharing. Technical report, Veris, 2016.