How companies *manage* their security

Introduction into Information Security Management Systems (ISMS)

Tilman Runge

About this talk

- Tilman Runge
- In-house Information Security Officer
- Trained Clinical Psychologist

Why this talk:

- Get an insight into what companies don‘t talk about publically
- Learn about ISMS and how they work
- Security in ISMS: Property versus Process
- Job info: Chief Information Security Officer

FlySlow Airlines

- They fly people for money
- They have no concept whatsoever how to avoid IT-related incidents
- But they don‘t want to go bankrupt because…
  - … a ransomware trojan infected their check-in terminals
  - … they did not use redundant database servers and now lost their flight schedule
  - … their contractor for payments was hacked and all payments got redirected
  - … an angry employee deleted all bookings

- How does FlySlow think about all possible scenarios leading to their demise and also react apriopriately?

Lecture Contents

Introduction:

- Terms and basic concepts with ISMS
- What is an ISMS and why would you need it?
- Relevant persons doing the ISMS
- What is Information Security [in your organization]?

Part 1: Asset Management and Risk Analysis

- Determine the „mission“ of our organization
- Determine the relevant threats to our mission
- Draw conclusion about risks → know which risks to fix

Part 2: ISO27001 specifics

- Management-Reviews
- Documentation
- Audits and Certification

Terms

Organization

- company, public authority, government department, non-governmental organization (NGO), political party
- in this talk: all terms used interchangeably

Assets

- Everything that is part of making the organization work such as computers, IT-infrastructure, information, processes, external service providers, buildings, employees, money, properties

Information Security

- like IT-security but includes assets, that are not part of IT-security
- in this talk: IT-security = Information Security

Information Security Management System (ISMS)– WTH?

But what is this *Information Security*?

… more all-encompassing conception which includes IT-security, for example:

Thieves break into your server and steal your business expansion plans

↓

Matter of IT security (insecure configuration enabled easy access)

Your business expansion plans are lying printed on paper in your office. Thieves break in and steal them

↓

Matter of Information Security (your confidential data is no longer confidential even though it is not an IT issue/vulnerability)

Information Security Management System (ISMS)– WTH?

SMSI: A System to Manage the Security of Information

Why do you need that?

- If you want a structured approach that also fits into management thinking or in other quality management systems (ISO9001)
- Managing large organizations (e.g. VW, Deutsche Bahn, Bundestag)
- Legal requirements
  - KRITIS: IT-Sicherheitsgesetz
  - General Data Protection Regulation (GDPR) / EU-DSGV
- Customer requirements

Large scale security in a company like German Railway

Security incidents are not a question of IF or WHEN but HOW OFTEN

Example: How would a company the size of the German Railway deal with phishing incidents?

- employees: 300.000
- phishing mails per employee and year: 3
- employees convinced by phishing email: 7%
- security incidents due to successful phishing (300.00*3*0,07): 63.000

→Countermeasure: install mail filter and educate 300.000 employees to spot phishing emails

- phishing mails per employee and year after installation of mail filter: 0,1
- employees convinced by phishing email after training: 0,2%
- still 60 security incidents due to successful phishing

No 100% security possible. Better: Resiliency against threats

ISMS: Main Goals

Main goals:

1) We want to keep the business/organization running (=profitable/achieving its goals)
   - We need to define what threats are relevant → Risk Analysis
2) We want to distribute resources for redundancy appropriately
   - We need to know which system(s) may never fail → Business Impact Analysis
3) We want to create accountability for our IT-system
   - We need to describe operational procedures, policies, requirements, rules
   - We need to verify ("audit") that these operational procedures, policies, etc. are:
     - In place (=everyone follows the rules)
     - Useful (=they help us achieve our goals)
   - We may need to prove the existence & functioning to third parties (government, customers) by having the ISMS certified

Relevant People in ISMS

- (Chief) Information Security Officer (CISO)
  - Situated in management. Reports directly to the CEO, has no other superiors
  - Training: No particular
- Data Privacy Officer (DPO)
  - Situated equally. In Germany DPO is legally protected
- Head of IT
  - System administrators
  - Software developers
- Employees/members of the organization
- External service providers

But What is this Information Security?

… you get to define it in the context of your organization:

- **C as Confidentiality**: Your data stays private (no unauthorized access)
- **I as Integrity**: Your data stays consistent (no unauthorized change)
- **A as Availability**: Your data stays available (no burned down datacenter)

But wait, there‘s more:

- **Authenticity**: The email really is from Paypal (and not a phishing email)
- **Privacy**: Your Personal Information stays private
- **Thrustworthiness**: The .docx-document does not contain a virus

Define your Information Security Goals: Confidentiality

	Airline	Social Network	Political Party	Electricity Company	Your organization
What is the objective?	Fly people, earn money.	Connect people, earn money.	Represent interests, get elected.	Produce energy, earn money.	
Incident example:	Japan Airlines frequent flyer club leak		Email leak of Democrats in US election		
Worst case if security goal fails	- Passengers‘ travel data becomes public - Passengers‘ passwords become public, can be reused on other sites	- All your private messages and pictures are public now. You stop using $socialnetwork	Democrats loose credibility and popularity, helps Trump to get elected.	- Everyone can read the internal network plans of the powerplant	
Rating	2/5 Low, company objective not seriously endangered	5/5 High, likely to be existentially threatening	4,5/5 High, can be existentially threatening	2/5	

Define your Information Security Goals: Availablility

	Airline	Social Network	Political Party	Electricity Company	Your organization
What is the objective?	Fly people, earn money.	Connect people, earn money.	Represent interests, get elected.	Produce energy, earn money.	
Incident example:	British Airways IT outage 2017		Loss of member database	Ukraine power grid cyberattack	
Worst case if security goal fails	- All flights cancelled - 14 days needed to reinstate regular schedule - 150 million British Pounds financial damage	Users cannot access service. Some users store critical data they now cannot access.	Party does not know anymore who their members are	¼ million people without electicity for several hours	
Rating	4,5/5 High, income decreased by 15%	1/5 Low, users likely to return anyway	3/5 Medium	5/5 Presumable act of cyber warfare	

Define your Information Security Goals: Integrity

	Airline	Social Network	Political Party	Electricity Company	Your organization
What is the objective?	Fly people, earn money.	Connect people, earn money.	Represent interests, get elected.	Produce energy, earn money.	
Incident example:	Database corruption after check-in	Database corruption			
Worst case if security goal fails	After checking in your luggage the database crashes: Now your luggage is gone but the airline has no record of it	Due to database corruption your private pictures are now visible in someone else‘s Snapchat		Malfunctioning controller firmware causes generator to break down	
Rating	4/5 medium, data inconsistency is hard to resolve	4/5 High, can be existentially threatening		5/5 High, posibility of destruction of critical infrastructure	

Information Security Goals: Summary

	Airline	Social Network	Political Party	Electricity Company	Your organization…
Confidentiality	2	5	4,5	2	
Integrity	4	4	5	5	
Availability	4,5	1	3	5	

Conclusion:

- What Information Security means depends on the organization‘s context
- Information Security Goals relate to your Information Security Threats
- Don‘t start doing things (patching, backing up, encrypting) unless you have a plan *what* shall be achieved and *how*

Risk Analysis and Asset Management

But how to create such a plan?

→ Use an Asset Management, Risk Analysis and Risk Relevance Analysis

- **Asset Management**: Tells us which assets we have and how vulnerable they are and how they relate to our business processes
- **Business Impact Analysis**: Tells us, which level of disruption each business processes may endure
- **Risk Relevance Analysis** (threat*probability): Tells us which threats are relevant for our business goals
- **Risk Analysis** (threat*probability*asset): Tells us for each business process which threats exist and how bad they are
- **Risk Management**: What will we do how against the risks?

Example: FlySlow Airlines

- They fly people for money
- They have no concept whatsoever how to avoid IT-related incidents
- But they don‘t want to go bankrupt because…
  - … a ransomware trojan infected their check-in terminals
  - … they did not use redundant database servers and now lost their flight schedule
  - … their contractor for payments was hacked and all payments got redirected
  - … an angry employee deleted all bookings

- How does FlySlow think about all possible scenarios leading to their demise and also react apriopriately?

Business Impact Analysis: FlySlow Airlines

Business Processes	Longest, still acceptable loss of availability	Assets that are required for this Business Process to function
Flight booking	24 hours	• Booking database • Flight schedule database • IT-Infrastructure • Payment system
Flying	6 hours	• Flight schedule database • Booking database • IT-Infrastructure • Airplanes
Complaint handling	12 months	• Customer database • Flight schedule database • Flight history database • Payment system • Complaintment-Office

Assets	Availability Requirements
Flight schedule database Booking database IT-Infrastructure Airplanes	6 hours
Payment system	24 hours
Customer database Complaintment-Office Flight history database	12 months

Asset Management: FlySlow Airlines

Asset class	Assets
Assets: Objects	Airplanes Complaintment-Office IT-infrastructure (webpage, databases, servers)
Assets: Information	Booking database Customer database Flight schedule database Flight history database
Assets: other	Payment service provider

Security Goal	Levels
Confidentiality	• public • internal use only • confidential
Integrity	• Corruption acceptable • Corruption may be acceptable • Corruption unacceptable
Availability	• Months(s) • Week(s) • Day(s) • Hour(s)

Risk Relevance Analysis: FlySlow Airlines

Business Process	Flight booking			Flying			Complaint handling		
Threat	**Damage**	**Probability**	**Risk**	**Damage**	**Probability**	**Risk**	**Damage**	**Probability**	**Risk**
Fire	medium	low	**medium**	medium	low	**medium**	medium	low	**medium**
Natural Catastrophe	medium	very low	**low**	medium	very low	**low**	medium	very low	**low**
Power loss	medium	medium	**medium**	high	medium	**high**	medium	medium	**medium**
Internet loss	medium	medium	**medium**	high	medium	**high**	medium	high	**high**
Spying	medium	medium	**medium**	medium	low	**medium**	medium	low	**medium**
Manipulation	high	medium	**high**	high	medium	**high**	medium	medium	**medium**
Trespassing	very low	very low	**very low**	very low	very low	**very low**	high	medium	**high**
Abuse of rights	high	medium	**high**	medium	medium	**medium**	medium	medium	**medium**
Malware	medium	low	**low**	high	medium	**high**	medium	high	**high**
Denial of Service	high	medium	**high**	medium	medium	**medium**	medium	medium	**medium**
Release of radiation	very low	very low	**very low**	high	very low	**medium**	high	very low	**medium**

Asset Management: FlySlow Airlines

- We have determined „what we do“: Flying people, earn money
- We have defined Information Security Goals to get #1 done
- We have determined which things („assets“) enable #1
  - Processes (flight booking, flying, complaint management)
  - Objects (IT-infrastructure, airplanes, buildings, …)
  - Information (customer database, flight database, …)
- We have determined which assets we need to „do what we do“

- Implemented protective measures

Part 2: Other ISO27001-related aspects

- ISO27001 and ISO27002
- Management Review
- Documentation
- Audit
- Certification

Inside ISO2700/ISO27001/...

ISO27001: The Standard

- Defines an ISMS and defines required processes such as:
- Audits
- Management Reviews
- Risk Analysis
- Circular improvement (Plan-Do-Check-Act)

ISO27002: The Controls

- (Binding) implementation recommendations:
- A9.4: Implement Secure Log-On
- A10: Use of Cryptography
- A12.3: Make Backups
- A16.1: Identify Security Incidents
- A17.1.1: Create Emergency Plans

Tip: Search „ISO27001 translated into plain English“

ISMS: Documentation

Policies

Exist on various levels:

- Top-level policies are the management‘s declaration of intend towards Information Security, giving relevant actors (CISO, DPO, …) all the power they need
- Mid-level policies already include technical language but are still abstract („No password may be transfered unencrypted at any time“)
- Low-level policies/codes of behavior describe very specific ways how users must and must not use a system („Do not re-use passwords“)
- Technical documentation
- Policy creation depends upon level.

Proof your ISMS exists

External auditors/certification bodies/clients also want to see that your ISMS is real and not just advertisement.

Document everything done as part of the ISMS:

- Audit reports, auditing plans, fulfilled auditing plans,
- Improvement measures (system hardening, penetration tests, risk analysis, code refactorization, external support)
- Incidents
- Emergency Management Exercises

Management Reviews

The part where the management learns about reality:

- The Chief Information Security Officer responsible for reporting to the management, topics of interest include:
  - internal & external audit reports
  - how we deal with our risks
- The management itself is responsible for
  - Green-lighting/accepting risks OR taking action
  - Approving changes in IT-policies
  - Approving of the general state of the ISMS

ISMS: Audits to compare ‚ought to‘ and ‚is‘

Internal Audits

- Are conducted by someone within the organization: CISO, internal auditor, Admin, Developer, Data Privacy Officer
- Some parts are hard to audit (secure passwords)

Advantages:

- Uncomplicated, easy & cheap to conduct

Disadvantages:

- Neutrality issue: There may be a conflict of interest between the person auditing

External Audits

- Conducted by external service provider

Advantages:

- Neutral instance looking at your ISMS
- Usually an external ISMS contractor
- Required as part of certification process

Disadvantages:

- External auditors don‘t know your IT in detail and therefore will overlook issues
- If you want, you can hide things that are not going well
- Expensive

Certification of ISMS

You can have your ISMS certified. Why?

- Legal requirement(s)
- Customer requirement(s)

Two certifications possible:

- IT-Grundschutz: ISMS published by German BSI (Federal Office for Information Security)
- ISO/IEC 27001:2013

What DOES it not DO?

- Does not guarantee security
  - Not even if certified
  - Certification scope very relevant (“We certified cleaning the bathrooms”)
- Does not give you 100% security
- Does not (necessarily) cost less money
- There is no success guarantee
- ISMSs do not make insecure software go away

ISMS: Conclusion

- Security is not state but a process
- „We are 100% secure“ versus resiliency
- Lifecycle/circular process
- Helps you adapt to YOUR threat model

Thanks for listening

contact: $lastname@mailbox.org