ERNW
Living Security.

Rapid Risk Assessment

Enno Rey
erey@ernw.de

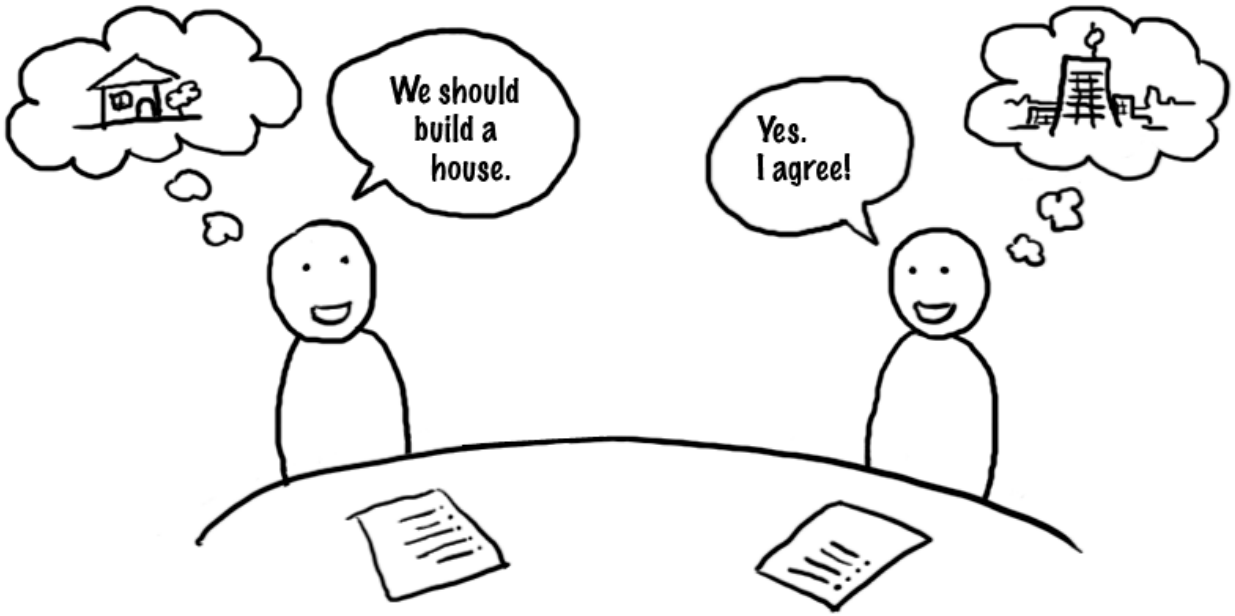
Who I am

- **Old-school infosec guy & founder of**
- **Germany based ERNW GmbH**
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- **Blog: www.insinuator.net**
- **Conference: www.troopers.de**

Agenda

- **Terms & Definitions**
- **Benefits and obstacles in corporate life**
- **Room for improvement**
- **Where's RRA different?**
- **Case studies**
- **Lessons learned**

Risk



Risk has different meanings for different people…

Initially, a very simple definition

ERNW
Living Security.

- **“Exposure to loss”**

[http://risktical.com/2008/07/31/what-is-risk/]

A more complex definition

ERNW Living Security.

„The **probability** of a **threat** overcoming **security controls resistance** to **exploit** a **vulnerability** that results in a **loss**“

[http://risktical.com/2008/07/31/what-is-risk/]

Overall good definition, but too complex for our needs.

ISO 27005

ERNW Living Security.

"information security risk

potential that a given **threat** will exploit **vulnerabilities** of an asset or group of assets and thereby cause **harm** to the organization.

NOTE It is measured in terms of a combination of the likelihood of an event and its consequence."

ISO/IEC GUIDE 73:2002

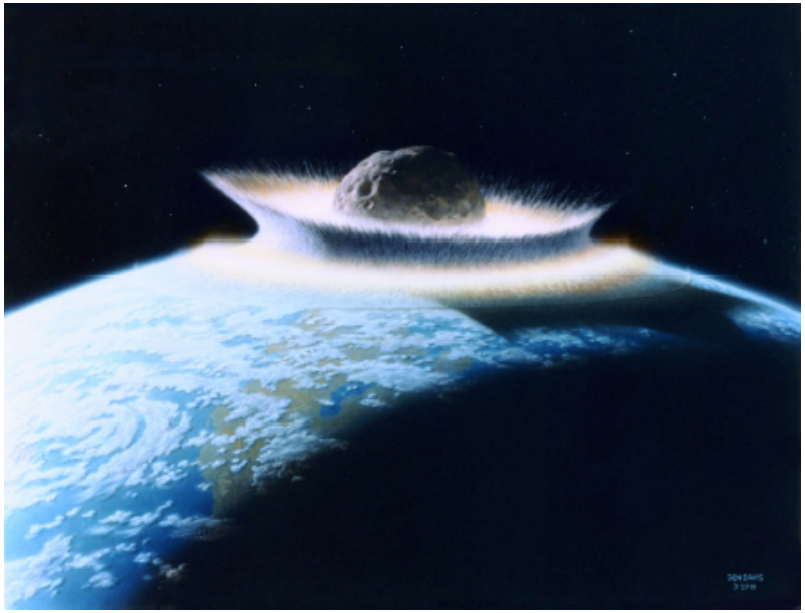
Event = occurrence of a particular set of circumstances

Consequence = outcome of an event

Difference between *threat* and *risk*... pls explain...

ERNW Living Security.

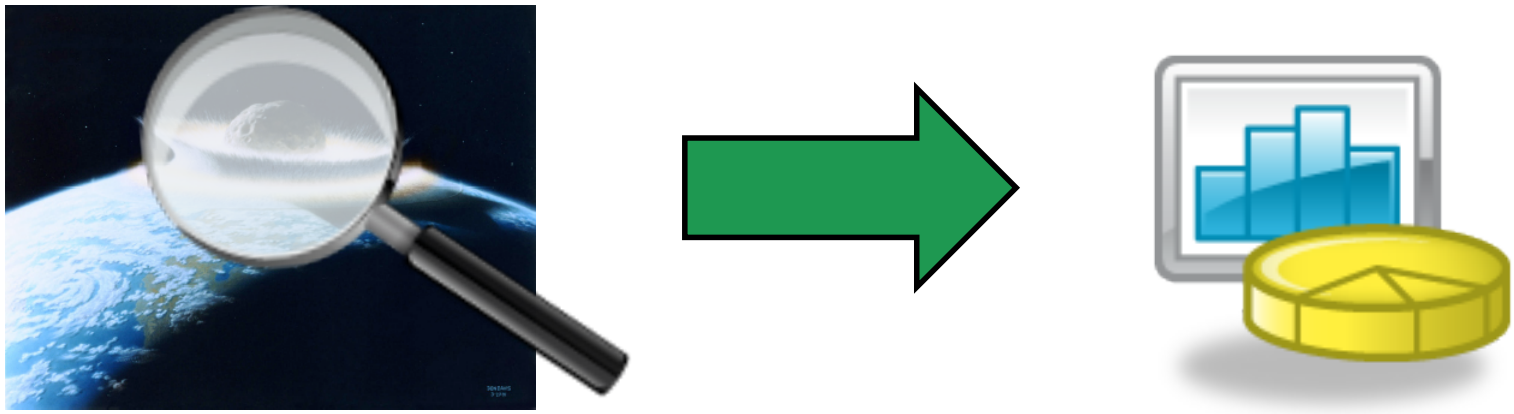
- **Threat: something bad that can happen**
  - **Regardless of relevance**
    - **Meteorite hitting planet earth**



Difference between *threat* and *risk*... pls explain...

ERNW Living Security.

- **Risk: threat "viewed by some dimensions"**
  - **How likely is it going to happen? [*Probability*]**
  - **Are we susceptible if it happens? [*Vulnerability*]**
  - **What harm is caused in case it hits us? [*Impact*]**



- **Talking about *threats* does not make too much sense**
  - **At least in corporate infosec context…**

ISO/IEC GUIDE 73:2002 on *Risk Analysis*

ERNW Living Security.

"Systematic use of information to identify **sources** and to estimate the **risk**".

Source: item or activity having a potential for a **consequence**

- Risk analysis provides a basis for **risk evaluation**, **risk treatment** and **risk acceptance**.
- Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.

Methods & Tools

ERNW Living Security.

- ***Quantitative* vs. *Qualitative***
  - **In IT/infosec usually qualitative approach used.**
- **Quite a number of methods available**
  - **OCTAVE, ISAMM, MEHARI et.al.**
- **Quite a number of supporting tools around**
  - **E.g. CRAMM**

- **See also: http://rm-inv.enisa.europa.eu/rm_ra_methods.html**

Main “Standard” (nowadays, since ‘08)

ERNW
Living Security.

INTERNATIONAL STANDARD

ISO/IEC 27005

First edition
2008-06-15

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion du risque en sécurité de l'information

Benefits of Performing RA

- **Communication!**
  - **Which is always a good thing.**
  - **Make participants aware of threats & – more importantly – risks.**
  - **Usually some "I never thought of this" moments…**
  - **We sometimes call this "discussion mode".**

- **Basis for decision taking / moving forward**
  - **By "answering a question"**
    - **→ Appropriate question is key!**
  - **If RA is prescribed as part of infosec process, we sometimes call this "governance mode".**

More Benefits

- **Document process (of decision taking).**
- **Hold parties involved accountable.**
  - **→ Right mix of “people with authority” needed then.**
- **ISO 27001 mandates for risk assessment ;-)**

Examples of “The Question“

ERNW Living Security.

What’s the current state of risks in our environment?

- **Usually part of a (corporate) risk management process.**
- **Performed periodically (e.g. every 12 months).**
- **Uses threats from threat catalogue**
  - **→ always the same, generic threats.**
- **We sometimes call this *inventory mode*.**

- ***Does the risk landscape shift if some change happens?***
  - **Technology/architectural change (e.g. virtualization).**
  - **Organizational change, e.g. outsourcing.**
  - **In most cases, threats from a catalogue do *not* make sense.**

Refresher

- **“Discussion Mode”**
  - **Goal: structure and progress discussion.**
  - **(Initial) Result serves as input for ongoing debate.**
  - **Open for modifications during exercise (threats etc.)**

- **“Governance Mode”**
  - **Goal: *end discussion* (→ “produce final result”).**
  - **Result serves as input for decision-taking process/step.**
  - **Usually time-constrained**
    - **Assumptions agreed on beforehand**
    - **No new threats allowed during exercise**

All this sounds nice and well...

ERNW
Living Security.

… but – given the (obvious) benefits and the ISO 27001 mandate – why the hell doesn't everybody do this on a daily basis ?!?!

Common problems

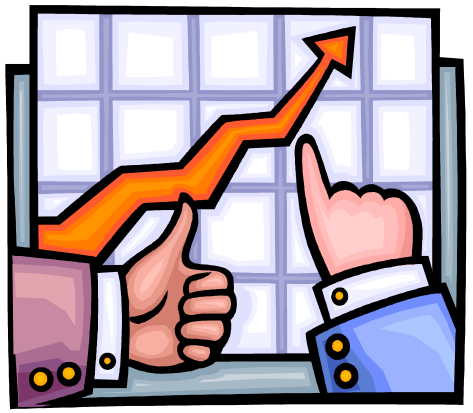
ERNW Living Security.

- **Resource and time constraints.**
- **People striving for the “holistic big hit”.**
- **People confusing (discussion|inventory|governance) mode**
  - **→ lack of rights tools for right purpose.**
  - **E.g. threat catalogue based approach might not make sense in governance mode.**

Critical Success Factors (*Gov_Mode*)

ERNW Living Security.

- **Essentially, it's only one:**



- **Practicability !**

- **Missing to "deliver result" (→ "answering the question") in a timely manner will render whole effort useless.**
  - **This is exactly what happens in many organizations.**
- **Avoid "academic discussions", but (& just) *agree*!**

Intro to Rapid Risk Assessment

ERNW Living Security.

- **Approach to perform *governance mode* RAs.**
- **In a timely manner.**
- **Uses quite common approach (see below)**
  - **→ No *rocket science*.**
  - **However, does *not* work with generic threats.**
    - **Some degree of experience and maturity needed.**

RRA, Goals

ERNW Living Security.

- **Clear, concise methodology to**
  - Perform risk assessments
    in a quick manner
  - Answer a question!
    - → Question has to be formulated in advance

- **Facilitate the process of well-informed decision taking**
  - → *Governance Mode*

It's all Rs…

ERNW
Living Security.

- **Rapid!**
- **Relevant Risks**
- **Repeatable**
- **Business Reasonable**

ISO 27005 suggests…

ERNW Living Security.

- **(… what many practitioners have been doing before)**
- ***Qualitative* risk assessment**
  - **Not based on detailed numbers, but on some scale**
  - **Scale usually 1 (very low) to 5 (very high)**
- **Three factors "contributing to risk"**
  - **Probability of an event**
  - **Vulnerability (of asset, in it's context)**
  - **Impact**

It looks like...

ERNW Living Security.

Threats	Probability	Vulnerability	Impact	Risk
Attacker with physical access to device trying to get unauthorized network access.	3	2	3	18
Malware grabs authentication data.	5	2	4	40
Seed distribution (intentionally) intercepted / misdirected (human failure).	2	1	4	8
Man-in-the-middle attack against data channel.	4	2	4	32

Probability

- **Usually scale from 1 (very low) to 5 (very high)**
- **In most cases scale has to be defined, e.g.**
  - **1: less than once in half of system's lifetime […]**
  - **5: more than once a week**

- **Generally, try to *not* consider existing controls**
  - **If asset not susceptible to event materializing… good for you, but that's part of (then low) "vulnerability"**
    - **People "knocking on datacenter's door" → probab.**
    - **Biometric AC prohibiting them from entering → vul.**

Vulnerability

Threat	Vulnerability
Trap	Desire for cheese and a wimpy neck
Theft	Open door and no security guard
Information Disclosure	Clear-text transport in public networks
Unauthorized access	Weak authentication

Threat:

> "A threat has the potential to harm assets such as information, processes and systems and therefore organizations."
> (ISO 27005)

Vulnerability:

> A "vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it."

Some Notes on *Vulnerability*

ERNW Living Security.

- **Usually this is the factor “that you can influence”**
  - **→ This is “the important one”!**

- **For some threats differentiating between *probability* and *vulnerability* might not be easy.**
  - **Usually applies to “abstract / organizational threats”**
    - **E.g. “Loss of change control accuracy”**
  - **Still, mostly this is not too much of a problem for RA**

Rating *Vulnerability*

ERNW Living Security.

- **Try to answer/understand "overall picture" of asset being susceptible to threat, including exposure, controls etc.**

- **Possible scale:**
  - **1: Extensive controls, threat can only materialize if multiple failures coincide.**
  - **2: Multiple Controls, but highly skilled+motivated attacker *might* overcome those.**
  - **3: Some control(s) in place, but highly skilled+motivated attacker *will* overcome those. Overall exposure might play a role.**
  - **4: Controls in place but they have limitations. High exposure given and/or medium skilled attacker required.**
  - **5: Maybe controls, but with limitations if at all. High Exposure and/or low skills required.**

Impact

ERNW Living Security.

- **Some debate “out there” on splitting impact into (at least) three pieces (usually *Availability*, “*CI*”, *Compliance*)**

- **For sake of practicability we do _not_ differentiate**
  - **Might cause some discussions/confusion, we are aware of that…**
  - **Still, necessary for overall goal.**
  - **Trust us, you will still get value out of it ;-)**

Ok, so how does this stuff work?

ERNW Living Security.

- **Get (“the right”) people on table (confcall ;-)**
- **Agree on “some parameters” (see below)**
  - **Ideally done _before_ actual exercise**
- **Fill out table(s)**
- **Here we go…**

Prerequisites I

- **Discipline**
- **Discipline**
- **Discipline**

- **Ground rules (besides all those appl. to confcalls anyway)**
  - Follow timeframe & -limits and agenda
  - Remain highly goal-oriented
  - Do not assume anything can be discussed “later” or outside_this_call

Prerequisites II

- **Formulate the question!**

- **Agree on**
  - Asset
  - Security objectives / requirements
  - Main *threats*
    - *_Not_ risks!*
    - *5, max 10*
    - *Collect in advance of RRA meeting, consolidate*
      -> Moderator

- **Just “security risks” or *reward* to be considered as well?**

Formulate the question!

Example

ERNW Living Security.

- **Question:**

  What are the main risks and the risk delta between hard vs. soft tokens?

- **Asset to be protected:**
  Corporate network housing all Corporate Data

- **Security Objectives as for asset:**
  Confidentiality, Integrity, Availability & Compliance

Example, part 2

ERNW Living Security.

Assumptions as for environment/context:

- **Some standard corporate laptop image deployed.**
- **SSL VPN same or better risk profile than IPSec.**
  - ??? ;-) → heard Talk on SSL negotiation attacks at Troopers 2010?
- **Keyfob style hard token.**
- **Best practice of not storing PC and hard token in same place is mostly followed. Still violations of practice must be accepted as matter of fact.**

Agreeing on *asset*

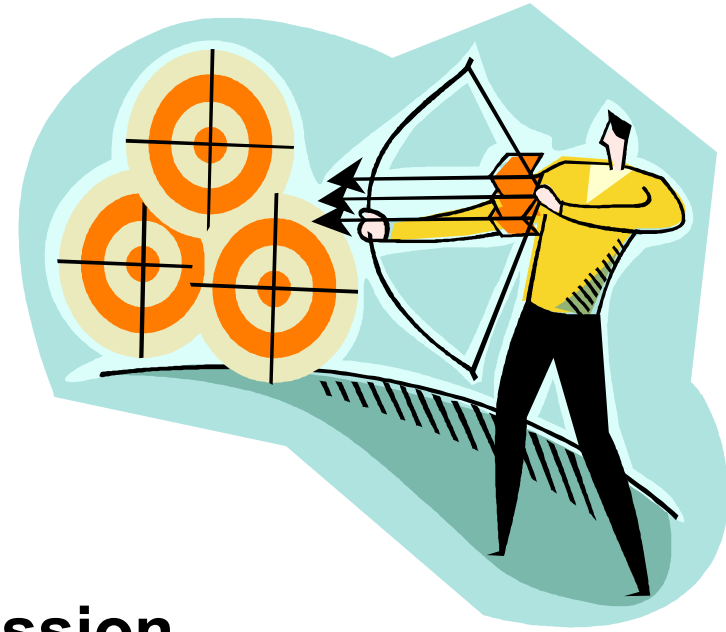
ERNW Living Security.

- **Examples**
  - Corporate Data (*PII*, *Restricted* or sth)
  - Corporate Network

Agreeing on security objectives (of $ASSET)

ERNW Living Security.

- **Examples**
  - Integrity / Confidentiality
  - Availability
  - Regulatory Compliance



- **Usually without agreed-on sec_objectives inefficient discussion.**

Agreeing on threats

- **This is an absolute MUST!**
- **Whole discussion will be inefficient if not strictly followed.**
- **Agree on threats _before_ going into RRA**

  - Threats brought on table after some defined point will be discarded.
  - So identify relevant “threat contributors” in advance and collect threats.

Case Study I

ERNW Living Security.

- **Very large corporation with “total IT-partnering” (= IT nearly completely outsourced).**
- **Currently (since two years ;-) in transition state from one outsourcing partner to another.**
- **High degree of global dispersion**
  - → relevant infosec people on different continents.

- **VUCA (*volatile, uncertain, complex, ambiguous*) type of environment.**
- **Large project ongoing to enhance user experience for remote access, incl. webified services, SSL VPNs etc.**

Case Study I

ERNW Living Security.

- **Various lengthy discussions with many people involved beforehand**
  - → kind-of-stuck situation.
- **RRA was prepared by key players, incl. identification of threats (three people, 60 min. conf call + some email xch.).**
- **RRA exercise itself performed (8 people, 2h conf call).**
- **Results delivered “to business”/”the large project”.**

Case Study I

ERNW Living Security.

Hard Tokens

Threats	Probability	Vulnerability	Impact	Risk
Attacker with physical access to device trying to get unauthorized network access.	3	2	3	18
Malware grabs authentication data.	5	2	4	40
Seed distribution (intentionally) intercepted / misdirected (human failure).	2	1	4	8
Man-in-the-middle attack against data channel.	4	2	4	32

Soft Tokens

Threats	Probability	Vulnerability	Impact	Risk
Attacker with physical access to device trying to get unauthorized network access.	4	2	3	24
Malware grabs authentication data.	5	4	4	80
Seed distribution (intentionally) intercepted / misdirected (human failure).	3	3	4	36
Man-in-the-middle attack against data channel.	4	2	4	32

What happened next

- **Guess what: “business” got back to us… asking for compensating controls**
  - → New exercise after identifying those
  - Very easy, as people already familiar with method & stuff (60 min call)
  - NOTE: “Hard Tokens” were used as a baseline, therefore they weren’t re-evaluated

Soft Tokens W/Compensating Controls

Threats	Probability	Vulnerability	Impact	Risk
Attacker with physical access to device trying to get unauthorized network access.	4	2	3	24
Malware grabs authentication data.	5	3	4	60
Seed distribution (intentionally) intercepted / misdirected (human failure).	3	1	4	12
Man-in-the-middle attack against data channel.	4	2	4	32

Case Study II

- **Global manufac. company in US$ 20 billion turnover range**

- **Many business units & high degree of innovation/R+D**
  - Quite some joint ventures
  - Every year a number or acquisitions of smaller (specialized) companies
  - Participation in many industry consortia

Case Study II

ERNW Living Security.

The “usual static network security policy” going like:

- ***If an untrusted network gets connected, this has to be done by a 2-staged firewall*.**
  - → Which networks are untrusted? Industry peers? Recently acquired subsidiaries? “All (external)”?
  - Usually business “not too delighted” about delays induced by this ;-))
  - We suggested “risk based approach” for deciding on connect. options.

Case Study II

ERNW Living Security.

- **Getting the “right people with the necessary knowhow and level of authorization” was a bit difficult.**
  - Took about three weeks.
  - Most probably much faster next time.
- **Exercise itself performed in 2h conference call.**
  - Went surprisingly smooth given they had not too much RA experience.
- **“Interesting result” (see next slide)**
  - Traditional 2-staged firewall would not have provided protection anyway.
- **Business *very* happy with way this was handled.**

Case Study II

ERNW Living Security.

Threats	Probability	Vulnerability	Impact	Risk
Malware Spread	2	3	3	18
Targeted attack from compromised host in remote network	2	3	4	24
Network connection leading to opportunities of eavesdropping on/hijacking of sensitive traffic (restricted, PII)	3	4	4	48
Introduction of untrusted networks (e.g. WLANs with insufficient crypto)	2	2	2	8
Backdoor internet access leading to undesired traffic profile or attack opportunities	3	3	2	18
Unmanaged components leading to loss of mgmt/visibility	3	2	3	18
Network troubles due to address space collisions, routing protocol interference etc.	2	2	5	20
Overall security stance of existing services in local network degraded (e.g. SMB dialect downgrade)	1	3	3	9
Insufficient logging/monitoring/auditing leading to regulatory non-compliance	2	2	5	20
Violation of regulations (e.g. personal data/PII processed in Non-EU countries without adequate protection level)	3	3	5	45

Lessons Learned

ERNW Living Security.

- **Joint understanding of scope & asset is paramount.**
  - Provide clear directions.
    - Overall architecture, authentication methods, number of users affected
    - Classification of/applicable regulations as for data processed!!
  - Spend sufficient time (usually 10-15 min.) on agreeing on this. There will *always* be people in the group/call who did not perform "their homework" (read their mails).
  - Have network diagrams etc. readily available for moderator/presenter.
  - Remember: delivering result (staying on time) is crucial.

- **Everybody has to be "on track" (as for RA methodology).**
  - No time for explaining overall process again+again.
  - Have a 1-pager outlining process available for moderator/presenter.

More Lessons Learned

- **Providing information about threats/likelihood in advance (statistics from SANS etc.) might be helpful.**
  - At times an area of heavy discussion.

- **Explanatory comments are important**
  - Certainly somebody (again: “important”/VIP) will ask questions *after* the fact. Even if *governance mode* was agreed on beforehand.
  - Assign different person than moderator/presenter to take extensive minutes, besides filled-out RRA itself.

- **Comment fields giving additional info on threats can be helpful.**

Summary

ERNW Living Security.

- **Risk assessment is an essential tool in efficient infosec management.**
  - Every CSO/ISO should use it. On a nearly daily basis ;-)
- **Still, many organizations fail to implement it. One reason is that current methodologies are too complicated for “a fast moving business”.**
- **RRA might be a way to perform RAs efficiently, especially for *governance mode*.**

There’s never enough time…

ERNW
Living Security.

THANK YOU…

...for yours!