UP YOUR INFOSEC GAME: ENABLE THE BUSINESS

WHO AND WHY?

Michalis Kamprianis

MBA, MSc, CISSP, CCSK, COBIT, Prince2, ISO27001LA, ITIL

BSides Hannover - March 19th 2017

1.

MYTHOLOGY

DAEDALUS' PROBLEM

Business problem:	->	I want to expand
Vague idea:	->	I have to be able to move around, I need to start by getting out of here
Technological solution:	->	Build wings and fly!

1.1

THE MISSING ELEMENT: RISK MANAGEMENT

Security says:
I need to enable
the business

RISK MANAGEMENT

- Visibility
- Educated guesses
- Confident decisions
- Preparation for the “unexpected”
- Assurance, accountability

RISK 1 : HEAVY WINGS

Risk	Description
Vulnerability	Wings can not be used properly if they are too heavy
Threat	Moisture from the sea may wet the wings
Impact	Inability to operate the wings will result in falling to the sea
Mitigating Control	Do not fly too close to the sea

RISK 2: THIN WINGS

Risk	Description
Vulnerability	Wings can not be used properly if they are too thin
Threat	Heat from the sun may melt the wax and dissolve the wings
Impact	Inability to operate the wings will result in falling to the sea
Mitigating Control	Do not fly too close to the sun

OTHER POTENTIAL RISKS

- Rain causes the wings to dissolve
- Birds attack Daedalus & Icarus
- Guards see them and take them down
- Icarus & Daedalus get too tired
- Any random God gets angry and does something

THE WRONG STORY

- Ensure users can not fly too high
- Ensure users can not fly too low
- Design a defence mechanism against bird attacks
- Ensure you do not fly until you are sure the humidity is not too high
- Ensure users will not get too tired
- Ensure you can hide from the guards

THE RIGHT STORY

Team spirit	->	Business cooperation
Proactivity	->	Security by design
Respect risk appetite	->	Business acumen

“

Courage is the middle between one extreme of deficiency (cowardliness) and the other extreme of excess (recklessness)

-Aristotle: the Golden mean

OPTIONS FOR RISK MANAGEMENT

- Mitigate, Reduce, Optimize
- Avoid, Eliminate
- Transfer, Share
- Accept

“

… sometimes risk is compensated by opportunity

- ENISA

2.

REALITY

identity
management
user
Services
business
system
control
model
organizations
framework
mobile
privacy
secure
users
manage
including
requests
provides
request
cloud
theft
IAM
risk
roles
apps
also
used
help
pure
may
like
get
first
SAML
known
name
real
try
role
SSO
Special
best
identities
ever
able
use
set
key
ID

IDENTITY & ACCESS MANAGEMENT

- Access control
- Consistent password policy
- Strong password policy
- Quick access revocation
- Audit response
- Access auditing and segregation of duties

STAKEHOLDER ALIGNMENT

Stakeholder		Benefit
Applications Manager	->	Reduce overhead
Finance Manager	->	Manage licenses’ cost
Human Resources	->	Reduce onboarding time
End user	->	User friendly
Compliance & Audit	->	Improve report efficiency
Governance	->	Establish transparency

3.

ENABLE BUSINESS

VALUE GENERATING ACTIVITIES

- ISO 27001 certification
  - Objective proof that we are secure
- Mobile device management
  - Enhanced efficiency, faster response on the road
- VPN concentrators and two factor authentication
  - Home office and remote workers
- GDPR
  - Competitive advantage, due diligence

GAME RULES

- Scare tactics : Use scarcely
- Ask the right questions
- Provide the right answers
- Get your numbers and story straight
- Talk efficiency and value

3.1

THE RIGHT QUESTIONS

DON'T ASK THE WRONG QUESTIONS

- Can we afford not knowing who logged in our systems?
- Do we want to lose our data?
- Are we ready for a virus outbreak?
- What if users get hit by ransomware?
- Can we afford being hit by a train?

ASK THE RIGHT QUESTIONS

- How big is the train?
- What is its speed?
- Where are we when it hits us?
- Do we have insurance?
- How old are we?
- How likely it is?

Can we afford being hit by a train?

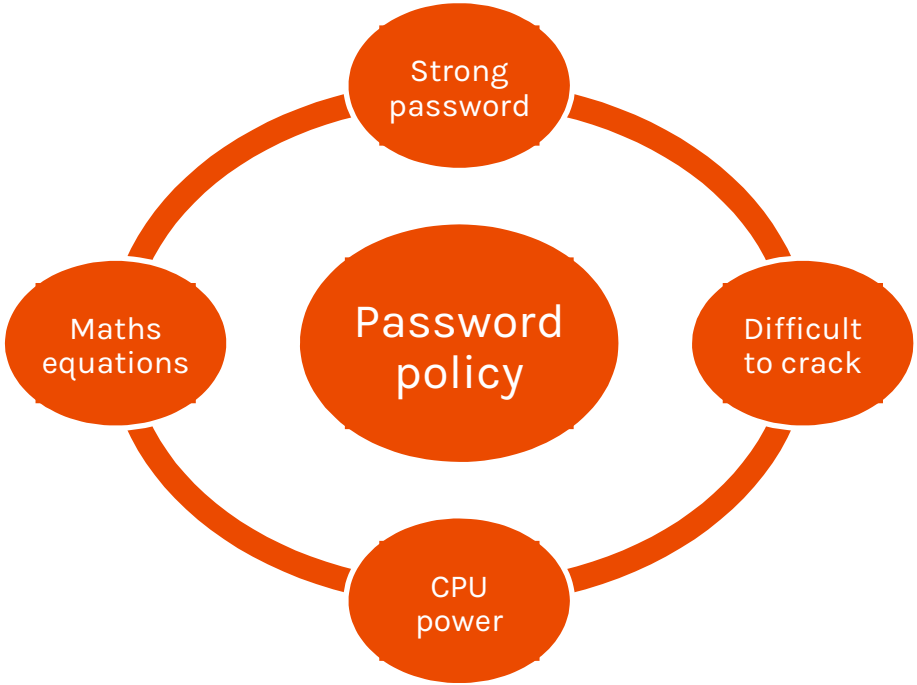
YES

WE CAN!

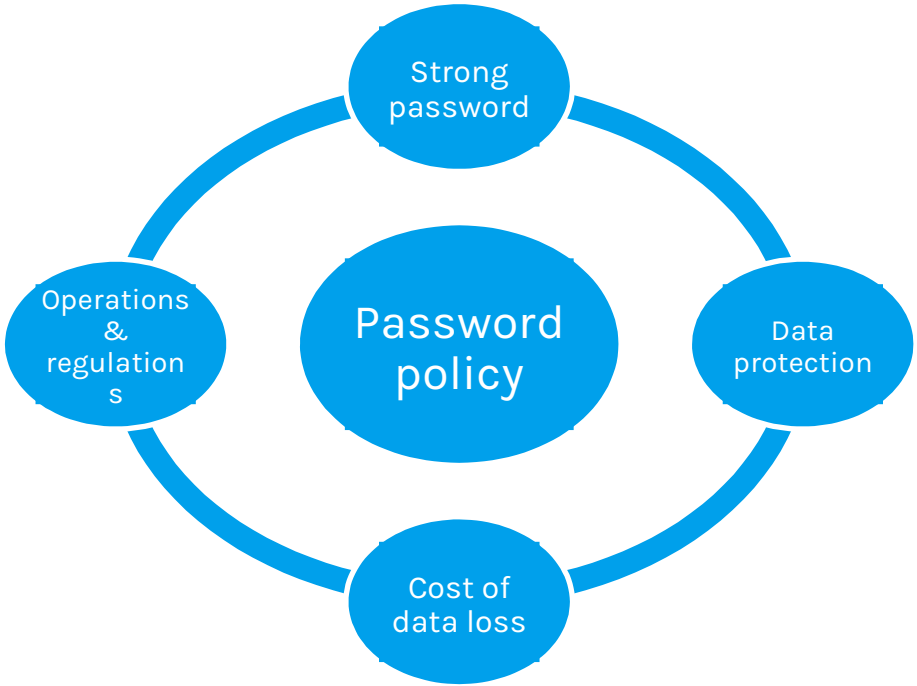
3.2

THE RIGHT ANSWERS

DON'T GIVE THE WRONG ANSWERS



PROVIDE THE RIGHT ANSWERS



3.3

GET YOUR NUMBERS AND STORY STRAIGHT

- Use known and respected sources
- Use sources relevant to your industry
- Use numbers that make sense to what you want to sell

DO NOT MISINFORM

Format Preserving Encryption offers

- Usability as it maintains the format
- Efficiency as it allows correlation
- Compliance with standards that **require encryption,** such as GDPR

“

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.

- GDPR, §26, page 5

3.4

TALK IN BUSINESS TERMS

TALK ABOUT EFFICIENCY

- Time spent in support
- Time to produce reports
- More efficient operations
- Process maturity
- Use seasonality

TALK ABOUT VALUE

- Win new business
- Meet contractual obligations
- Improve reputation
- Intellectual property
- Protect share price

CREDITS

Special thanks to:

- Presentation template by SlidesCarnival
- Icarus & Daedalus illustration by Dylan Meconis
- Train & toddler picture by Mari Kanezaki @pixabay

THANKS!

Any questions? Ask me now or

On Twitter: @kamprianism
On my blog: https://kamprianis.eu/michalis/i.think
On LinkedIn: https://www.linkedin.com/in/michaliskamprianis