What is worth to be afraid of?
in
financial institutions and other
critical – noncritical infrastructures

Dr. Katalin Szenes, CISA, CISM, CGEIT, CISSP, PhD
szenes.katalin@nik.uni-obuda.hu

Obuda University
John von Neumann Faculty of Informatics

Table of Contents

Table of Contents

SOLUTION: strategic excellence:
passport for security to corporate governance

- strategic goals ♫♪ security goals

- 10 useful strategic / security subgoals:
  - operational excellence criteria:
    - effectivity, efficiency, compliance, reliability,
    - strategy-driven goal & operational risk management excellence
    - functionality
    - order
  - asset handling excellence criteria
    - availability, integrity, confidentiality

- on authorities' directives and guidelines - for financial institutions
- on IT security & IT audit best practice
- directives and guideline-like references
- some security URLs

Table of Contents

further buzzwords

- remarks on cloud security
- research initiatives of the Cloud Security Alliance - 2017
- hope concerning cloud computing - half a decade ago
- how to plan: the strategy - my personal opinion

GDPR - EU General Data Protection Regulation

Key changes to EU data protection introduced by the GDPR (2016 / 679 EU)

- More rigorous requirements for obtaining ***consent*** for collecting personal data.
- Raising the age of consent for collecting an individual's data from 13 to 16 years old.
- Requiring a company to ***delete data if*** it is no longer used for the purpose it was collected.
- Requiring a company to ***delete data if*** the individual revokes consent for the company to hold the data.
- Requiring companies to ***notify*** the EU government of data breaches in 72 hours of learning about the breach.
- Establishing a single national office for monitoring and handling complaints brought under the GDPR.
- Firms handling significant amounts of sensitive data or monitoring the behaviour of many consumers will be required to appoint a data protection officer.
- ***Fines up to € 20m or 4%*** of a company's global revenue for its non-compliance.

what then?

Szenes 5

GDPR - EU General Data Protection Regulation

remedies

based on:

1 lectures of the vice-president of the
Hungarian National Authority for Data Protection and Freedom of Information - NAIH

2 Hungarian legislation (that have always been much more stricter than the EU average)
- 1992 LXIII. law: On the protection of personal data and on the publicity of the data of public interest
- and its updates, e.g. data protection officer, data protection procedural rulebook

3 courses attended and exam on data protection

the GDPR requirements are not dramatically new, "only"
- emphasized transparency and accountability
- reinforced position of the NAIH

to do:
- process of the outsource-related data-handling
- if necessary: voluntary reporting for audit

why?

present fines < < fines from 25 May 2018: 20 million EUR or 4% of revenue

Szenes 6

GDPR - IT security issues (some of my personal examples, without completeness)

pillars of operational excellence:

- organizational, regulational, technical

organizational control objectives & measures:

- privacy officer appointed
- identification of related business processes ➜ related organizational units
  - where: customer data, or outsourced support are involved,
  - privacy-sensitive applications, etc.
- join efforts with the regular obliged + BCP-related risk assessment
  ➜ business process & business data privacy classification ➜ encryption**?**

regulational control objectives & measures:

- procedural rulebook
  - handbook-like policy is not enough **!**
  - rules for the involved organizational units:
    how to handle / what / who / permission / acknowledgment / when

Szenes 7

GDPR - IT security issues (some of my personal examples, without completeness)

technical control objectives & measures:

- monitor the activities of the staff / access to sensitive systems / data

already at development phase, ***systems analysis knowledge is needed everywhere***

organizational, regulational, and technical control objectives & measures:

- incident handling
- identity management
- access right management / **!** by business processes

joining efforts with PO (Privacy Officer) where needed:

- introduce ***usable*** metrics for qualifying the level of enterprise privacy protection
  (e.g. number of privacy-sensitive applications - join efforts with risk assessment
  % of systems affected by incidents,
  average time to recover, etc.)
- tailoring incident handling to satisfy privacy issues, too
  (special contact rules, communications plans & procedures, etc.)

Szenes 8

PSD2

- European Commission:

"Brussels
27. 11. 2017.
C (2017) 7782 final"

here:
https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-7782-F1-EN-MAIN-PART-1.PDF

- from the CEO of EBF - European Banking Federation:

“European citizens demand pan-European services that are safe and efficient. Consequently, there is a need to look carefully at the governance and regulation of payment solutions.”

here:
https://www.ebf.eu/priorities/digitaltransformation/payments/

Szenes 9

PSD2 duties of the banks
to be assigned to
security experts with systems analysis and systems programming practice

security requirements - no problem:
as these are not new, already long ago required by:

- either the "Hpt.": 2013. CCXXXVII. Law on Financial Institutions
- or the government decree 42/2015. (III. 12.)
- or the more or less regularly updated Supervisory Authority advice:
  more explicit present version: Hungarian National Bank July 2017 Recommendations

- regular risk & vulnerability management
- improving the quality of IT operations
  - operational security, e.g. authentication, encryption, etc.
- improving the quality of IT infrastructure
- business continuity management
- monitoring
- incident reporting (already regular to the Hungarian National Bank)
- audit, etc.

but

Szenes 10

PSD2 - disadvantages for the banks

disadvantages in relations with different service providers:

AISPs - Account information service providers

- are subject ***only to registration instead of authorisation***
- have many exemptions, e.g.
  - requirements related to AML,
  - to statutory audits,
- etc.

see: EBA/GL/2017/09 11/07/2017 final report

TPP (third-party payment service providers) ➔➔ Banks
experts' opinion in 2017 March:

customers' - TPP - bank relation:
does not matter, who made the mistake,
it is the risk of the bank, TPP has the advantage

PSD2 - disadvantages for the banks

TPP ➔➔ Banks examples:

- if the customer complains, then the bank has to credit ***immediately*** the questioned amount onto the customer's account,
- and ***only afterwards*** can the ***bank begin proving***, it was not a mistake of the bank
- the bank is the one, that ***has to notify the TPP***, that the latter has to commence an investigation to prove its faultlessness
- the way of notification - investigation - result processing is not detailed

(I wonder if the TPPs will admit any fault)

- should the TPP admit its mistake, then it is obliged to pay back the money of the bank

(what if it does not?)

- should the customer be mistaken, then the bank has to find a way to get its money back
- the bank may be obliged to compensate even the TPP

I still have a question:

how to prove, which organization did, what?

(it is important to choose a premium log management tool
but even this might not help
at least it might be able to monitor the employees' behaviour
- MNB requirement)

3rd set of requirements:

Hungarian Supervisory Authority
the Hungarian National Bank
Magyar Nemzeti Bank - MNB

Recommendation
of the Hungarian National Bank 7/2017. (VII.5.) on the defense of IT systems
↓ ***mitigation*** requires security experts with ***proven systems analysis practice***

the issues of the Supervisory Authority Recommendation are mostly sensible, e.g.

- not required to fulfill every contradicting viewpoint at the same time

and

- IT enterprise management is required

how? **strategy-based BPR !** (business process reengineering)
corporate strategy → IT strategy
↘ classification of business goals
↘ classification of business processes
meanwhile: identification of the "data" - process owners
↘ classification of IT systems & data
↘ we have the data necessary to risk assessment +
\+ we fulfill the data classification requirement of the Supervisory Authority

risk assessment → IT business continuity plan
classification of IT systems & data → vulnerability management with sensible targets
Recommendation: network: yearly, card components: quarterly

Szenes 15

requirements of: Recommendation of the Hungarian National Bank 7/2017. (VII.5.)
on the defense of IT systems
↓ issues requiring security experts with ***proven*** systems analysis practice

the Recommendation explicitly requires an application security expert, having
↘ practice in application development
↘ practice in security

further requirements of the Supervisory Authority, e.g.

- the security expert should ***participate*** in the development of applications from the planning phase →
- **[**throughout the whole life-cycle**]**
- documentation of the connections between the individual application systems
- this documentation, together with the communications documentation should contribute to the tracing of the business data streams
- the applications should functionally suit to the fulfillment of the legislatonal compliance requirements

[COBIT 5:

- implementation of business issues
- implementation of audit trails **]**

Szenes 16

HELP:

strategic excellence

the relation between the fulfillment of the

- strategic goals and
- security goals

strategic goals

⬇

business goals

⬇

operational & asset handling excellence goals

⬇

very practical goals

but:

where is security?

➔ in the practical HELP

IN SOLVING the problems and "problems"

10 useful strategic / security subgoals

☺ ground level, practical goals

☺ contributing to strategic / security goals

ground-level goals contributing to strategy / security

- *criteria* characterizing *excellent* operations:
  - effectivity,
  - efficiency,
  - compliance,
  - reliability,
  - strategy-driven goal & operational risk management excellence,
  - functionality,
  - order
- *asset handling excellence criteria*:
  - availability,
  - confidentiality,
  - integrity

Szenes 19

on authorities' directives and guidelines - for financial institutions

- EBA/GL/2017/09 11/07/2017 final report
  On the EBA Guidelines under Directive EU 2015 /2366 PSD2 on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers
- EBA/CP/2017/12 24 July 2017 Consultation Paper
- Recommendation of the Hungarian National Bank 7/2017. (VII.5.)
  on the defense of IT systems in force: 15th July 2017
- Hungarian Banking Association: report on the activity of the PSD2 Working Group (April, 2017)

Szenes 20

on IT security & IT audit best practice

(ISACA, ISC2. ISO, NIST, PCI DSS, BSI IT-Grundschutz-Kataloge 9/40, ...)

ISACA: information Systems Audit and Control Association, founded in the USA
www.isaca.org

- CISA Review Technical Information Manual © ISACA
  (member of the Quality Assurance Team of the Manual from 1999: K. Szenes)
- Enabling Processes - COBIT 5 An ISACA Framework © 2012 ISACA
  (member of the Subject Matter Expert Team in 2010-2011: K. Szenes)

CISA – Certified Information Systems Auditor designator: ISACA
(I have been teaching at the Hungarian CISA Review Course from 1999)
CISM - Certified Information Security Manager designator: ISACA
CGEIT - Certified in Governance Enterprise IT designator: ISACA
CRISC - Certified in Risk and Information Systems Control designator: ISACA

CISSP - Certified Information Security Professional designator: ISC2
ISC2: International Information Systems Security Certification Consortium,
founded in the USA, www.isc2.org

Szenes 21

directives and guideline-like references

on authorities' directives and guidelines - for financial institutions

- EBA/GL/2017/09 11/07/2017 final report
  On the EBA Guidelines under Directive EU 2015 /2366 PSD2 on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers
- EBA/CP/2017/12 24 July 2017 Consultation Paper
- Recommendation of the Hungarian National Bank 7/2017. (VII.5.)
  on the defense of IT systems in force: 15th July 2017
- Hungarian Banking Association: report on the activity of the PSD2 Working Group (April, 2017)

on best practice of NIST

the source of the Hunguard practice (related to Government Decree):

- Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0)
  National Institute of Standards and Technology, February 12, 2014
- Security and Privacy Controls for Federal Information Systems and Organizations
  (joint task force transformation initiative) NIST Special Publication 800-53
  Revision 4 April 2013 U.S. Department of Commerce

Szenes 22

some security URLs

some URLs on vulnerabilities

- https://nvd.nist.gov/
- https://cxsecurity.com/
- http://www.securityfocus.com/
- Hungarian: Nemzeti Kibervédelmi Intézet http: //www.cert-hungary.hu/

supporting systems development

- https://www.oasis-open.org/
- control measures to be applied (e.g. ISACA)

devices supporting defense

- http://www.checkpoint.com
- http://www.cisco.com
- https://www.snort.org/ -network intrusion detection for Linus and Windows

remarks on cloud security

research initiatives of the Cloud Security Alliance

- network security
- continuous monitoring
- business continuity and disaster recovery
- SIEM - security information and event management
- identity and access management
- vulnerability assessments
- best practices for cyber incident exchange
  will help remove barriers and enable secure, timely and effective
  intelligence incident exchange and collaboration
- Mobile Working Group Security Guidance for
  critical areas of mobile computing
- SDP - software defined perimeter specification [seems to be very strong]

https://cloudsecurityalliance.org/
(2017)

hope concerning cloud computing - half a decade ago

- ISACA - Information Systems Audit and Control Association
  - efficient, agile enterprise
  - with innovative, competitive services
  - decrease the operating costs

"Cloud governance: questions boards of directors need to ask"

- NIST - USA National Institute of Standards and Technology
  - automatic providing for processor time, storage capacity
    without human interference
  - broadband network access
  - resource pooling - dynamic service, independently from location
  - elastic service
  - measurable, supervised service

NIST Special Publication 800-145 (Draft), 2011

how to plan: the strategy - my personal opinion

obligatory steps:

- compliance overview
  - legislation
    - prepare an inventory of every applicable home country / EU / other laws & directives
  - collect the requirements of every relevant supervisory authority
    - industrial
    - mother company
  - take into consideration every above kind requirements related to "traditional" outsourcing, too
  - etc.
- fulfill usual IT security requirements before going out
  - ***see GDPR audit issues here, too***
  - network security
  - etc.

how to plan: the strategy - my personal opinion

- reconciliation of the present situation
  - prepare for preserving applications security
    - identify strategic, sensitive, other data of outstanding importance
    - prepare infrastructure - important data flow map
    - investigate / add monitoring facilities to those applications that are to go out
    - and clean their data if necessary
  - reconcile cloud-like commitments and other not-declared / not realized outsource practices
    - e.g. off-premises data storage, systems use, etc.
      - ▲ in Dropbox, and other cloud apps: frequent phishing and other malware
    - investigate the call center service and the like
    - eliminate the unnecessary / redundant practices, if you may
  - etc., depending on the type of business

how to plan: the strategy - my personal opinion

- customers' hope concerning guarantee
  - collect the standards & best practice you want to (try to) impose upon your cloud provider or at least to hope it complies to
    - security ISO-s, 27000 family, BCP, or even governance guidelines, etc.
    - ISO/IEC 27018:2014

    Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
    - ISACA COBIT 5 and other recommendations
    - ISC2 other recommendations

  - the accreditations of the candidate
    - ask
    - determine the weight to be assigned to this viewpoint in the tender process

- identify and determine the ***measurable*** requirements of a service level agreement
- plan, how to leave the service provider in case of need
  - how to get back, and then
  - how to delete your data from the cloud

Szenes 29