Beyond IT/Fintech: Between Good and Evil. EA/SA and CSO/ISO: To Hire or To Fire?

OWASP Limassol

Albert Fedoseev
Limassol, Cyprus
15.12.2023

Albert Fedoseev

fedoseevalbert@gmail.com

@Albert18486

Experience

2023 - Now	Head of IT, bbf: Cyprus
2021 - 2022	Lead Architect, Innotech, VTB
2011 - 2021	Head of IT Direction, PM, developer, NORE, Eurochem

Education

Ranepa, IT Manager

HSE, Enterprise IT Architecture Management

NCFU, Engineer

Main point:
We should use special financial arguments, risk management tools and strength to prove the need for security and architecture specialists outside the IT area

Agenda:

- Cybersecurity and architecture in startup, entrepreneurship, business.
- Business outside of IT. Conversation with management.
- Where does IT HR optimization begin?
- Efficiency or security.
- Budget and safety\reliability.
- Hire or fire?
- Protection of personnel positions. Protection of IT solutions.

Cybersecurity and architecture in startup, entrepreneurship, business.

Start UP

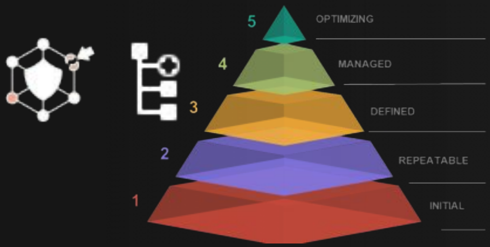
No resources
No money
60% without budget for cybersecurity and architecture

Entrepreneurship

Low control, Lack of scalability
Low level of IT maturity
SysAdmin it's a God
First big incident

Business

Scalability
Reliability
Controllability
70% have serious CS incidents



Cybersecurity and architecture in startup, entrepreneurship, business.

A simple case

Start UP with business tools

Our Mistakes:
Overqualified persons
Design, corporate architecture - 3 months
Security actions - 2 month
Solution architecture - 1 month

Result:
Lack of resources, team burnout
Slowdown of processes, loss of time
lag behind the market, loss of initiative

Conclusion:
In a startup you can’t use business tools. You should take risks.

Business outside of IT.
Conversation with management.

“We need cybersecurity officer”
“We need architects”

“But you are a computer guy!”
“We have programmers!”
“It’s issues for our sysadmin!”

Business outside of IT. Conversation with management.

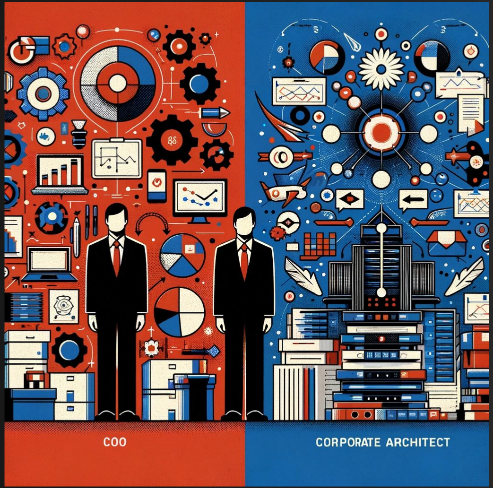
Do not be afraid

- Tell us about the problem
- Accusations of incompetence
- Accusations of low qualifications

Need to try

- HR should be your allies
- Consider potential damage
- Record incidents
- Calculate the economic effect

Business outside of IT.
Conversation with management.



SysAdmin
isn’t
CS officer

Software developer
isn’t
Solution Architect

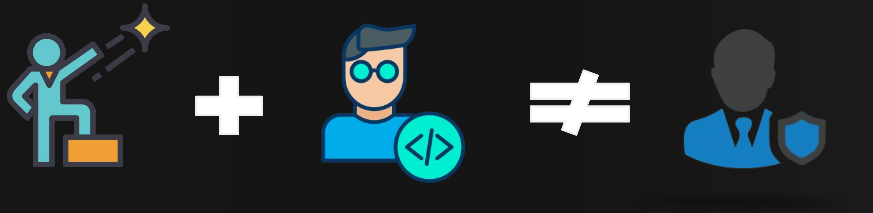
COO
isn’t
Enterprise Architect

Business outside of IT.
Conversation with management.

- Misconception: Don't assume that you are saying obvious things.
- If the roles are combined - costs may increase by 30% or more, depending on the complexity of the IT landscape

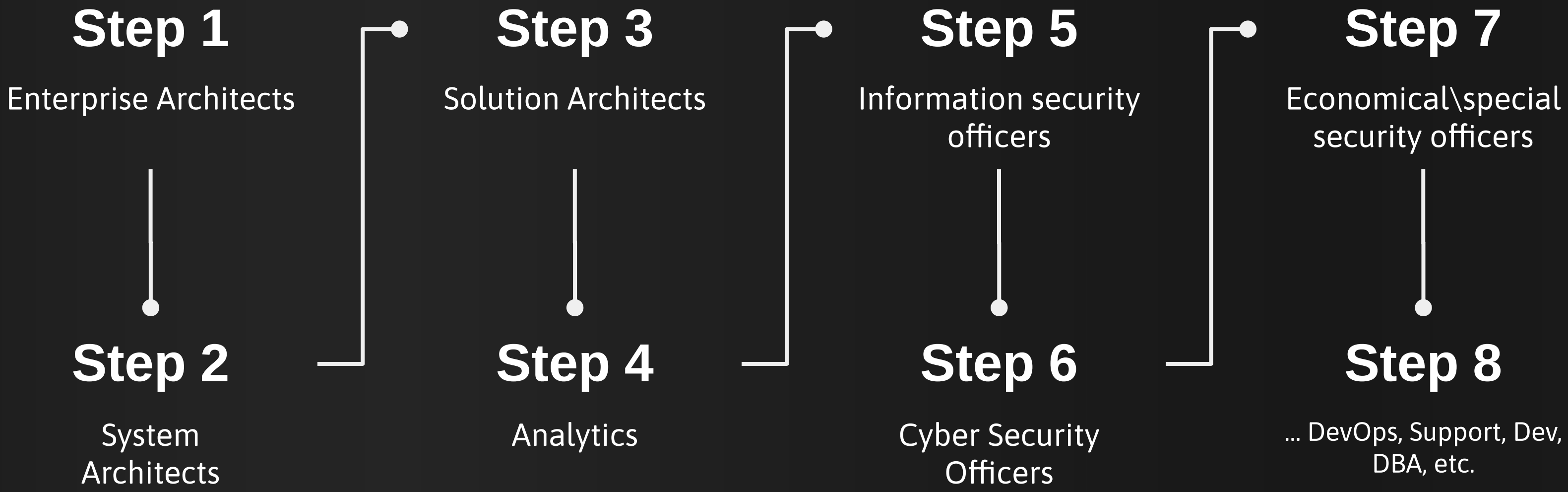
A simple case

Business



Coordination with a security specialist takes a month instead of 3 months.
Product commissioning time reduced by 20%

Where does IT HR optimization begin?



Step 1

Enterprise Architects

Step 2

System Architects

Step 3

Solution Architects

Step 4

Analytics

Step 5

Information security officers

Step 6

Cyber Security Officers

Step 7

Economical\special security officers

Step 8

… DevOps, Support, Dev, DBA, etc.

OWASP Limassol

Impact on late deliveries. The business point of view

60% Security

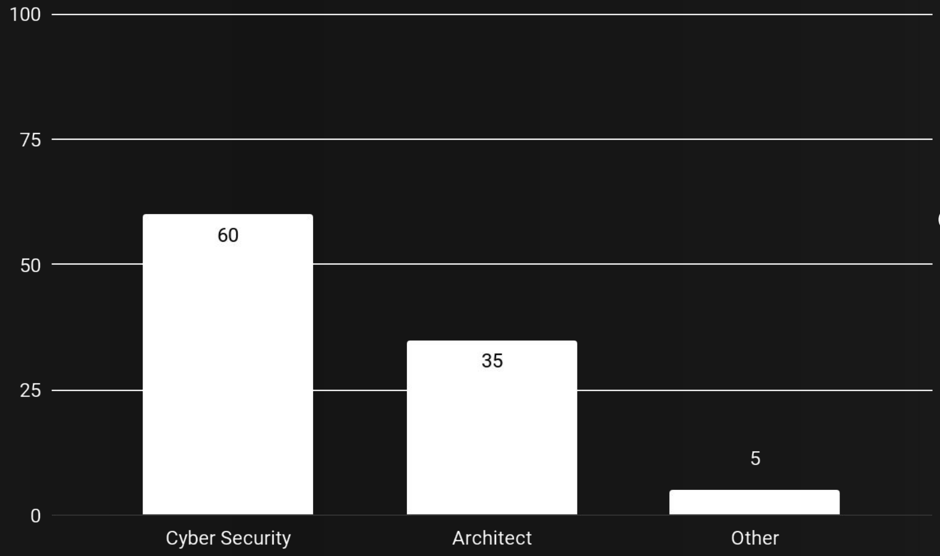
Cyber, economic, informational

35% Architect

Enterprise, solution

5% Others

Analytics, Devops, Dev



Impact on late deliveries. The business point of view

Delays in projects often result in shifting blame to architecture and security teams.
This leads to negative views from the business side.

It's important for management to identify and address such blame-shifting tactics promptly.

Solution:

- Fixing risks. There are no perfect solutions.
- The balance between quality and deadlines is the height of professionalism.
- We fix the risks with the business and move on.

Budget and safety\reliability.

Shouldn't we fire those who interfere with business?

+20 % → Design (architecture, security)

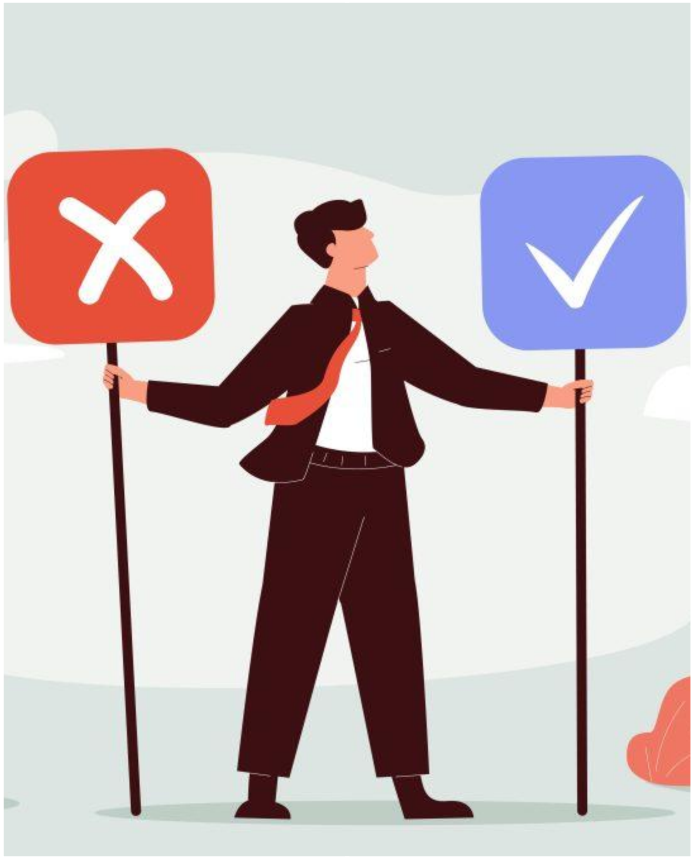
+50 % → Execution of all reliability patterns

Simple Case:
Business features - 50k euro. (PM, analytics, dev, test, devops, etc.).
Arch.\Sec.\Reliability - 35k euro. Total 85k euro.

Option 1 (with stupid Manager):
Manager reduced costs. Only 50k.
Remade every year = 50k euro + 40% indirect costs (remade) + 30% support.
For 3 years spent **220k euro.**

Option 2 (with smart manager):
Costs 85k
Support 20% per year.
For 3 years spent **150k euro.**

This difference it’s 1 junior position for 3 years. Only 1 feature.



Between Evil and good.

Risks

- Bureaucratization of processes
- Budget increase
- Exaggerating problems
- Excessive caution, lag
- Manipulation of risks and vulnerabilities

Solutions

- Control of decisions and metrics
- Make a profit now
- Plan to make a profit
- Bring profit in the future

TO HIRE or TO FIRE?

Security & Reliability

1. To Hold ✋

Take the time and do the analysis
Move personnel within the company
Assess risks and process criticality

2. To Teach 🎓

Form competence centers
Form a personnel reserve
Train employees, grow inside

3. To Fire

At maturity levels 1-3, if there is doubt, fire.
Stagnation, systematic delays, recurring incidents

4. To Hire

Don't hire until last minute
Create a transparent need
Prove financial feasibility

Be extremely careful about increasing your security staff. This is dangerous for the company. Consider the risks carefully.

TO HIRE or TO FIRE?

Security

A simple case

Business

- Approvals from Cyber Security took months. Huge staff of security specialists.
- Transferring files between developers and the customer only through special flash drives manually, with long-term an inventory.
- Prohibitions without alternative solutions
- Hundreds of thousands of losses due to delays

How we managed to improve the situation a little

To Hold. Conducted an internal audit. Defended the results.

To Teach. Increased team qualifications to protect IT-solutions

The approval period has been shortened. Protected file sharing tools and other IT Stack. Affected by changes to the CS service.

Protection of personnel positions. Protection of IT solutions.

Don't waste your time

- It's always about money
- No need to talk about

technology

development

logic

beauty of solutions

methodologies

without money

How to count

- Count everything. Direct costs, indirect costs, cost of ownership, maintenance, electricity, involvement of neighboring departments, speed of task completion
- Play with the planning horizon, manage risks, increase decomposition

Protection of IT solutions

A simple case

Business

AS-IS:

- On premise infrastructure. Accidents, failures, downtime.
- Significant investments have been made.
- Negative attitude towards cloud technologies.
- Strong beliefs about the cost and security of cloud solutions.

TO-BE:

Switch to a hybrid infrastructure.

How we won this:

Detailed calculation of more than 20 direct and indirect costs.
Risk management, controlled damage. Recording and calculating damage.
Collecting references and cases into a report.

Albert Fedoseev

fedoseevalbert@gmail.com

@Albert18486

OWASP Limassol

Thanks!

Beyond IT/Fintech:
Between Good and Evil.
EA/SA and CSO/ISO:
To Hire or To Fire?

15.12.2023

Limassol, Cyprus.