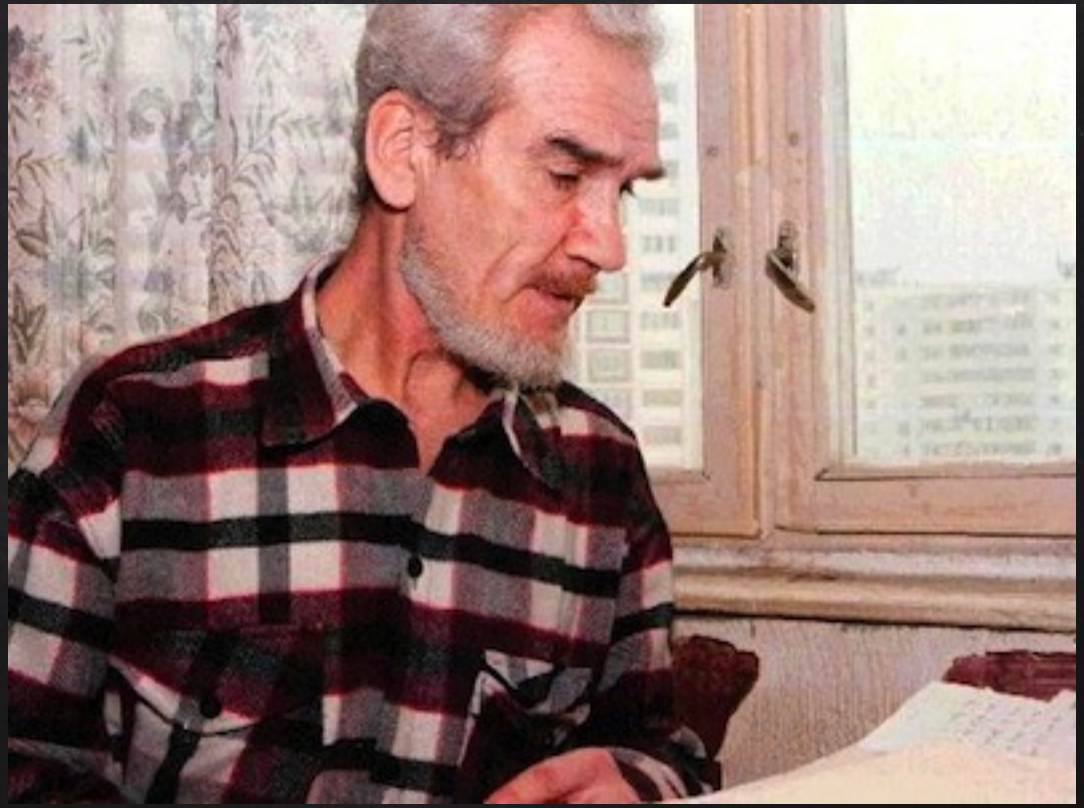
Do Architects Need To Be Security Experts?


I'm Victoria
Security girl at MS
Find me at @texnokot
or victoria.almazova@microsoft.com

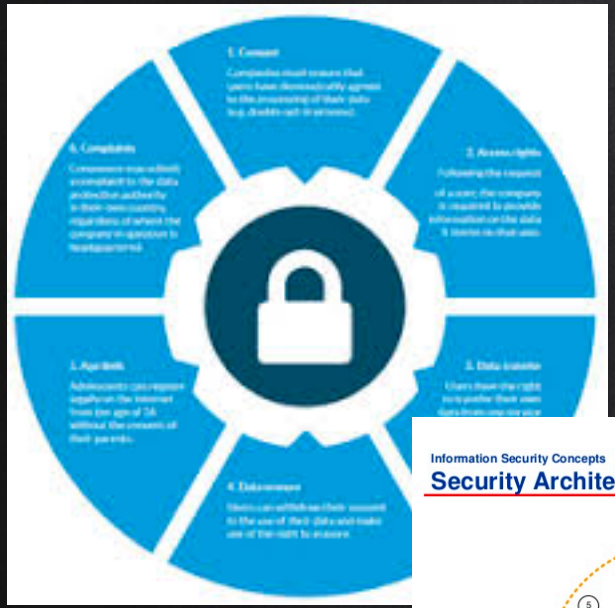
Remember the Mars Climate Orbiter incident from 1999?

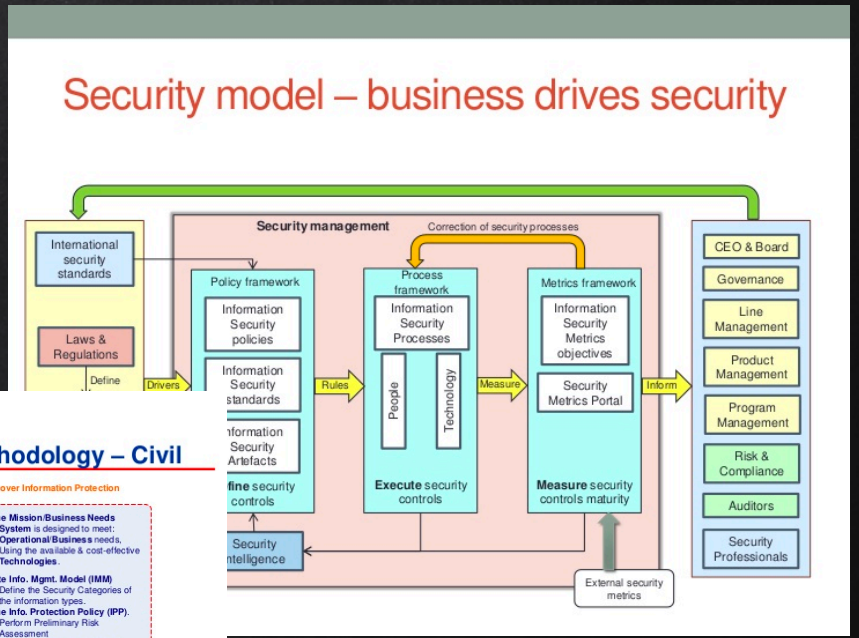


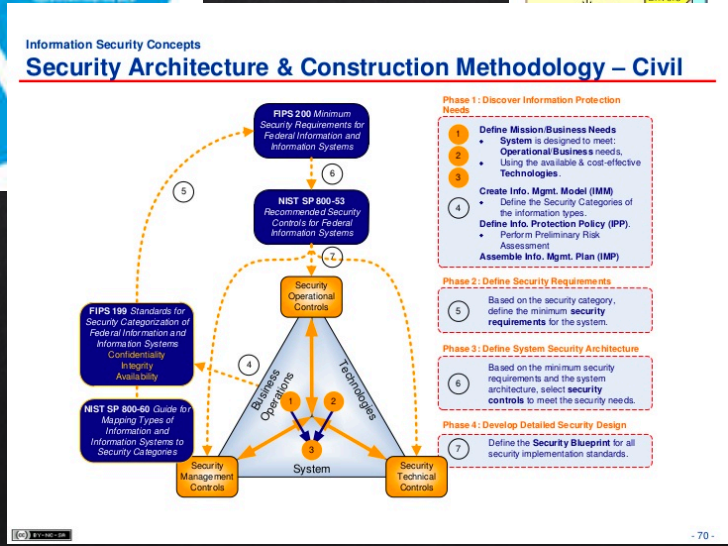
HAD A FUNNY FEELING IN MY GUT

IF A BUILDING HAD 20 EXTERIOR DOORS, AND YOU LOCKED 19 OF THEM, WOULD YOU BE 95% SECURE?

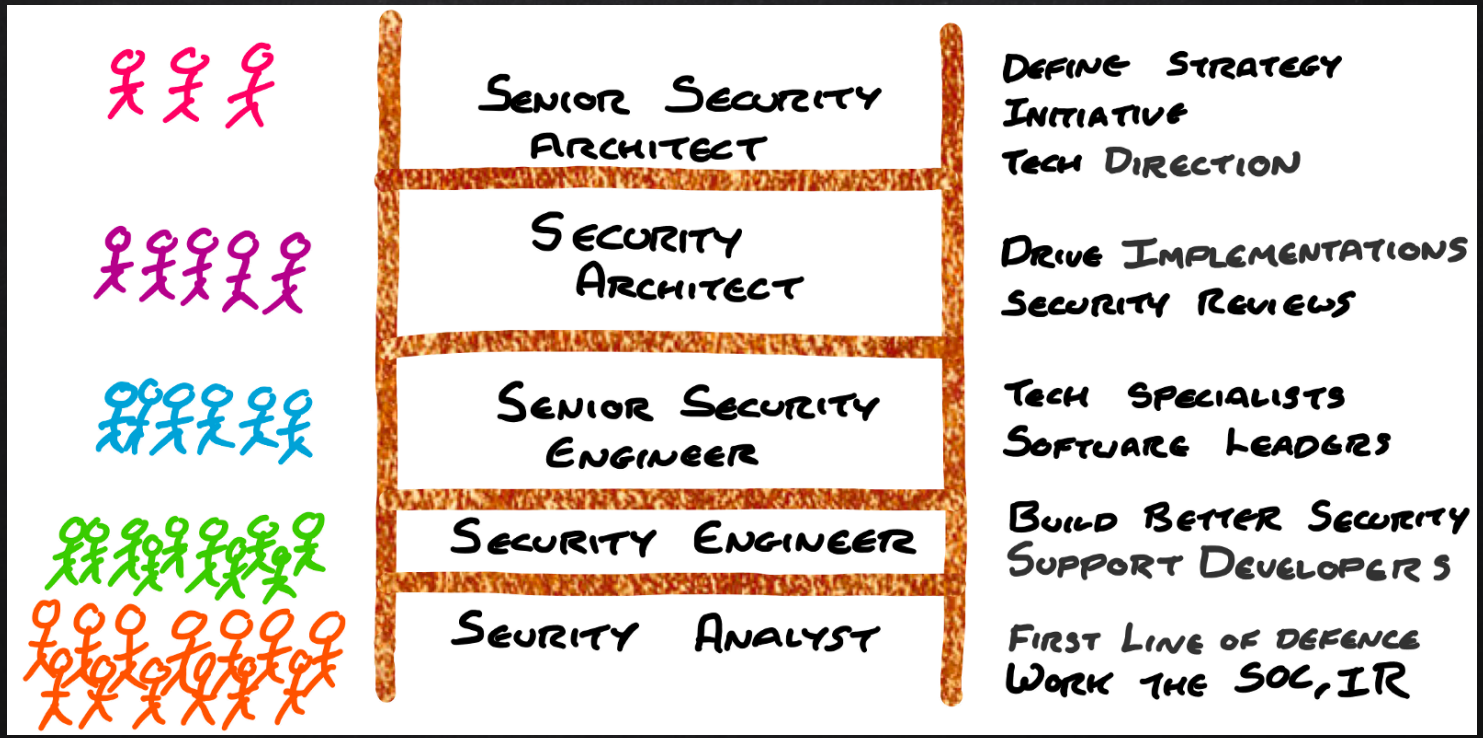
SO WHAT DO WE DO TODAY?




Security model – business drives security
Security management
Correction of security processes
International security standards
Laws & Regulations
Define
Drivers
Policy framework
Information Security policies
Information Security standards
Information Security Artefacts
fine security controls
Rules
Process framework
Information Security Processes
People
Technology
Execute security controls
Measure
Metrics framework
Information Security Metrics objectives
Security Metrics Portal
Measure security controls maturity
Inform
Security Intelligence
External security metrics
CEO & Board
Governance
Line Management
Product Management
Program Management
Risk & Compliance
Auditors
Security Professionals


Information Security Concepts
Security Architecture & Construction Methodology – Civil
FIPS 200 Minimum Security Requirements for Federal Information and Information Systems
NIST SP 800-53 Recommended Security Controls for Federal Information Systems
FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
Confidentiality
Integrity
Availability
NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
Security Operational Controls
Business Operations
Technologies
System
Security Management Controls
Security Technical Controls
Phase 1: Discover Information Protection Needs
Define Mission/Business Needs
System is designed to meet: Operational/Business needs,
Using the available & cost-effective Technologies.
Create Info. Mgmt. Model (IMM)
Define the Security Categories of the information types.
Define Info. Protection Policy (IPP).
Perform Preliminary Risk Assessment
Assemble Info. Mgmt. Plan (IMP)
Phase 2: Define Security Requirements
Based on the security category, define the minimum security requirements for the system.
Phase 3: Define System Security Architecture
Based on the minimum security requirements and the system architecture, select security controls to meet the security needs.
Phase 4: Develop Detailed Security Design
Define the Security Blueprint for all security implementation standards.
- 70 -

What is a Security Architect?



https://medium.com/secjuice/what-is-a-security-architect-a65d3b0c9707

WHAT IS WRONG WITH THAT?

THOUGHTS AND OBSERVATIONS

- ✗ security team – separate field of knowledge
- ✗ or no security architects at all
- ✗ security as a response. We tackle the symptom not the disease
- ✗ should security profs have a seat on Architecture Review Boards?
- ✗ security profs must learn what their respective business is and does

SO WHERE TO GO OR TO DO?

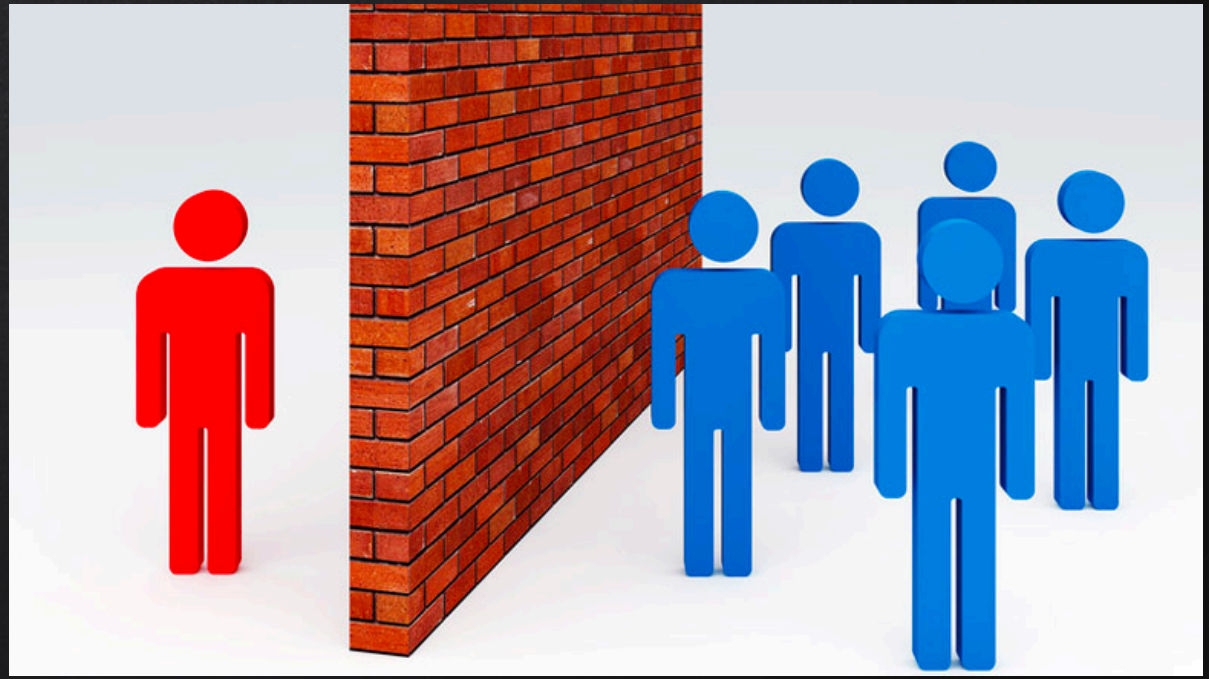
- ✗ build the next generation of Enterprise architects with security embedded into their architecture frameworks

- ✗ security architecture –> a secure architecture

Security architecture -> Secure architecture

- ✗ No wall between security and enterprise architects
- ✗ Mindset change towards «Security by design»
- ✗ Continuous security awareness program
- ✗ Internal criminals
- ✗ Integrate security into EA
- ✗ From rules to principles

No wall between security and enterprise architects



Mindset change towards "security by design"

Pre-commit

- ✗ Threat modeling
- ✗ IDE Security plugins
- ✗ Pre-commit hooks
- ✗ Secure coding standards
- ✗ Peer review

Commit (CI)

- ✗ Static code analysis
- ✗ Security unit tests
- ✗ Dependency management

Acceptance (CD)

- ✗ IaC
- ✗ Security scanning
- ✗ Cloud configuration
- ✗ Security acceptance testing

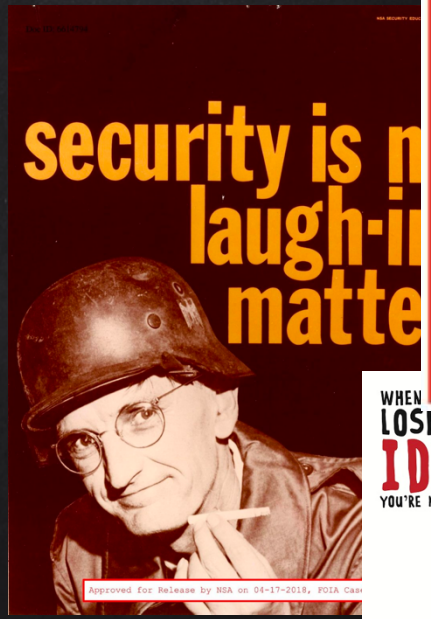
Production

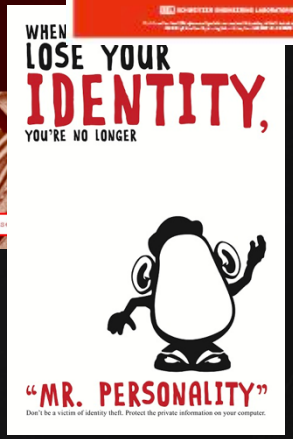
- ✗ Security smoke tests
- ✗ Configuration checks
- ✗ Penetration testing

Operations

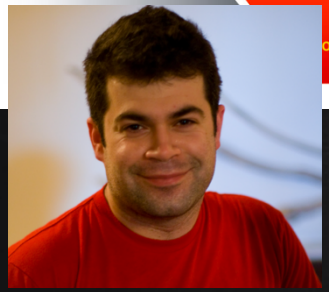
- ✗ Continuous monitoring
- ✗ Threat intelligence
- ✗ Penetration testing
- ✗ Blameless postmortems

Continuous security awareness program





INTERNAL CRIMINALS



https://en.wikipedia.org/wiki/Jesse_Robbins

Integrate security into EA

- ✗ Security is an aspect in EA methods (TOGAF/SABSA)
- ✗ Combination with selecting the right standards like NIST or ISO
- ✗ No for a separate architecture

From rules to principles

- ✗ The concept of principle based design, rather than rule-based
  - Security by design principles from OWASP:
    - *Minimize attack surface area*
    - *Establish secure defaults*
    - *Principle of least privilege*
    - *Principle of defense in depth*
    - *Fail securely*
    - *Don't trust services*
    - *Separation of duties*
    - *Avoid security by obscurity*
    - *Keep security simple*
    - *Fix security issues correctly*

Summarizing:
Security architecture -> Secure architecture

- ✗ No wall between security and enterprise architects
- ✗ Mindset change towards «Security by design»
- ✗ Continuous security awareness program
- ✗ Internal criminals
- ✗ Integrate security into EA
- ✗ From rules to principles

GETTING BACK TO THE MAIN QUESTION

DO ARCHITECTS NEED TO BE SECURITY EXPERTS?

ARCHITECTS NEED TO BE SECURITY ~~EXPERTS?~~

AWARE

THANKS!

Any questions?

You can find me at
@texnokot
victoria.almazova@microsoft.com