

# **Security Testing – Introduction**

SAST 2012-11-22

**Anders Fristedt & Per Strömsjö, IT Security @ SEB**

# One view on Security

Security is the degree of protection to safeguard a nation, union of nations, persons or person against danger, damage, loss, and [crime](#). Security as a form of protection are *structures and processes that provide or improve security as a condition.*

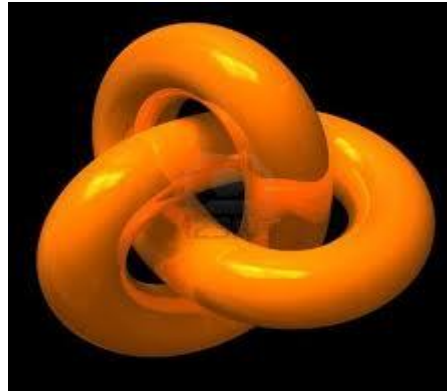
Source: en.wikipedia.org



**...a law enforcerer, firefighter or life saviour?**

# Another view on IT Security

Security is the quirky things someone else requires creative and business oriented people<sup>1</sup> to do in the last minute in stead of providing business value. Security is the snake-oil needed to pass through thongs of controls, forums and control instances.



**...someone to get around, and end-less loop or the eye of a needle?**

1) E.g. Developers, Architects and Project Leaders

# IT Security is about managing Risk

**Information Security Risks are managed through ensuring the correct levels of Information Security qualities**

**Confidentiality:**  
Ensuring the secrecy of information



**Integrity:**  
Ensuring correctness of information

**Availability:**  
Ensuring the availability of information and systems

# Reporting of it security in media

FREDAG DEN 9 NOVEMBER, UPPDATERAD FÖR 2 MINUTER SEDAN

## SvD NÄRINGSGLIV

START NYHETER LIVE BÖRS BRANSCHER INVESTERA ANALYS MOTOR

Industri & fordon Handel & tjänster Energi & råvaror Bank & fastighet Teknik & telekom

### Bedragare fick upp konton via Facebook

Bedrägerihärvan i Sparbanken Öresund växer. Mångmiljonbelopp har hittats på Egypten. Bedragarna har använt bankens Facebooksida för att elektroniskt dyrka kundernas konton.

### Hacker claims mass bank breach; releases Visa, Mastercard data

**Summary:** More than 79 banks have been breached, claimed a hacker on Twitter. Following a data release on Tuesday, he said he has more than 50 gigabytes of U.S. and foreign bank data in his hands.



By Zack Whittaker for Zero Day | June 19, 2012 -- 09:33 GMT (02:33 PDT)

Follow @zackwhittaker

Comments 69 Vote 1 Like 670 Tweet 275 Share more +

Update: see below.

A hacker, who claimed on Twitter to have illegally accessed the networks of dozens of large banks, has released a vast cache of personal information relating to Visa and Mastercard credit card data.

ANDREAS

Världen  
Cervenkas pe

2012-10-01 11:48 Computer Sweden

### Ddos-attack mot TT

Av Jonas Ryberg | CS ComputerSweden



Nyhetsbyrån TTs tjänster ligger nere efter en överbelastningsattack.

ARTICLE

### Societe Generale: A cautionary tale of insider threats

Bill Brenner, Senior News Writer

Published: 31 Jan 2008



The \$7.2 billion in fraud a rogue trader carried out against French banking giant Societe Generale wasn't an attack against a flawed operating system or application, the kind of threat enterprise IT shops are constantly warned about. Instead, security experts say the incident illustrates something potentially worse -- the damage that can ensue when a trusted insider with sinister ambitions learns the inner workings of the company network.

## SvD NÄRINGSGLIV

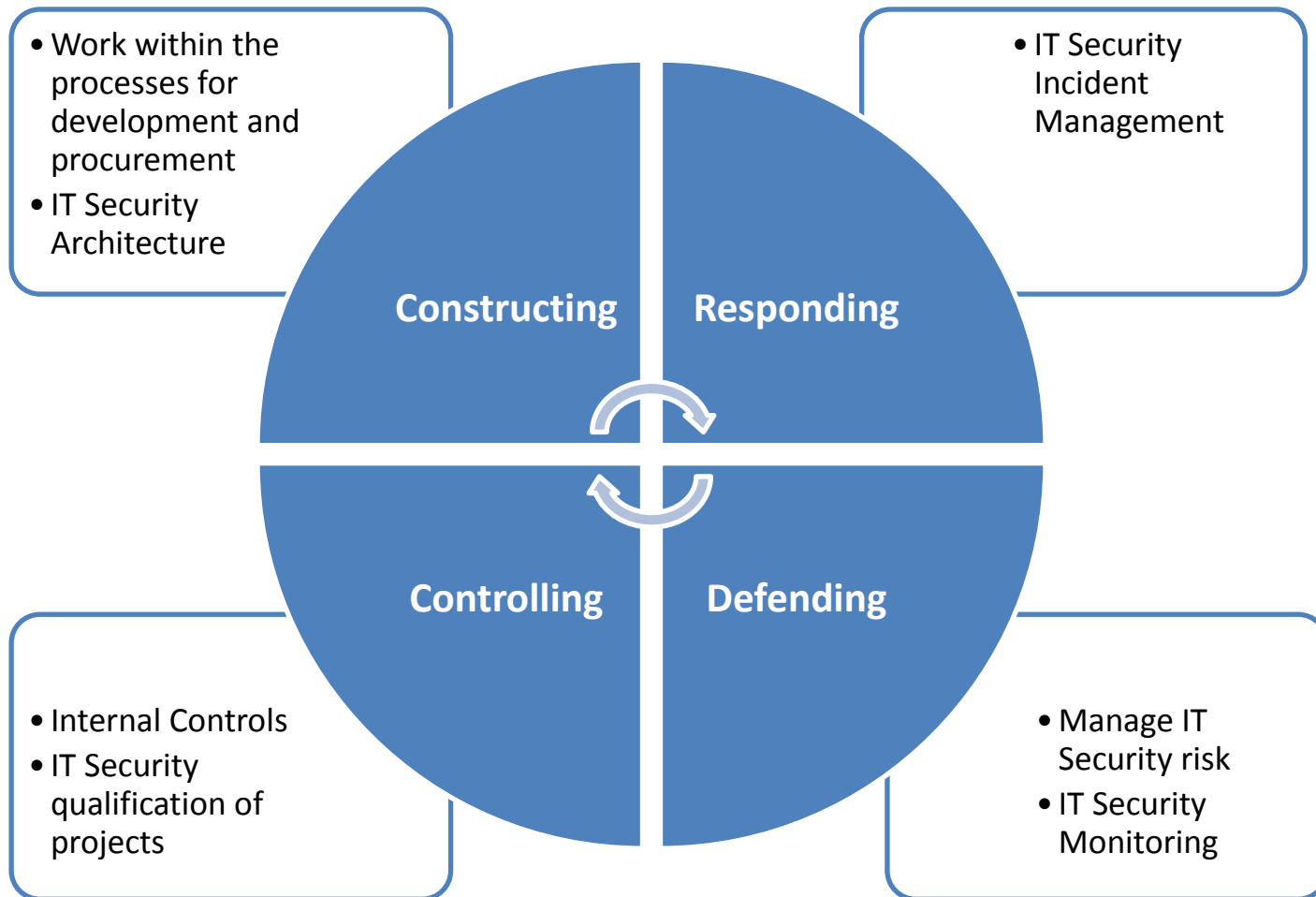
Cervenkas pe

START NYHETER LIVE BÖRS BRANSCHER INVESTERA ANALYS MOTOR

### Mångmiljonsvindlar på SEB

Ett 20-tal kunder i banken SEB har svindlats på sammanlagt 52 miljoner kronor, rapporterar Ekonominyheterna i TV 4.

# IT Security – fire fighting or process oriented daily business?



# Objectives with SEB's IT Security

- Support line organization as Subject Matter Experts
  - We must fight the view of IT Security Professionals as omnipotents know-it-all problemsolvers!
- Focus on the End-to-End perspective within applied IT Security
  - *"Security is not a product, it's a process" (Bruce Schneier)*
- Being First Point of Contact within issues concerning IT Security
  - SEB has several groups concerned with Information Security, Compliance and Risk

# Security Testing: Qualities

- Security is about Quality
- Information Security part of Information Quality
- Security Qualities
  - Confidentiality
  - Integrity
  - Availability
- Not a last-minute fix



# Security Testing: Requirements

- Security Requirements define Security Qualities
- Business is information
- Is our business secure?
- Can we bet our business on this system?
- How can we have assurance?

# Security Testing: Assurance

- Establishing confidence that a system...
- conforms to requirements or standards
- functions as intended
- is free of exploitable vulnerabilities





# Security Testing: Informed by Risk

- How much Assurance do we need?
- Risk in the business
  - e.g. sensitive to fraud
- Risk in system development/maintenance
  - planning
  - robust methods
    - Secure Development Life Cycle
  - trusted parties

# Security Testing: Assurance Practices

- *Formal* assurance
  - e.g. Common Criteria
- *Informal* assurance through practices
  - Analysis of Security Architecture
  - Code review with tools
  - Security Testing...
  - ...

# Security Testing: Scope v/s Requirements

<b>Requirement Category</b>  <b>Scope</b>	<b>Functional</b>	<b>Non-functional</b>
<b>Component</b>		
<b>Holistic</b>		

# Security Testing: Use & Abuse

**Does what it should do**



**Does not do what it should not do**

# Security Testing: The Adversary

- How is Security Testing different?
- Expect attacks!
- Probe resilience in the face of attacks
- Think like an adversary
  - How much does he know?
  - Given that knowledge, what can he do?
- Uncover vulnerabilities





# Security Testing: An Assurance practice

*Establishing confidence that a system protects data and functions as intended in the face of attacks.*

- Non-functional
  - security qualities
- Functional
  - security functionality, e.g. security logging



# Security Testing: Hats & Boxes

Knowledge	Black Box	White Box
<b>Role</b>		
<b>Black Hat</b> <i>the attacker</i>		
<b>White Hat</b> <i>the defender</i>		

# Security Testing: Security As A Process



# Security Testing: “Plan, Do, Check, Act”

- Test Plan
  - Scope, purpose and goals
  - Why do you do this?
  - Test Specification
- Test Protocol
- Test Report
  - Objectives
    - Business relevance through risk perspective
    - Traceability from plan to findings

# Security Testing: The “Badness-O-Meter”



© Gary McGraw

# Security Testing – Introduction

...and, finally:

*Security Testing is not secure testing...*