

# Risk Assessment in product development

Patrik Frost

## What's it all about?

If  $\tau_A = \inf\{n \geq 0 : X_n \in A\}$ , then  $P_z(\tau_A < \infty) > 0$  for all  $z$ .

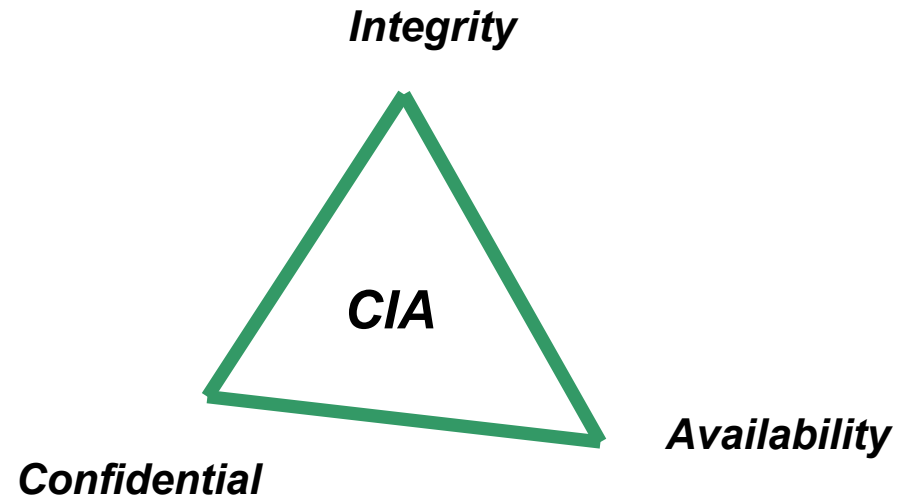
$$\begin{aligned}\Pr(X_n = i \mid X_{n+1} = j) &= \frac{\Pr(X_n = i, X_{n+1} = j)}{\Pr(X_{n+1} = j)} \\ &= \frac{\Pr(X_n = i) \Pr(X_{n+1} = j \mid X_n = i)}{\Pr(X_{n+1} = j)}.\end{aligned}$$

If  $x \in A$  and  $C \subset B$ , then  $p(x, C) \geq \varepsilon p(C)$ .

# What's it all about?

Product security is like a chain, it is not stronger than its **weakest** link!

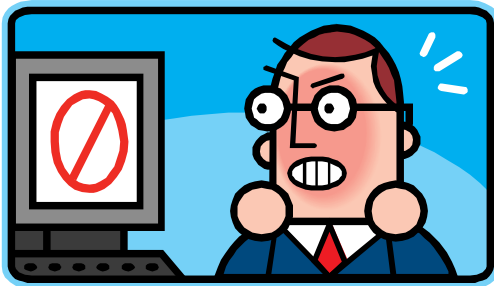
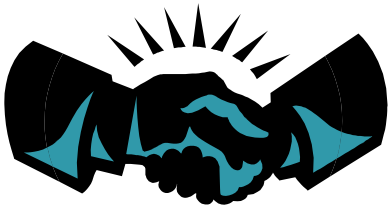
- It is also a balance between **availability** and **protection**.
- This presentation is not about organizational security (ISO27001)



# Key Assets

# Assets

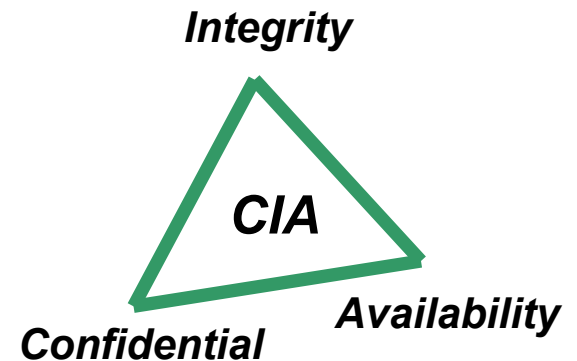
- Assets that is of high **value**, and will result in large financial **loss**, are considered key assets.
- **Asset can be tangible or intangible.**
- Examples of intangible assets are goodwill, copyrights, trademarks, patents, computer programs, files, information.
- Tangible assets are those that have a physical substance and can be touched, e.g buildings, machines e.t.c.



# Threats

# Threats to the key assets

- The act of someone or a group to **misuse** the asset in a negative and/or not intended way.
- Analyzing **the world around one** to identify possible threats.
- Analyzing threats gives understand of what can happen with the assets, and what type of security that is necessary!



# Vulnerabilities

# Vulnerabilities

- Assets has **weaknesses** that can be exploited by others with intent to damage or steal.
- These weaknesses must be blocked by protection.
- Examples of vulnerabilities are:
  - Weak or no **password**.
  - Weak protection of assets **environment**, e.g OS.
  - No security training for **staff** handling asset.
  - No or insufficient protection from **physical** access.
- Don't forget to do vulnerability test.



# Existing protection

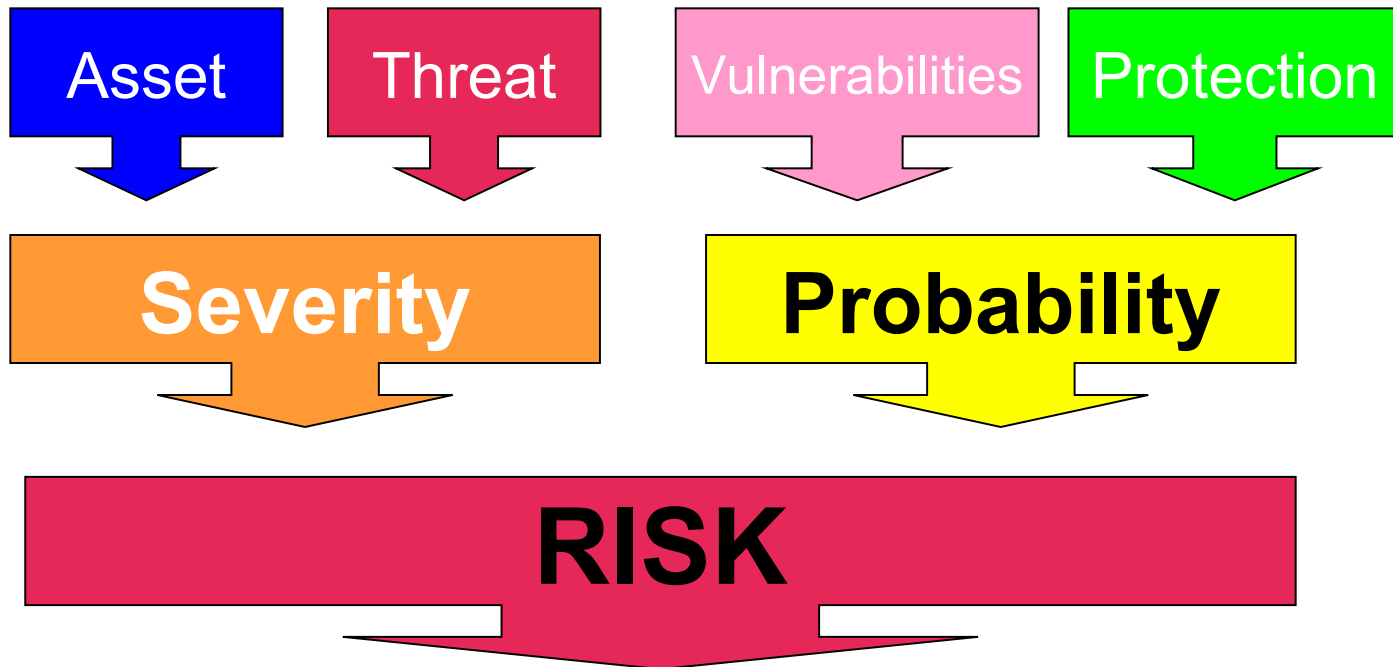
# Existing protection

- Consideration must be taken to any existing protection, or planned protection.
- Assets environment might need Hardening!



# Risk

# What is a risk?



# Risk Level matrix

		Severity		
		Low 10	Medium 50	High 100
Probability	High 1,0			1x100
	Medium 0,5			
	Low 0,1	0,1*10= 1		



# Reference to processes

- Octave (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM ):  
<http://www.cert.org/octave/>
- ISO 31000 [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=43170](http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170)
- Microsoft: The Security Risk Management Guide
- Risk Management Guide for Information Technology Systems  
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>



# Thank you

Patrik Frost

Tieto Sweden  
Patrik.frost@tieto.com