



Desafios da Gestão da Segurança

Marco Vaz, CISSP, CISA, ISO 27001 Lead Auditor
Information Security Solutions Manager

marco.vaz@oni.pt



"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

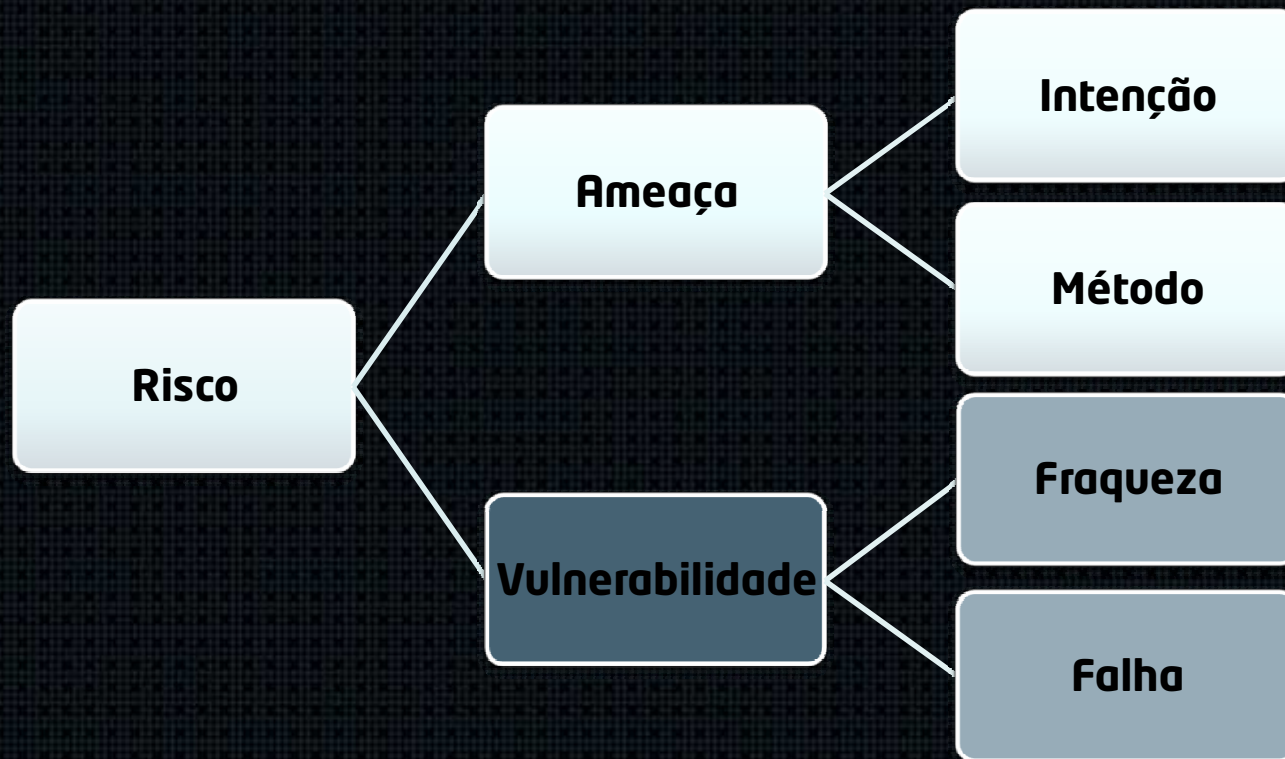
Bruce Schneier



Driver da Gestão da Segurança: RISCO

Todas as organizações estão expostas a factores de **risco** que podem ter **impacto negativo** na sua **continuidade**.

Risco = Ameaça x Vulnerabilidade



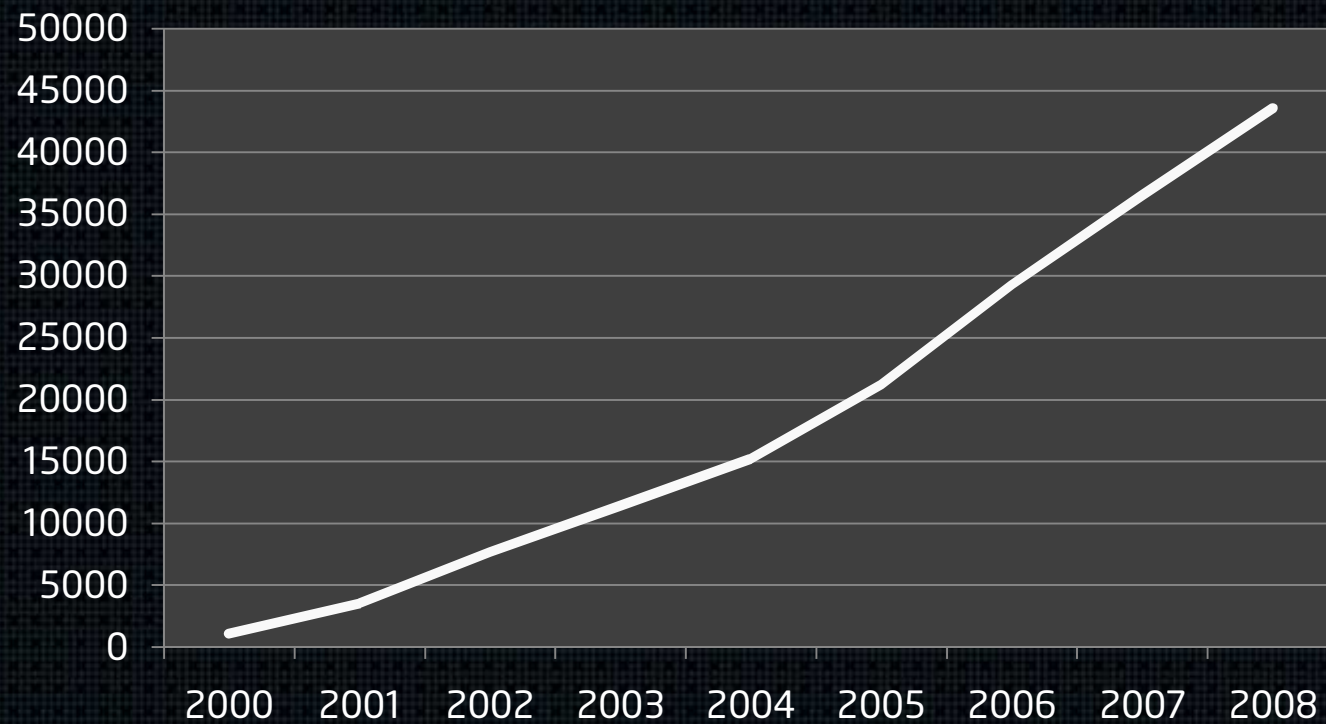
Risco = Ameaça x Vulnerabilidade



Risco = Ameaça x Vulnerabilidade

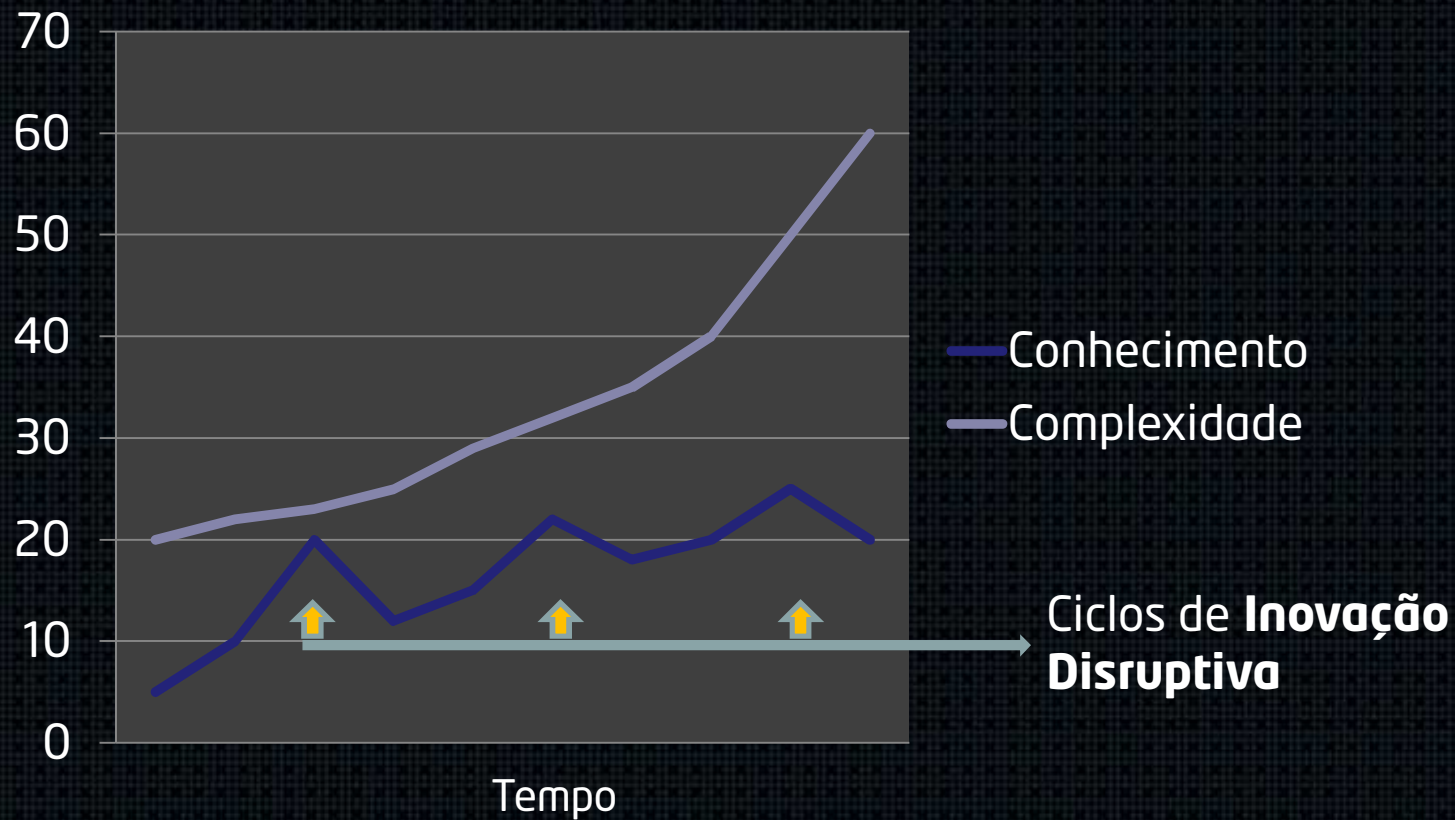
Sum

(Vulnerabilidades de *software* Publicadas)

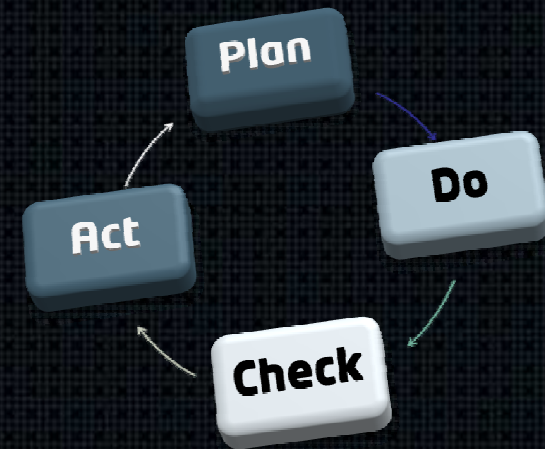


www.securityfocus.com

Risco = Ameaça x Vulnerabilidade



Como Medir o Risco?



Gestão da Segurança: Objectivos

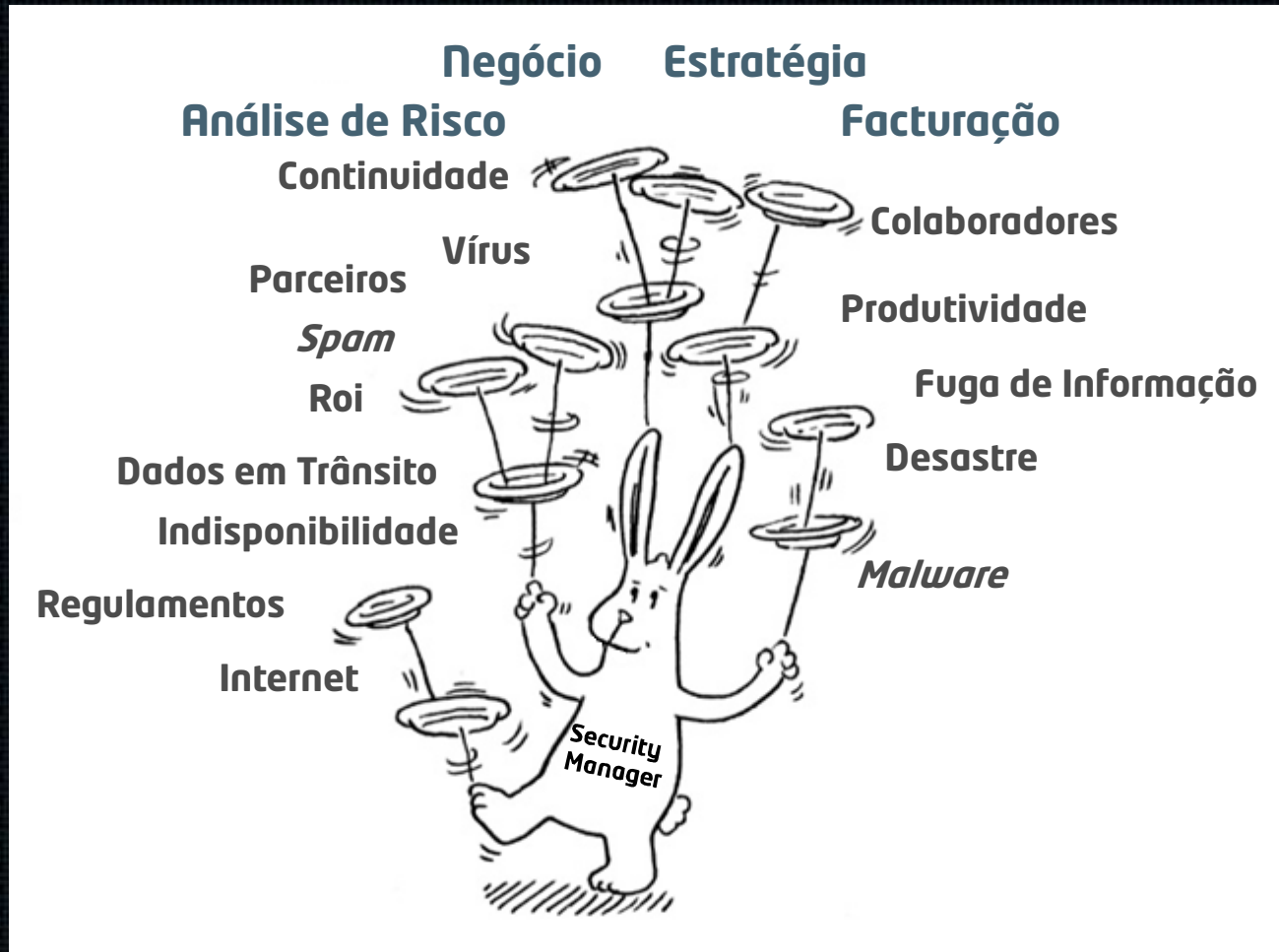
- Orientação estratégica da organização face ao risco.
- Facilitar o negócio.
- Redução do risco a um nível aceitável.

Gestão da Segurança: Ferramentas

- Análise de risco
- Plano de segurança
- Políticas, Standards, Guidelines, etc...
- Processos
 - *Incident Handling*
 - *Vulnerability Management*
 - *Business Continuity Management*
 - *Awareness Training*

...

Equilíbrio Dinâmico



ALGUNS PRINCÍPIOS DA GESTÃO DA SEGURANÇA

Estabelecer Fundações Sólidas

- Definição de uma estratégia.
- Aprovação pela gestão de topo.
- Montar um sistema de gestão de segurança da informação.

Princípio da Proporcionalidade:

Fazer mais com menos

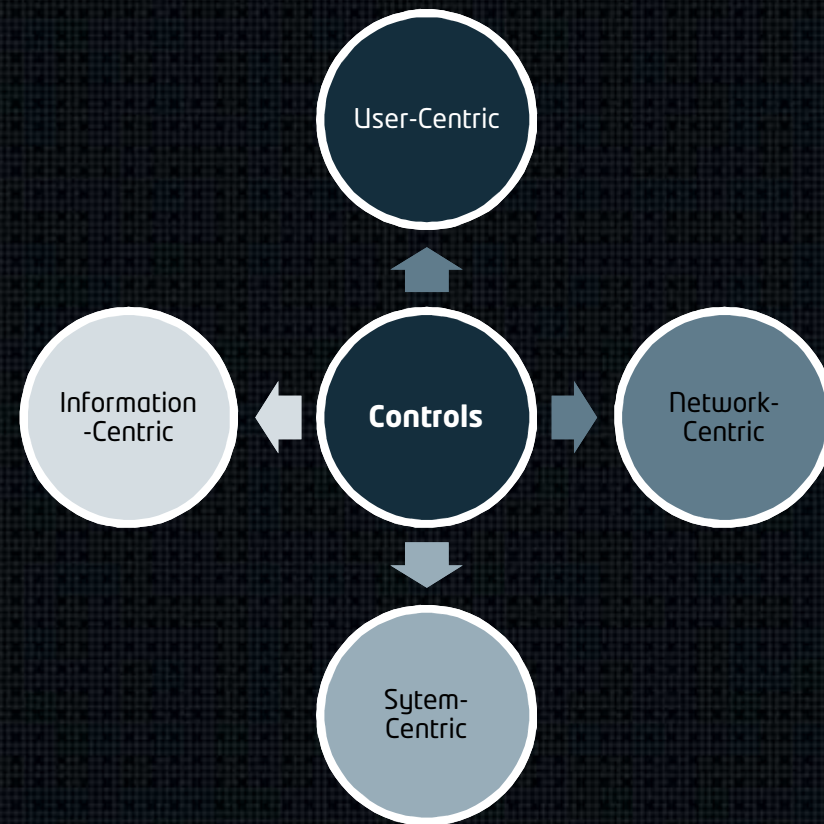
- Apenas os controlos necessários.
- **NÃO** aumentar a complexidade com controlos redundantes.

Segurança como Propriedade

- Segurança como propriedade de um sistema e não como *add-on*.
- Segurança desde o desenho à implementação e operação dos sistemas.

Segurança nas Diferentes Fases da Informação

- Criação
- Processamento
- Trânsito
- Armazenamento
- Destruição



Classificação da Informação

- Identidade
- Proprietário
- Custódia
- Tipo de Conteúdo
- Criticidade - CIA

Segurança Transcende a Tecnologia

"Security is Not a Product; It is a Process."

Bruce Schneier

Risk Management

Awareness Training

Performance Management

Identity & Access
Management

Change Management

Vulnerability management

Incident Handling

EXISTE RETORNO DO INVESTIMENTO EM SEGURANÇA?



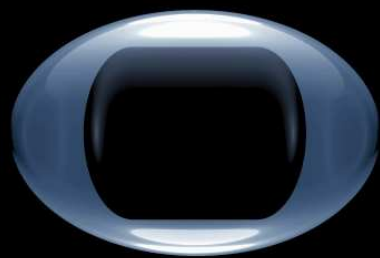
NÃO, quando os controlos não vão ao encontro dos riscos...



SIM, quando o investimento é baseado numa análise dos riscos e orientado às necessidades do negócio.

Q&A

OBRIGADO!



oni communications

youuniversal business solutions

www.onicomunications.pt