



# Riscos Cibernéticos

## Tendências, Desafios e Estratégia para IoT

**Paulo Pagliusi** Ph.D., CISM – [ppagliusi@deloitte.com](mailto:ppagliusi@deloitte.com)

Diretor de Cyber Risk Services

[www.pagliusi.com.br](http://www.pagliusi.com.br)

[www.deloitte.com](http://www.deloitte.com)



**Deloitte.**

# Risco Cibernético: Contexto - [Video](#)

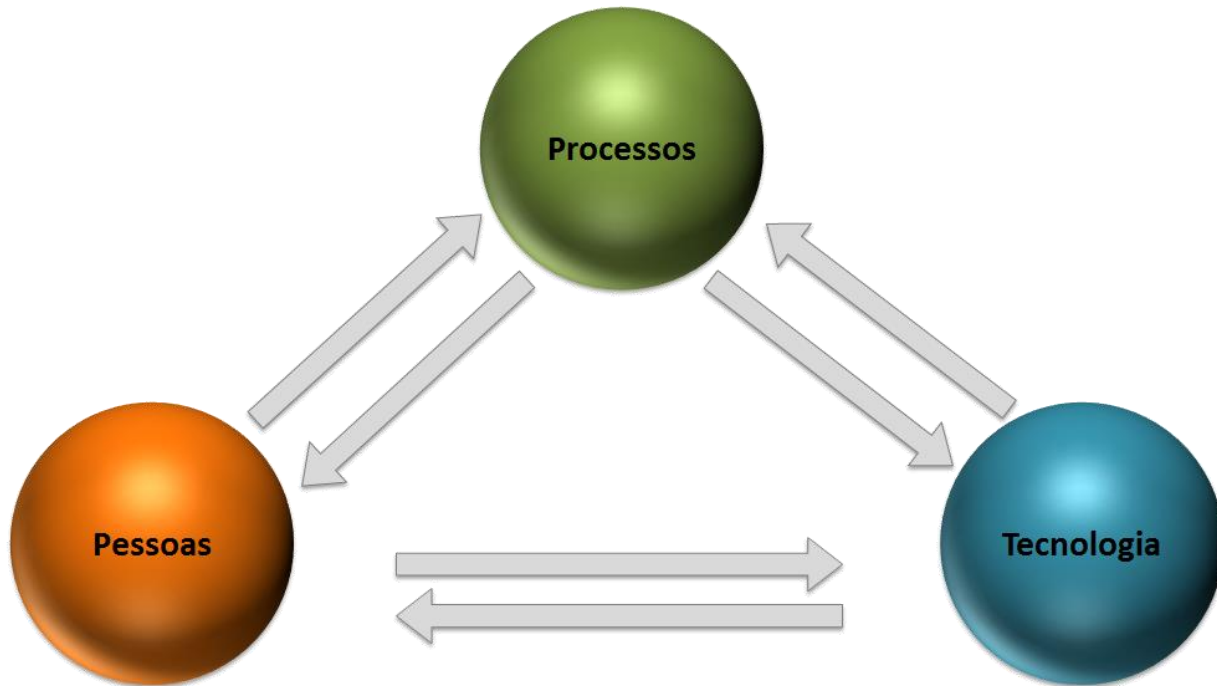


**Fonte: Deloitte** – A Company Like Yours <http://www2.deloitte.com/global/en/pages/risk/articles/cybervideo-companies-like-yours.html>



# Segurança da Informação

## Fator crítico de sucesso



Segurança > Matérias > Avião que oferece internet sem fio pode ser hackeado, afirma relatório



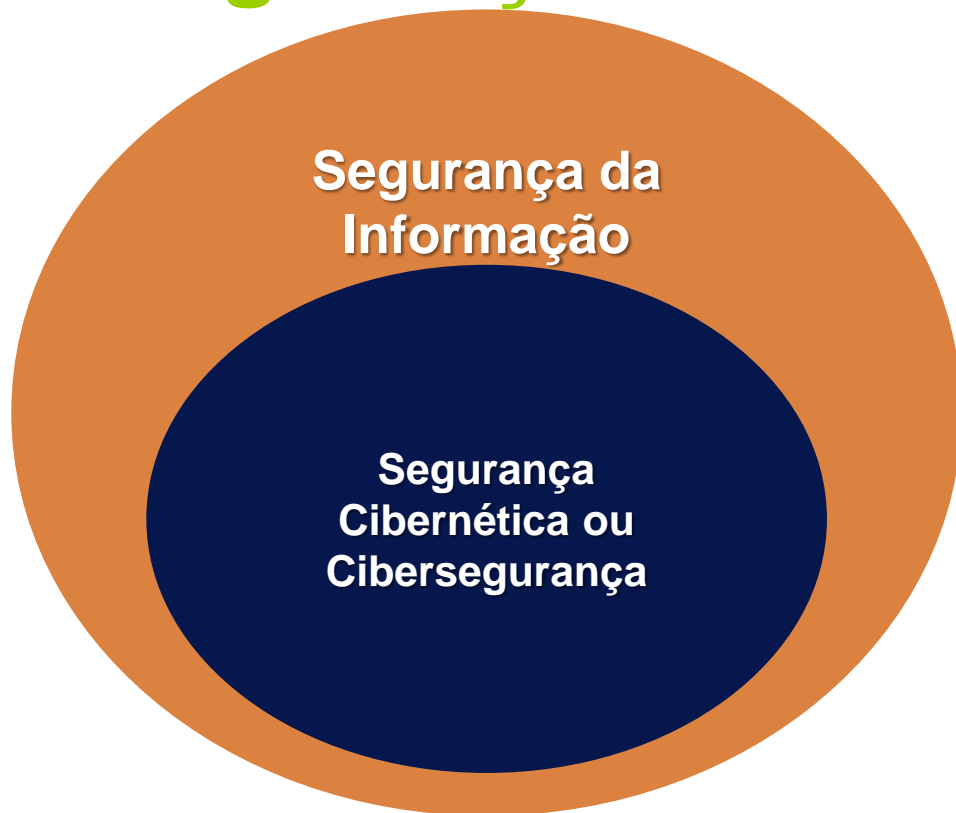
[http://olhardigital.uol.com.br/fique\\_seguro/noticia/aviao-que-oferece-internet-sem-fio-pode-ser-hackeado-afirma-relatorio/47990](http://olhardigital.uol.com.br/fique_seguro/noticia/aviao-que-oferece-internet-sem-fio-pode-ser-hackeado-afirma-relatorio/47990)

(Foto: Divulgação)

Avião que oferece internet sem fio pode ser hackeado, afirma relatório



# Segurança Cibernética



ISO IEC 27000 Series –  
Information Security Standards

ISO IEC 27032 - Guidelines for  
Cybersecurity:

- **Cibersegurança:** preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação no **Ciberespaço**
- **Ciberespaço:** Ambiente complexo, resultante da interação de pessoas, software e serviços na Internet, por dispositivos de tecnologia e redes conectadas





# Sistemas Cognitivos & Ameaças Cibernéticas



- Para a nova era tecnológica ser direcionada pela **experiência cognitiva**, em que computadores contribuirão com pensamento lógico do ser humano e talvez o contestem, é preciso garantir que os **sistemas cognitivos** – capazes de criar grandes mudanças e inovação disruptiva via automatização das tarefas tácitas – façam frente às **ameaças cibernéticas** presentes no espaço cibernético
- Novas **capacitações** serão solicitadas e novos modelos de negócio surgirão – é preciso **adaptar** os controles internos da sua organização, para minimizar crescente impacto de crises cibernéticas na sociedade e na economia



# Tendências em Cibersegurança

*Em 2020, 75% do orçamento de segurança cibernética será investido em detecção e resposta imediata de incidentes. Atualmente é menos de 10% dos investimentos.*



**Mercado global de Cyber Security:** US\$75 B (2015) a \$170+ B (2020): CAGR 10.3% [Gartner](#)



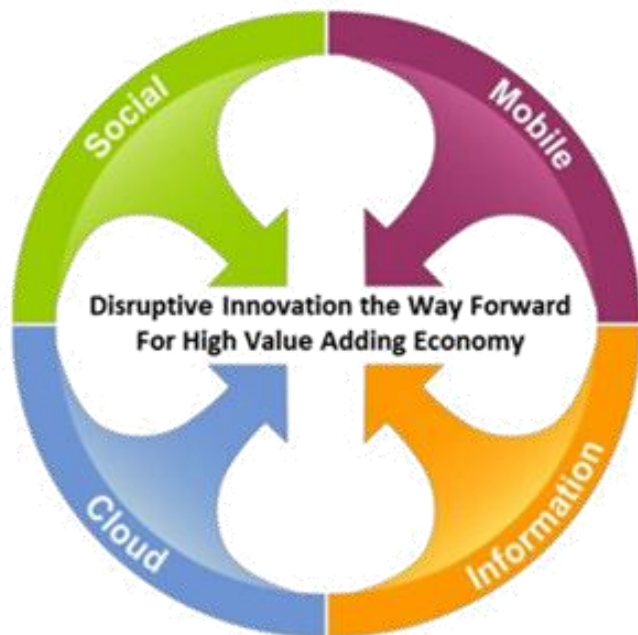
**Ciber incidentes:** Perdas anuais de US\$1 MM para entidades com receitas entre \$100 MM a \$1 B. Para entidades maiores (receita > \$1+ B), déficit \$5+ MM [Computerworld](#) (2015)





# Nexus of Forces (Gartner)

## 3ª Plataforma da TI (IDC)



The Nexus of Forces

Source: Gartner 2013

IDC: em 2020, +80% do crescimento da indústria de TIC será impulsionado pelas tecnologias da 3ª Plataforma



**4 Forças Vitais para Viabilização da Era dos Sistemas Cognitivos**



# Era dos Sistemas Cognitivos

Força a proteger para viabilizar - Nuvem





# Era dos Sistemas Cognitivos

Força a proteger para viabilizar – Mobilidade



**Toque:** Você poderá tocar através do seu telefone

Imagine usar seu smartphone para comprar vestido de casamento e **poder sentir** a seda do vestido, ou a renda do véu, tudo pela superfície da tela. Ou sentir as miçangas e o trançado de um lençol feito por um artesão local a meio mundo de distância.

Cientistas estão desenvolvendo aplicativos para setores como **varejo** e **saúde**, com tecnologias sensíveis hápticas, de infravermelho e pressão, simulando toque.

Qual o Risco Cibernético envolvido?

**Vídeo:**

Como funcionam os ataques a celulares



# Era dos Sistemas Cognitivos

Força a proteger para viabilizar – Social Business



inherittthemirth.com ©2011 Cuyler Black

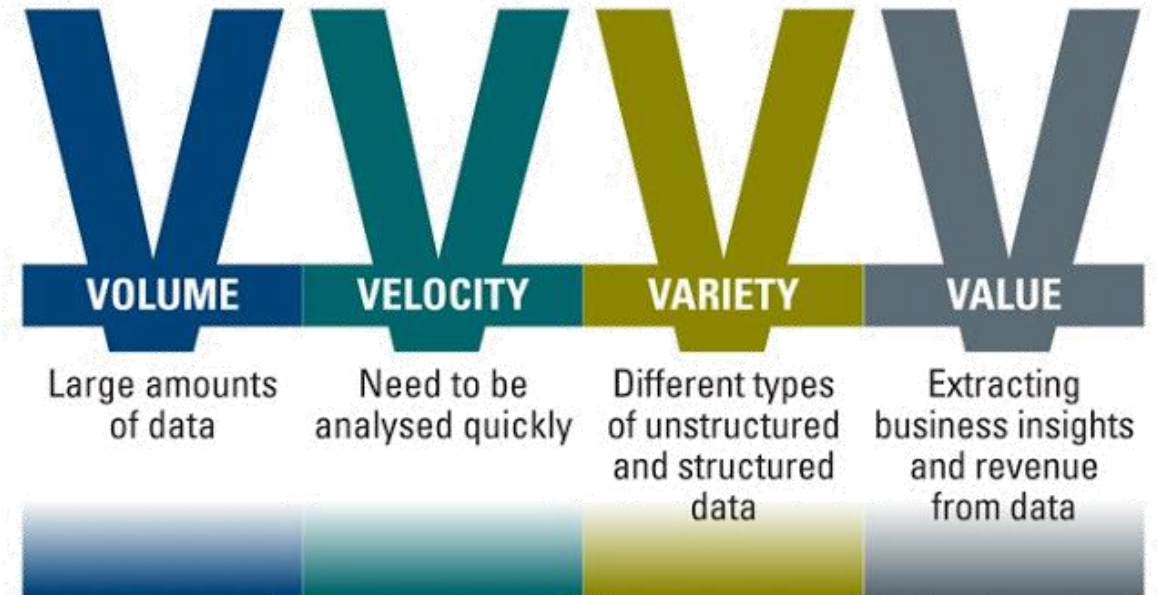




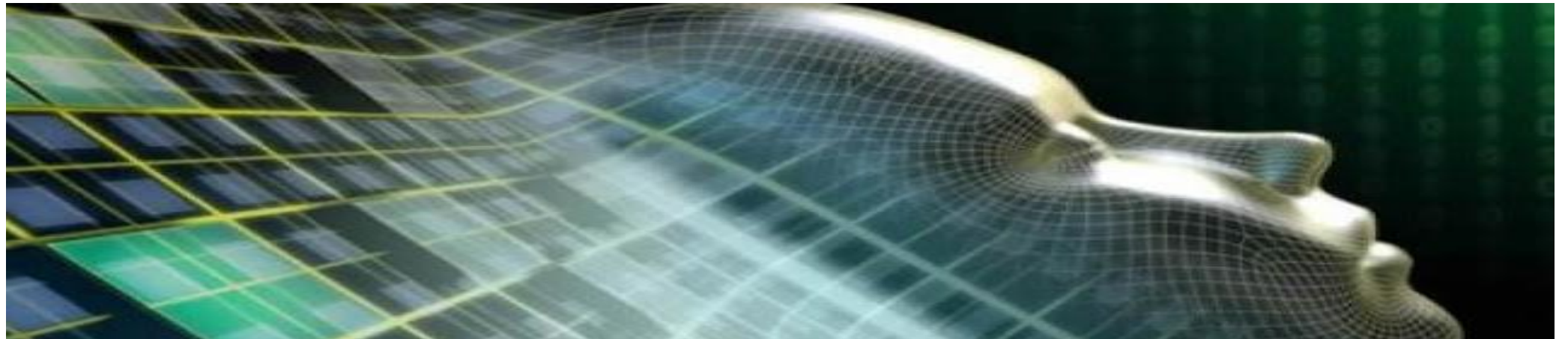
# Era dos Sistemas Cognitivos

Força a Proteger para viabilizar – Informação

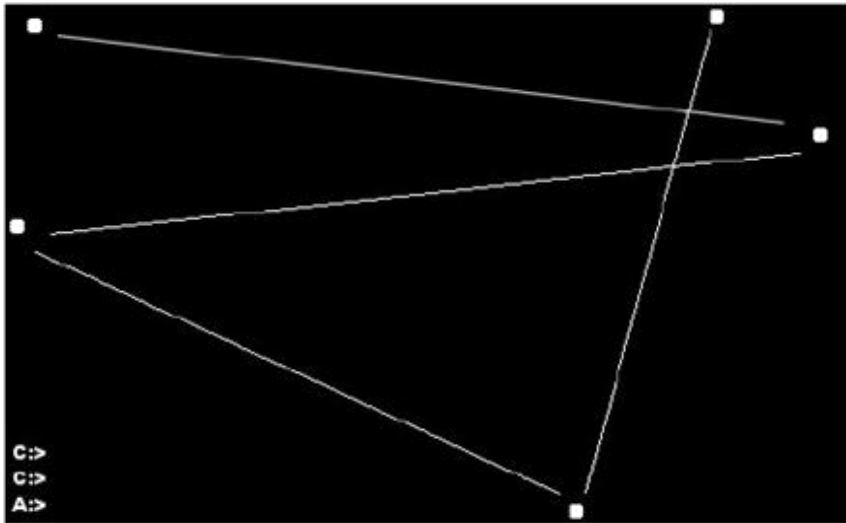
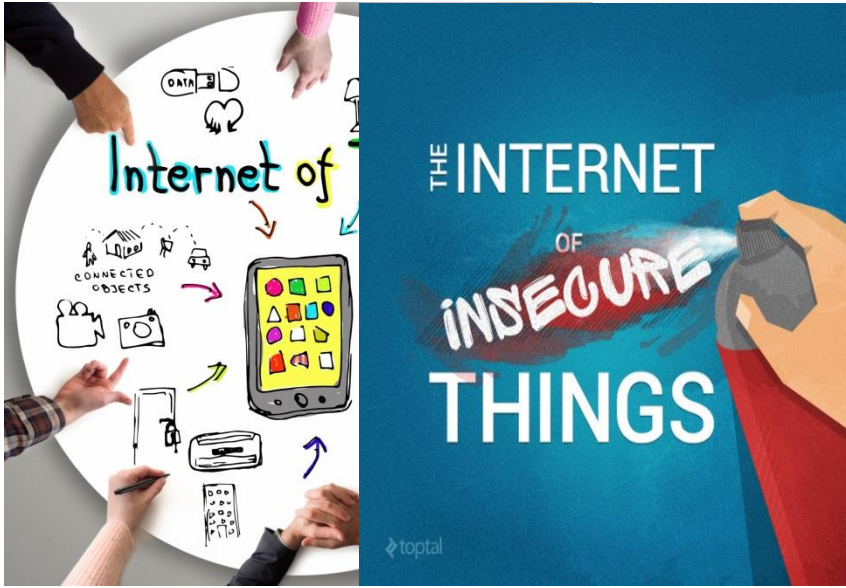
(Big Data/Analytics)



© World Newsmedia Network 2013



# +Desafios: Internet das Coisas (IoT), Deep Web, Malwares





## +Desafios: O Eterno Usuário...



# Estado atual das Ameaças Cibernéticas à IoT

Ameaças de Ataques Persistentes Avançados



Malwares Dinâmicos e Polimórficos



**NOVO CENÁRIO DE AMEAÇAS À IoT**



Ataques Multi-Vetor



Ataques Multi-Staged

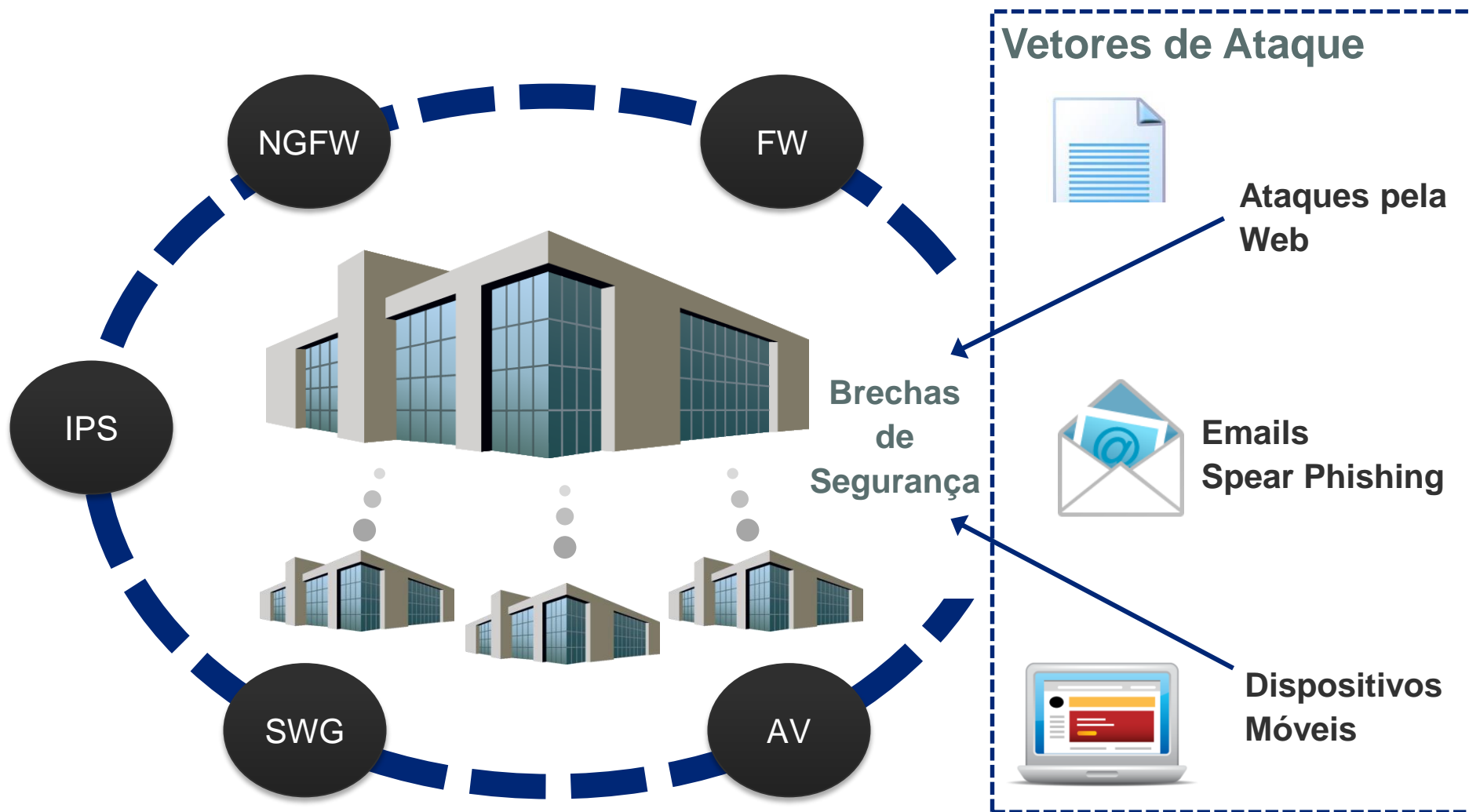




# Arquitetura de Defesa Típica de uma Organização



# Arquitetura de Defesa Típica – Portas de entrada

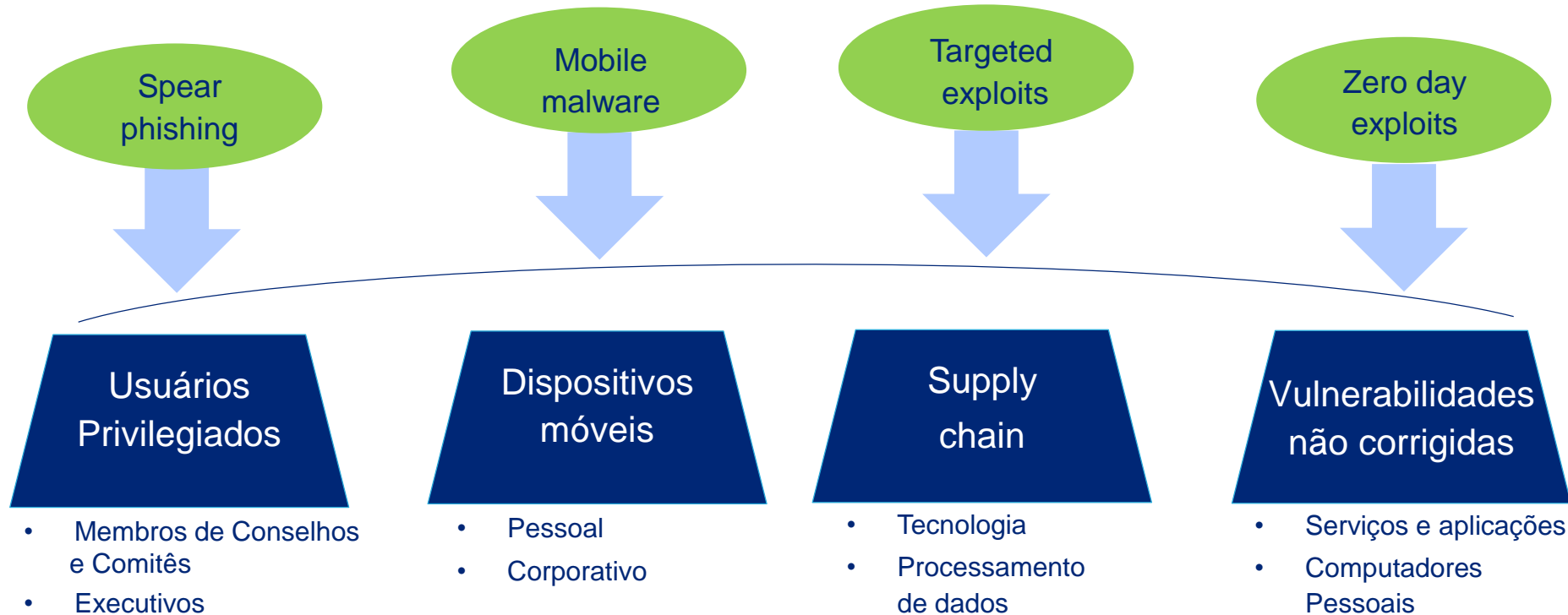




# Cenário de Risco à IoT

## Brechas nos Processos

Após análise de recentes brechas e do desenvolvimento ocorrido no underground cibernético, foram identificadas áreas precisando de melhorias e monitoramento contínuo em processos de TI que apoiam as organizações



# Fatores de risco à IoT

## Ransomware

Malware que infecta o dispositivo informático e restringe o acesso da vítima a seus arquivos ou ao dispositivo, exigindo taxa de resgate (ransom) para retornar ao serviço regular. Mecanismo de extorsão digital (ciber extorsão) utilizado por hackers.

### Ameaça Multiplataforma



- Windows
- MAC OS
- Dispositivos iOS
- Dispositivos Android



### Pesquisa



Apenas **3 em cada 10** empresas brasileiras reconhecem a ameaça do ransomware<sup>1</sup>

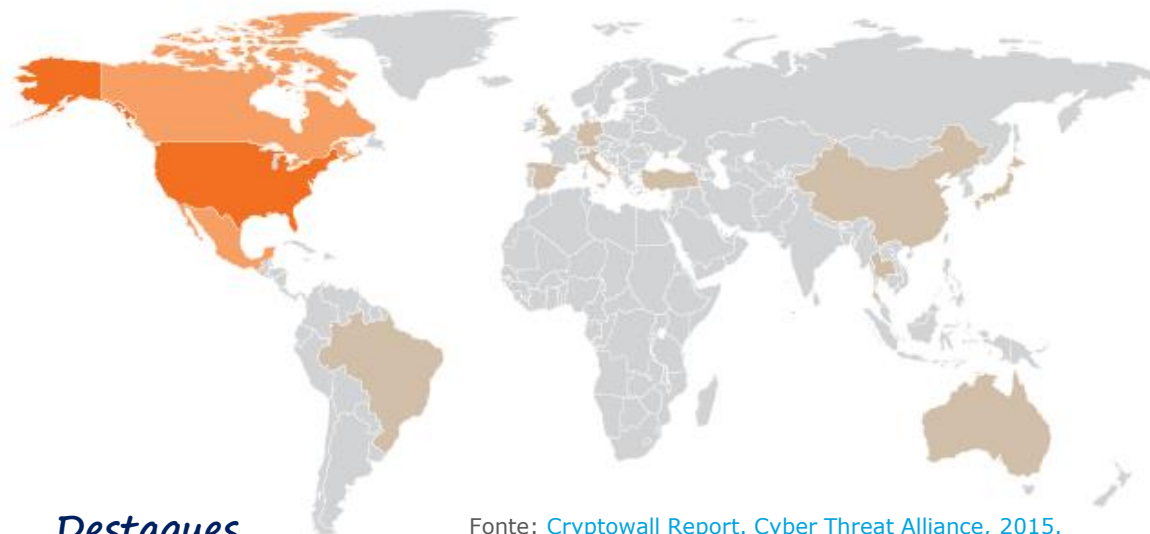
Fonte: [Kaspersky Lab, 2015.](#)



### Bitcoin

Os pedidos de resgate dos dados são feitos por meio de moeda digital como o bitcoin, devido as suas **características de irrestreabilidade.**

### Os países mais atacados por Ransomwares



Fonte: [Cryptowall Report. Cyber Threat Alliance, 2015.](#)

### Destaques

- 1 O FBI estima que os Ransomwares ultrapassem **US\$ 1 bilhão** em extorsões no ano de 2016. No primeiro trimestre, os dados da organização registraram perdas de **US\$ 209 milhões** com ataques dessa natureza .
- 2 Em 2013, a agência ZDnet descobriu que os donos do CryptoLocker já haviam arrecadado quase **US\$ 27 milhões** com suas fraudes.
- 3 Na atualidade, Cryptolocker já utiliza uma chave quase "Impossível" de decifrar (RSA de 2048 bits).



### Notícias Relevantes





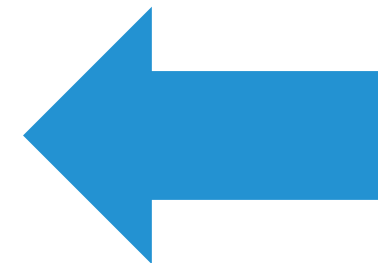
# Fatores de risco à IoT

## Pesquisa Deloitte – Jun2016 - Beneath The Surface of a Cyber Attack

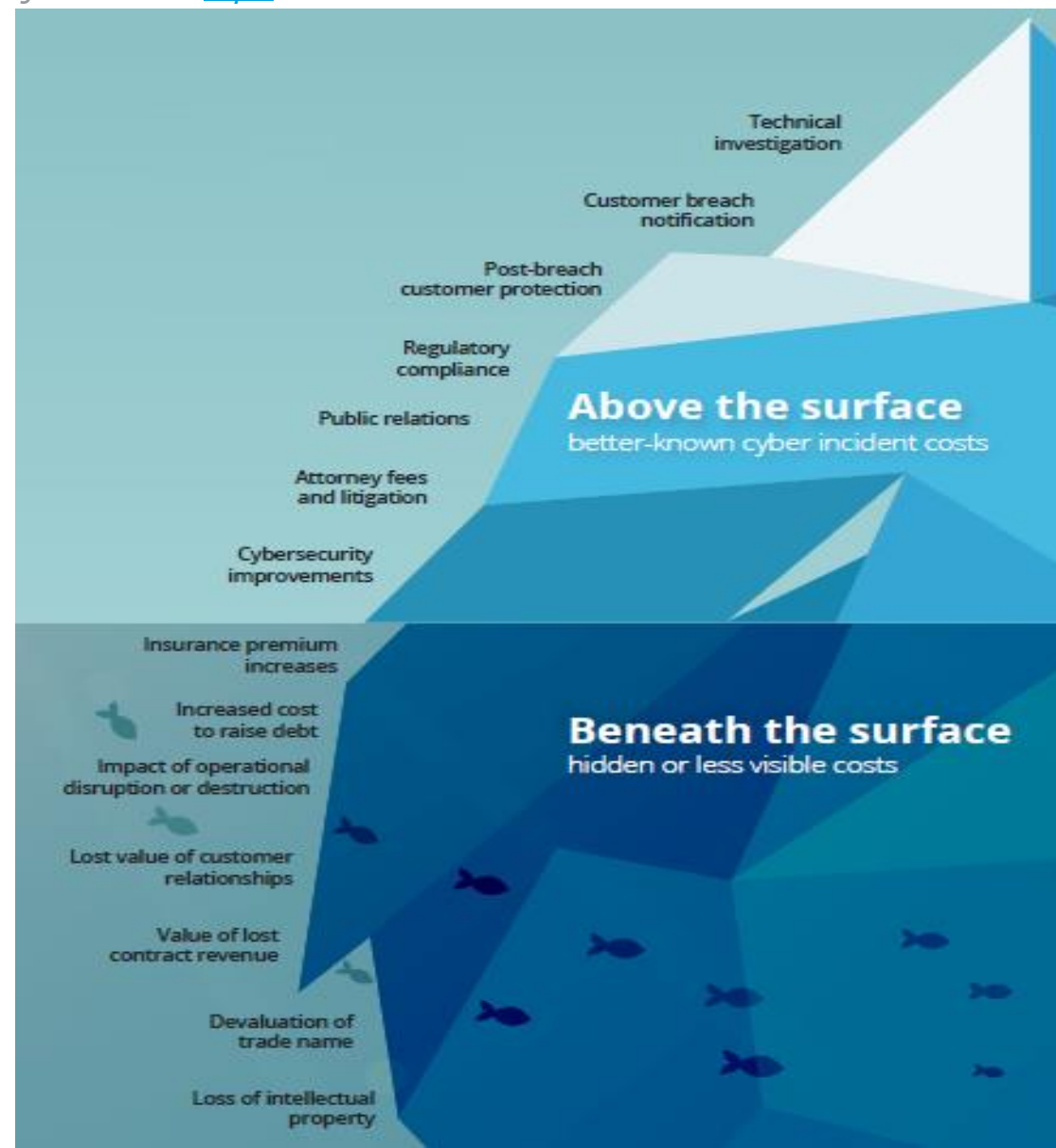
A Deloitte desenvolveu pesquisa mundial com mais de 1000 clientes em várias indústrias, com foco em Boards e C-Level Executives, a fim de avaliar principais impactos e ocorrências de Risco Cibernético hoje. Acesse [aqui](#) o relatório.

	Impact factor	Term	% Total cost	
Above the surface	Post-breach customer protection	3 years	1.25%	
	Cybersecurity improvements	1 year	0.83%	
	Customer breach notification	6 months	0.60%	
	Attorney fees and litigation	5 years	0.60%	
	Regulatory compliance (Health Insurance Portability and Accountability Act (HIPAA) fines)	1 year	0.12%	
	Public relations	1 year	0.06%	
	Technical investigation	6 weeks	0.06%	
	Beneath the surface	Value of lost contract revenue (premiums)	5 years	49.43%
		Lost value of customer relationships (members)	3 years	25.61%
		Devaluation of trade name	5 years	13.70%
Increased cost to raise debt		5 years	3.57%	
Insurance premium increases		3 years	2.38%	
Operational disruption		Immediate	1.79%	
Loss of intellectual property	Not applicable	0.00%		
<b>Total</b>			<b>100.00%</b>	

### Fatores de Impacto



**96,48%** custos escondidos ou menos visíveis



# Organizações divididas em 3 momentos



*Aquelas que sofreram vazamento e violações de dados*

*Aquelas que não sofreram – ainda*

*Aquelas que sofrem mas não sabem*

*“A maioria dos vazamentos e violações de dados, que se tornaram públicos nos últimos anos, demonstram que as organizações comprometidas podem passar semanas ou até meses antes de descobrir o que ocorreu.”*

Fonte: ISF Report e SC Magazine





# Reações Típicas de Executivos, Conselhos e Comitês

Diante de Riscos Cibernéticos capazes de comprometer a Organização & prejudicar inovações



***Isto é problema da TI...  
Mas... Cibersegurança não é TI***

# Perguntas Fáceis...

## Respostas Difíceis

### Presidente (CEO)

"Eu vi que nosso órgão vizinho/concorrente sofreu ataque de ativistas hackers. Estamos vulneráveis a isso também?"



### Conselhos e Alta Administração

"Qual nossa capacidade de preservar a reputação, se atacados por hackers?"



### Executivos do Órgão / de Negócios

"Quais os pontos fracos em nosso ambiente de controle interno?"



### CIO & CISO do Órgão/Empresa

"Qual investimento necessário para aumentar nossa capacidade de proteger ativos de informações?"

[Artigo](#) – Paulo Pagliusi: Jornal “Estadão” 10/05 (on-line) 31/05 (impresso) - **Como a cibersegurança pode ajudar na gestão dos negócios?** [Como falar ao Conselho](#)



# Maturidade na Gestão do Ciber Risco

*É preciso elevar o grau de maturidade da gestão do ciber risco, sem gastar uma fortuna em tecnologia, investindo também em pessoas & processos*

**Três formas de investir melhor, para maior maturidade – adotar um Modelo que seja:**



- **Resiliente:** para conter os danos e minimizar impactos de uma crise cibernética
- **Seguro:** obter benefícios da transformação provocada pela segurança da informação, com proteção aos ativos mais sensíveis ao risco
- **Vigilante:** capacidade de detecção proativa, inteligência e consciência situacional sobre ameaças cibernéticas






# Modelo de Inteligência Cibernética para IoT



# Gestão de Crise Cibernética - [Vídeo](#)

☰ YouTube BR

🔍



A day like any other

Deloitte

# Vamos interagir?

1. **Você tem 1 minuto para pensar em 3 aspectos principais que irá levar consigo sobre os assuntos que discutimos hoje**
2. **Agora olhe para seu colega à direita**
3. **O último da fileira pode olhar para a esquerda**
4. **Ouçã o que seu colega acredita que são os 3 principais aspectos que levará consigo**
5. **Vocês concordam com os mesmos pontos?**







# Riscos Cibernéticos

## Tendências, Desafios e Estratégia para IoT

**Paulo Pagliusi** Ph.D., CISM – [ppagliusi@deloitte.com](mailto:ppagliusi@deloitte.com)

Diretor de Cyber Risk Services

[www.pagliusi.com.br](http://www.pagliusi.com.br)

[www.deloitte.com](http://www.deloitte.com)



*Muito  
Obrigado!*

**Deloitte.**



# Deloitte.



"Deloitte" refere-se à sociedade limitada estabelecida no Reino Unido "Deloitte Touche Tohmatsu Limited" e sua rede de firmas-membro, cada qual constituindo uma pessoa jurídica independente e legalmente separada. Acesse [www.deloitte.com/about](http://www.deloitte.com/about) para uma descrição detalhada da estrutura jurídica da Deloitte Touche Tohmatsu Limited e de suas firmas-membro.