



# Os desafios da Segurança da Informação num planeta mais inteligente

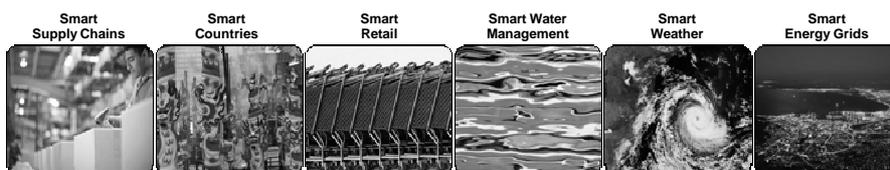
Eduardo Abreu  
IBM Security Solutions  
eabreu@br.ibm.com



IBM Security Solutions: Secure by Design. Innovate with Confidence.



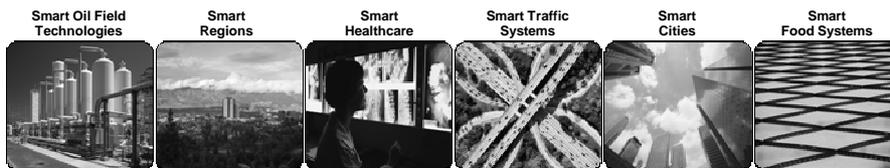
## O planeta está ficando mais ...



**INSTRUMENTALIZADO**

**INTERCONECTADO**

**INTELIGENTE**





## A INFORMAÇÃO DO NEGÓCIO ESTÁ EM TODA PARTE

Movimentação contínua dos negócios para novas plataformas como “cloud”, virtualização, mobilidade, mídias sociais, entre outras.



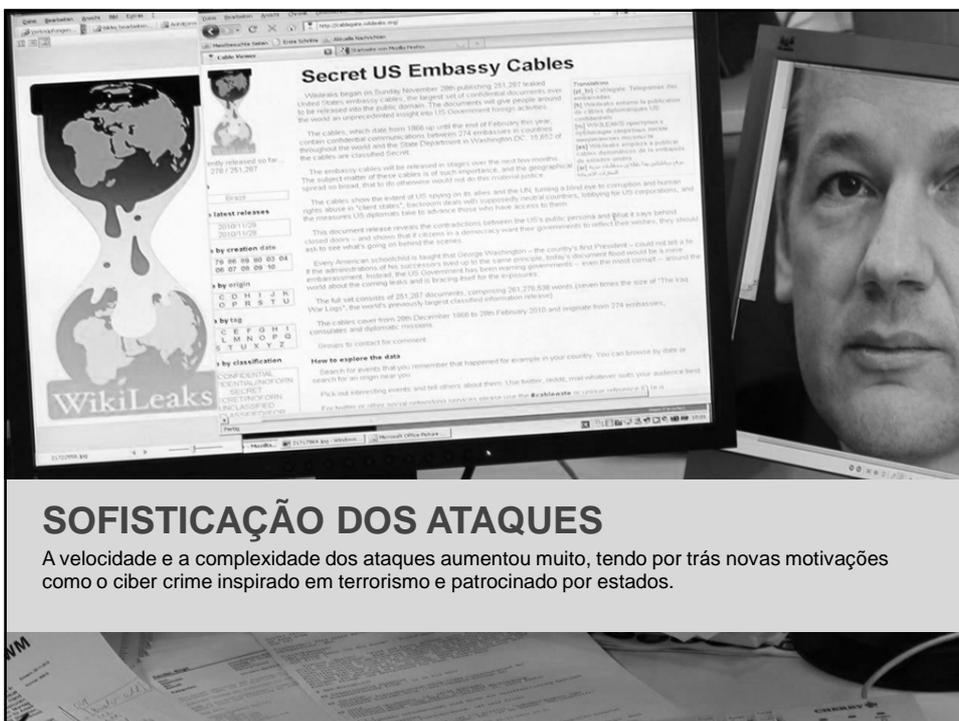
## “CONSUMERIZAÇÃO” da TI

Com a massificação do uso da TI, a fronteira entre o pessoal e o profissional desapareceu: tempo, equipamentos, dados e informações pessoais e profissionais se misturam



## EXPLOSÃO DE DADOS

Há uma explosão na quantidade de informações digitais, acessadas por aplicações distribuídas e usuários em toda parte.



## SOFISTICAÇÃO DOS ATAQUES

A velocidade e a complexidade dos ataques aumentou muito, tendo por trás novas motivações como o ciber crime inspirado em terrorismo e patrocinado por estados.

IBM Security Solutions: Secure by Design. Innovate with Confidence.

**AMEAÇAS EM EVOLUÇÃO**  
2011 X-Force Mid-Year Trend And Risk Report

- O início de 2011 veio com uma explosão de ataques à Segurança de TI fazendo dele o **“O ano das quebras de Segurança”**
- O número de vulnerabilidades publicadas diminuiu, mas **permanece alto - tendência p/2011 aponta aprox 7000 – e a falta de correções atinge aprox. 40%**
- O Grupo de Segurança de Aplicações IBM Rational testou 678 sites (Fortune 500) – **40% tinha vulnerabilidades**
- **Exploração massiva de endpoints**, não só através de vulnerabilidades do browser, mas também com **filmes e documentos maliciosos**
- Os Serviços Gerenciados de Segurança da IBM mostram que os métodos favoritos de ataque são **SQL injection e brute forcing** de senhas, databases e Windows compartilhado

7 © 2011 IBM Corporation

IBM Security Solutions: Secure by Design. Innovate with Confidence.

**Desafios da Segurança impactam a inovação nas empresas**

Ameaças Externas	Ameaças Internas	Compliance
Aumento de ataques externos de origens não "tradicionais"	Riscos devido a comportamentos descuidados ou maliciosos	Número cada vez maior de regulamentações
<ul style="list-style-type: none"> <li>• Cyber attacks</li> <li>• Crime Organizado</li> <li>• Espionagem corporativa</li> <li>• Engenharia social</li> </ul>	<ul style="list-style-type: none"> <li>• Erros administrativos</li> <li>• Comportamentos descuidados</li> <li>• Ações de funcionários descontentes mal intencionados</li> <li>• Mistura dos dados pessoais com informações corporativas</li> </ul>	<ul style="list-style-type: none"> <li>• Leis nacionais e internacionais</li> <li>• Padrões da indústria</li> <li>• Leis locais</li> </ul>

**Impacto na inovação**



**Cloud Computing**



**Mobile Computing**



**Social Business**



**Business Analytics**

8 © 2011 IBM Corporation

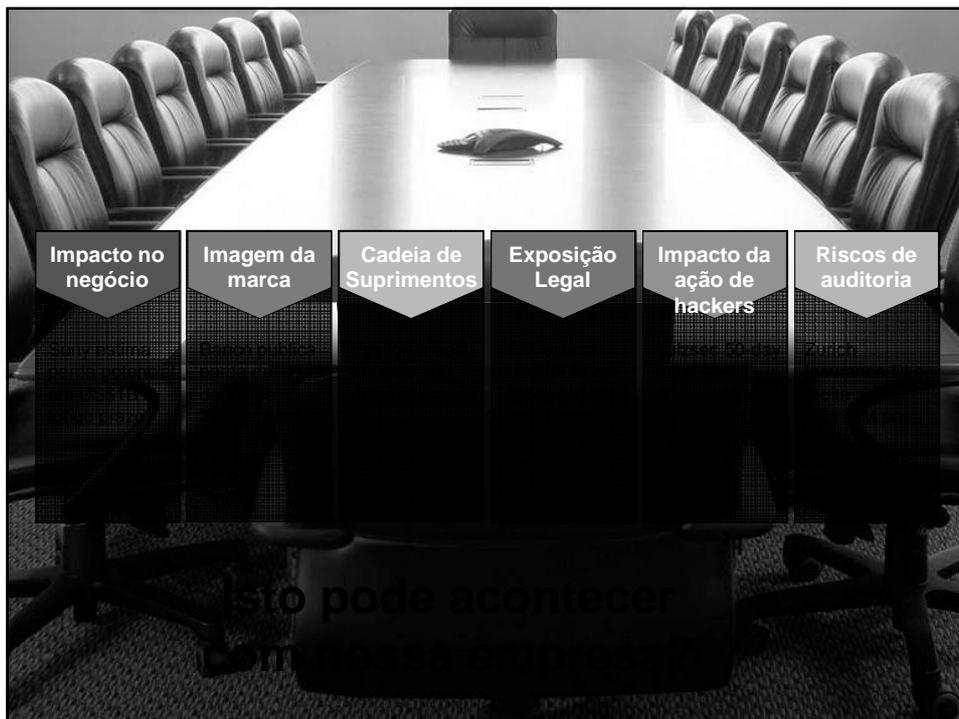
IBM Security Solutions: Secure by Design. Innovate with Confidence.



## O impacto de uma quebra de segurança agora não está mais restrito à área de TI, mas repercute através da corporação

	CEO	CFO/COO	CIO	CHRO	CMO
Prioridade	Evitar impacto de riscos de segurança na confiança e no valor percebido pelo acionista	Conhecer o impacto financeiro de incidentes de segurança	Entender o efeito desencadeado no negócio por falha na segurança da informação	Determinar risco associado com vazamento de dados dos empregados	Evitar danos à marca devido a falhas na segurança
Riscos de Segurança	Perda de propriedade intelectual Perda de dados sensíveis para os negócios	Falhas no atendimento de regulamentações	Proliferação de dados Endpoints inseguros e com acessos inadequados	Vazamento de dados sensíveis Comportamentos descuidados	Perda de dados de clientes ou da empresa
Impacto potencial	Perda de reputação ou market share Exposição legal	Nota de auditoria Multas e penalidades criminais Perda financeira	Perda de confidencialidade integridade e/ou disponibilidade dos dados	Violação da privacidade do funcionário	Perda de confiança dos clientes Marca prejudicada

Riscos de segurança podem impactar os negócios resultando em perdas financeiras, danos de imagem, reputação e até penalidades legais para seus executivos

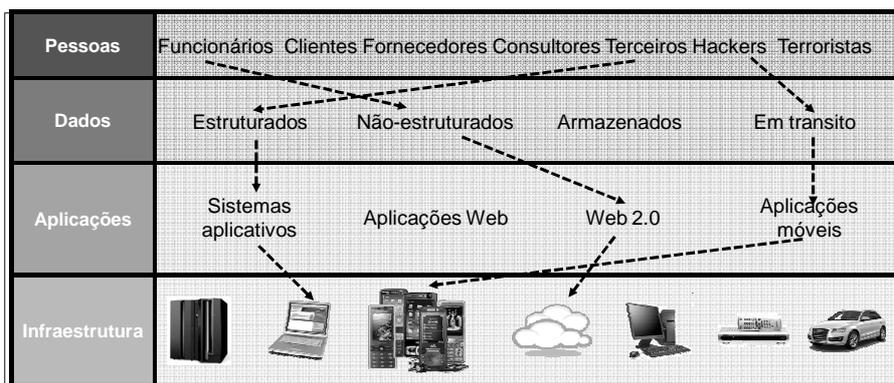




É hora de começar a pensar e agir diferente sobre a Segurança.



A superfície exposta a ataque está crescendo a uma taxa exponencial



- 77% das empresas acham difícil detetar cyber-ataques e 34% tem pouca confiança na capacidade de prevenção
- 75% acham que efetividade poderia aumentar com soluções fim-a-fim

IBM Security Solutions: Secure by Design. Innovate with Confidence.

Esta evolução no cenário requer um abordagem mais pró-ativa e automatizada em Segurança

The diagram illustrates the evolution of security approaches. It features a 2x2 grid of rounded squares. The vertical axis is labeled 'Manual' (bottom) and 'Automatizado' (top). The horizontal axis is labeled 'Reativo' (left) and 'Proativo' (right). In the center of the grid is an oval labeled 'Proficiente'. An arrow labeled 'Inteligência da Segurança' points from the 'Proficiente' oval towards the top-right corner. Text boxes provide descriptions for each quadrant: Manual/Reativo: 'Organizações protegem o **perímetro**, o que regula o acesso e alimenta reportes manuais'; Manual/Proativo: 'Segurança é incorporada no tecido da **organização de TI e das operações do negócio**'; Automatizado/Reativo: 'Básico'; Automatizado/Proativo: 'Otimizado'. A note on the right states: 'Organizações usam análise de dados de Segurança **preditiva e automatizada** para evoluir para a Inteligência da Segurança'.

13 © 2011 IBM Corporation

IBM Security Solutions: Secure by Design. Innovate with Confidence.

...e uma abordagem equilibrada e realista para cobrir os gaps entre a situação presente e a situação desejada

Domínios da Segurança	Hoje	Security Gap	Amanhã	
Pessoas	Gerenciamento de identidades por aplicação		Dash board centralizado com gestão de usuários privilegiados	Correlação e análise detalhada de eventos
Dados	Implementação de controle de acesso e criptografia		Monitoração do uso dos dados e do vazamento de informações	
Aplicações	Busca (scan) por vulnerabilidades		Contruir segurança a partir do "day one"	
Infraestrutura	Bloqueio de acessos não autorizados e de ataques e infecções		Executar detecção de ameaças avançadas e fazer análise forense em tempo real	

Reativo ←-----→ Pró-ativo

14 © 2011 IBM Corporation



**ENTRANDO NA ERA DA INTELIGÊNCIA DA SEGURANÇA:  
Um plano de 3 etapas**

<p><b>1 ESTEJA BEM INFORMADO</b></p> <p>Conduza uma abordagem estruturada para avaliar os riscos de TI e dos negócios</p>	<p><b>2 ESTEJA ALINHADO</b></p> <p>Implemente e faça seguirem práticas de excelência em Segurança por toda a empresa estendida</p>	<p><b>3 ATUE COM INTELIGÊNCIA</b></p> <p>Implemente controles e análises de dados inteligentes dentro e através dos principais domínios</p>
---------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------



**Conduza uma abordagem estruturada para avaliar os riscos de TI e dos negócios**

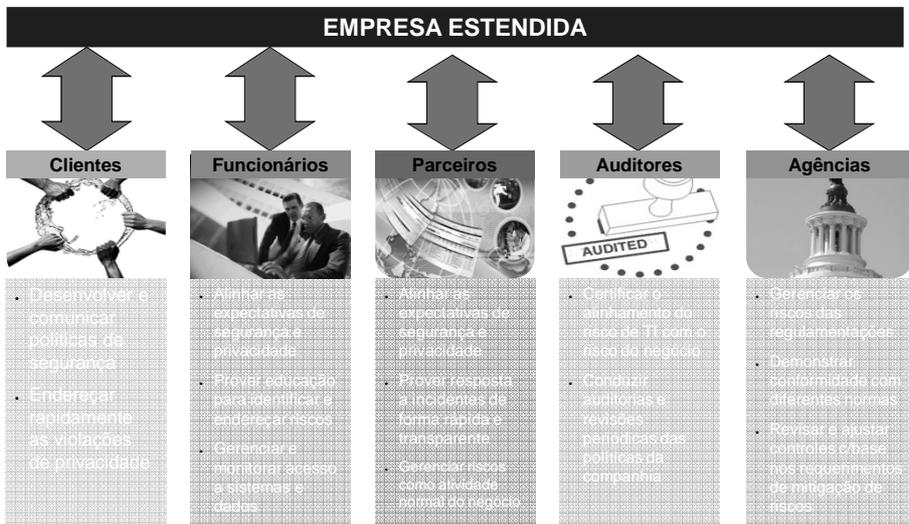


**CUIDANDO DA GESTÃO DE RISCO**

- Alinhe e integre a gestão de riscos de TI à estratégia de gestão de riscos do negócio
- Identifique as principais ameaças e os principais requerimentos de conformidade
- Implemente e faça seguir um processo e modelo de controles de gestão de risco
- Execute o processo de gestão de incidentes quando uma crise ocorrer



## Implemente e faça seguirem práticas de excelência em Segurança por toda a empresa estendida



## Implemente controles e análises de dados inteligentes dentro e através dos principais domínios

	Pessoas	Dados	Aplicações	Infra-estrutura	
	Governança, risco e compliance Correlação e análise detalhada de eventos				
	<b>Otimizado</b>	Análise baseada em Perfil de Negócios Governança de Identidades Controle de usuários privilegiados	Análise de fluxo de dados Governança de Dados	Ambiente de desenvolvimento de aplicações de seguro Detecção de fraudes	Monitoração avançada e forense de redes Segurança de sistemas
	<b>Proficiente</b>	Gestão de Identidades Autenticação forte	Monitoração de atividade Data Loss Prevention	Firewall de aplicação Análise de código fonte	Gestão de ativos Gestão de Segurança de Rede e Endpoints
	<b>Básico</b>	Senhas e identidades de usuários	Criptografia Controle de acesso	Scanning de vulnerabilidades	Segurança perimetral Antivírus

IBM Security Solutions: Secure by Design. Innovate with Confidence.

## O IBM Security Framework facilita a implementação de controles e de inteligência para a Segurança

### THE IBM SECURITY FRAMEWORK

### ABRANGÊNCIA

#### CONTROLES DE SEGURANÇA

- Governança
- Análise de riscos e de processos de TI e de negócios
- Arquitetura de Segurança
- Patch management
- Segurança de aplicações
- Segurança e integridade de dados
- Data loss prevention
- Segurança de Endpoints
- Segurança de Redes
- Gestão de identidade e acesso
- Gestão de incidentes
- Gestão de resiliência
- Digital video surveillance

#### INTELIGÊNCIA DA SEGURANÇA

- Análise de Advanced persistent threat
- Monitoração contínua
- Análise de vulnerabilidade
- Third-party ethical hacking
- Análise avançada de dados de segurança
- Serviços Gerenciados de Segurança
- Gestão de eventos de segurança
- X-Force Intelligence

19 © 2011 IBM Corporation

IBM Security Solutions: Secure by Design. Innovate with Confidence.

## ...tanto dentro como através dos principais domínios da Segurança

Enterprise Governance, Risk and Compliance Management					
IBM OpenPages		Algorithmics (recent acquisition)		IZ Corporation (recent acquisition)	
<b>IBM Security Portfolio</b>					
<b>IT Governance Risk and Compliance</b>					
Security Information and Event Management		Deep, custom analytics (SPSS, Streams, Cognos)		IBM Privacy, Audit and Compliance Assessment Services	
<b>Pessoas</b>	<b>Dados</b>	<b>Aplicações</b>	<b>Rede</b>	<b>Infraestrutura</b>	<b>Endpoint</b>
Identity & Access Management Suite	Guardium Database Security	AppScan Source Edition	Network Intrusion Prevention	Endpoint Manager (BigFix)	Managed Security Services
Federated Identity Manager	Optim Data Masking	AppScan Standard Edition		zSecure Mainframe	
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	DataPower Security Gateway	Server and Virtualization Security	X-Force and IBM Research
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service	Application Assessment Service	Managed Firewall, Unified Threat and Intrusion Prevention Services	Penetration Testing Services	
	Encryption and DLP Deployment	AppScan OnDemand Software as a Service			

20 © 2011 IBM Corporation

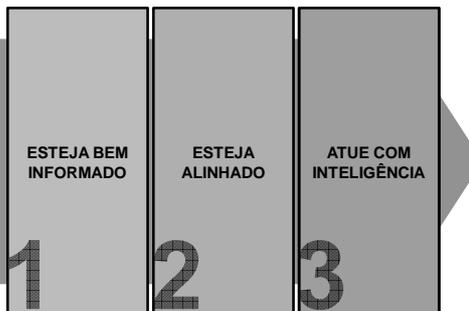


## Experiência da IBM com Segurança da Informação...

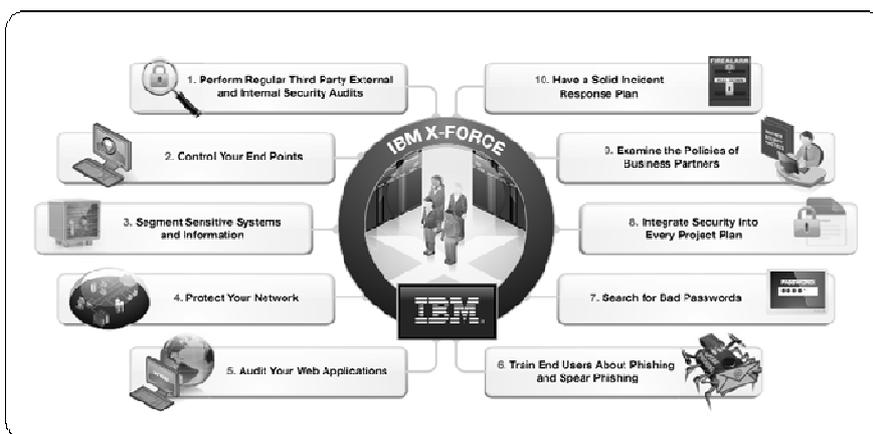
### EXPERTISE

- 21 bilhões de eventos monitorados por dia
- Mais de 4,000 clientes de serviços gerenciados de segurança
- 10 laboratórios de desenvolvimento de Segurança
- 9 centros de operação de segurança
- 6,000+ especialistas técnicos
- Mais de 20 reconhecimentos pela liderança em Segurança
- 2010 Security Company of the Year

### ABORDAGEM DE SEGURANÇA



## Deixo vocês com 10 sugestões... Se o X-Force estivesse à frente da operação de TI



IBM Security Solutions: Secure by Design. Innovate with Confidence.



**Eduardo Abreu**  
IBM Security Solutions  
[eabreu@br.ibm.com](mailto:eabreu@br.ibm.com)  
Cel:011.69057994