IBM Security Forum

Soluções para um ambiente seguro

PCI *Compliance*: Panorama do Mercado Brasileiro e Soluções IBM

Ed Wilson Menezes, CISSP,CISM
Especialista PCI
emenezes@br.ibm.com

AGENDA

- Mercado Brasileiro de Meios de Pagamento
- Payment Card Industry (PCI)
- Implementação do PCI no Brasil
- Fraudes e Crimes Eletrônicos
- Aderência do mercado brasileiro
- Soluções IBM para PCI

Modelo do Mercado Brasileiro de Cartões

Bandeiras

55 Emissores

- Outros
- Hipercard
- Credicard
- Bradesco
- Banco do Brasil
- Amex

6 Adquirentes

- Visanet
- Tecban
- Hipercard
- Amex
- GetNet
- Redecard

Portadores

217 Milhões de cartão de Débito
124 Milhões de cartão de Crédito
173 Milhões de cartões privados

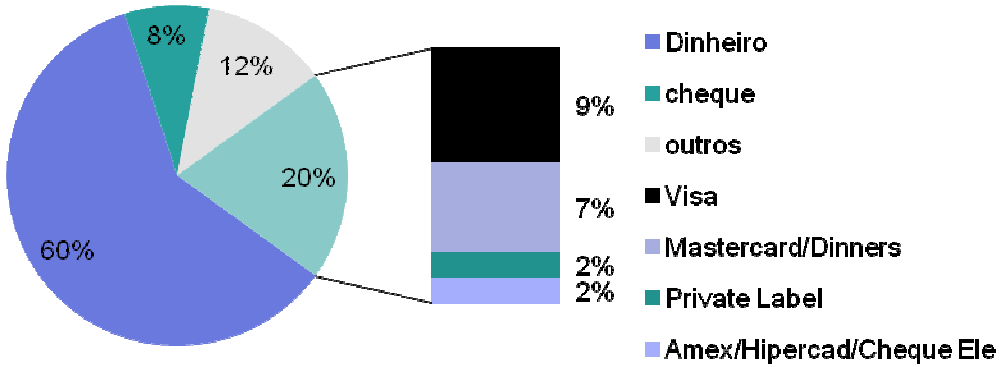
Estabelecimentos

Acima de 1,4 Milhões de estabelecimentos

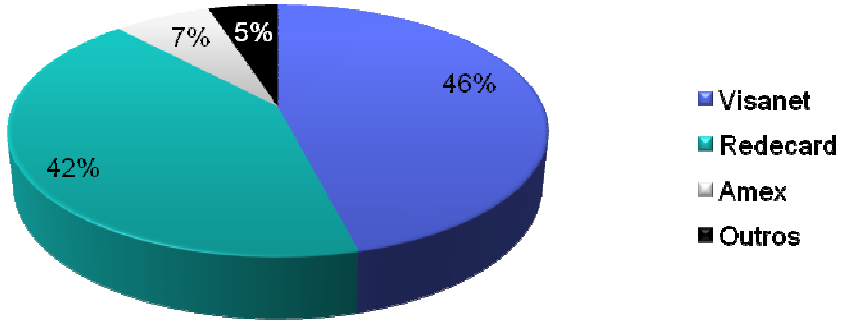
Fonte: ABECS (Associação Brasileira das Empresas de Cartões e Serviços)

Dados do Mercado Brasileiro de Meios de Pagamento

Consumo Privado no Brasil em 2007



Market Share Adquirentes



Fonte: ABECS (Associação Brasileira de Empresas de Cartões e Seviços

O que é o PCI

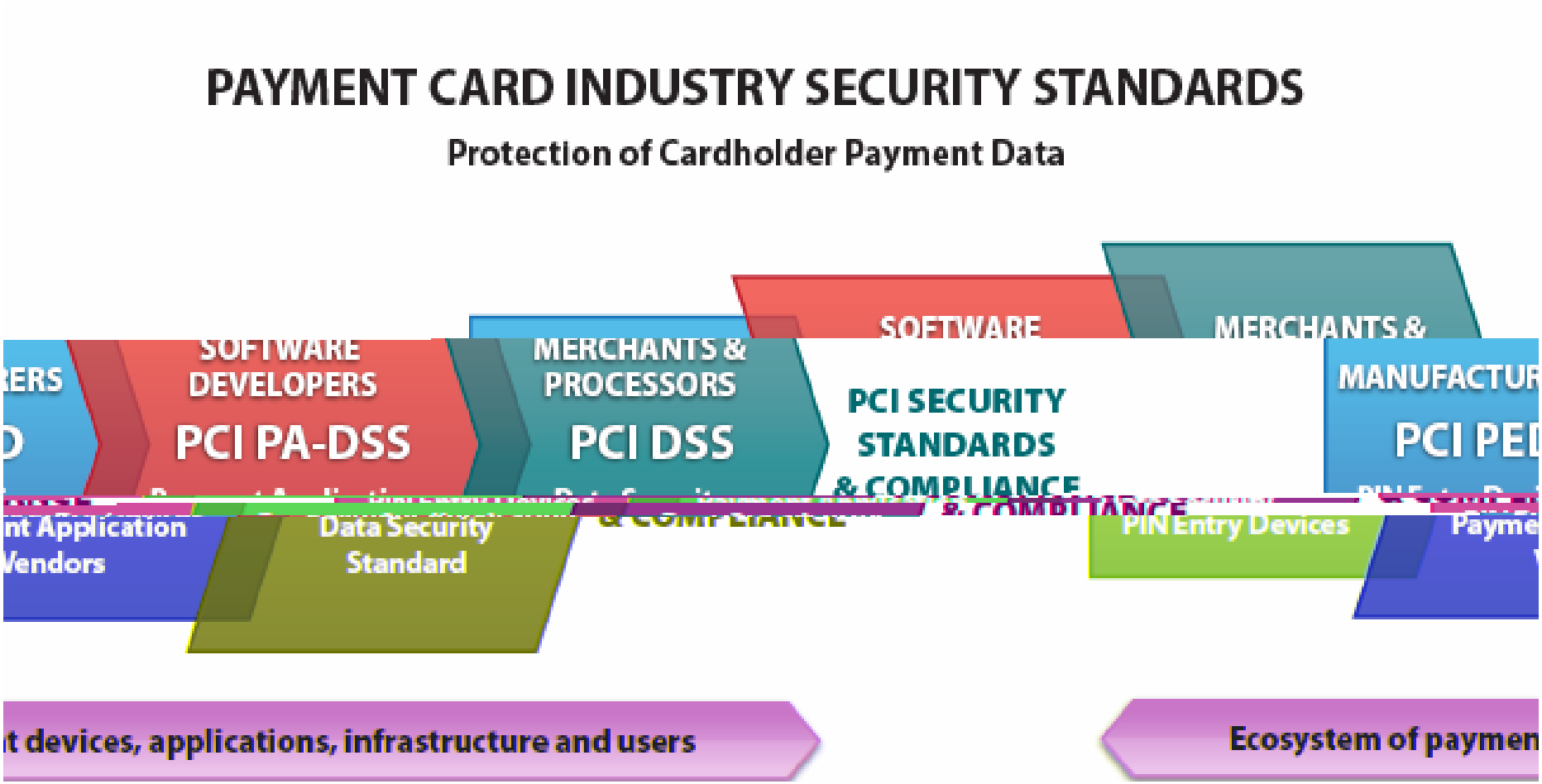
- **O PCI SSC (Payment Card Industry Security Standards Council) é uma organização que une os principais *players* internacionais do mercado de meios eletrônicos de pagamento, incluindo:**
  - **MasterCard;**
  - **Visa;**
  - **American Express;**
  - **Diner's Club;**
  - **Discover Card;**
  - **JCB.**
- **A organização foi reforçada por incidentes de segurança em massa;**
- **Seu objetivo é criar padrões de operação e segurança, para proteger os dados de cartão de pagamento contra roubo/fraude, desde 2004;**

Padrões de Segurança de Dados do PCI

- **O PCI DSS foi o primeiro padão publicado pelo conselho e visa a proteção dos números de cartão, código de segurança (CVC2) e trilhas em todos os níveis da cadeia de pagamentos:**
  - **Adquirentes (Redecard, Visanet, Amex);**
  - **Estabelecimentos Comerciais;**
  - **Bancos Emissores;**
  - **Processadoras;**
  - **As própias Bandeiras;**

- **O PCI-DSS foi baseado na ISO 27001/2 e em boas práticas de segurança da informação do mercado;**
- **Além do DSS, o PCI publicou outras normas de segurança para a indústria de cartões, focando a segurança de aplicações e segurança de hardware**

Padrões de Segurança de Dados do PCI



Padrões de Segurança de Dados do PCI

- **O PCI publicou até agora os seguintes padrões de segurança:**
  - ✓ **PCI – DSS (*Payment Card Industry – Data Security Standard*)**
    - o **Focado no ambiente (infra-estrutura) de Segurança**
    - o **A versão 1.2 do padrão foi publicado em 01 de outubro de 2008.**
  - ✓ **PA – DSS (*Payment Application – Data Security Standard*)**
    - o **Focado no desenvolvimento de sistemas de pagamento**
      - ➢ **POS, TEF, Gateways, Autorizadores, etc.**
  - ✓ **PCI – PED (*Payment Card Industry – Pin Entry Device)***
    - o **Focado na segurança física e hardware dos dispositivos de pagamento**
      - ➢ **POS, PinPAD, HSM, ATM, Quiosques**

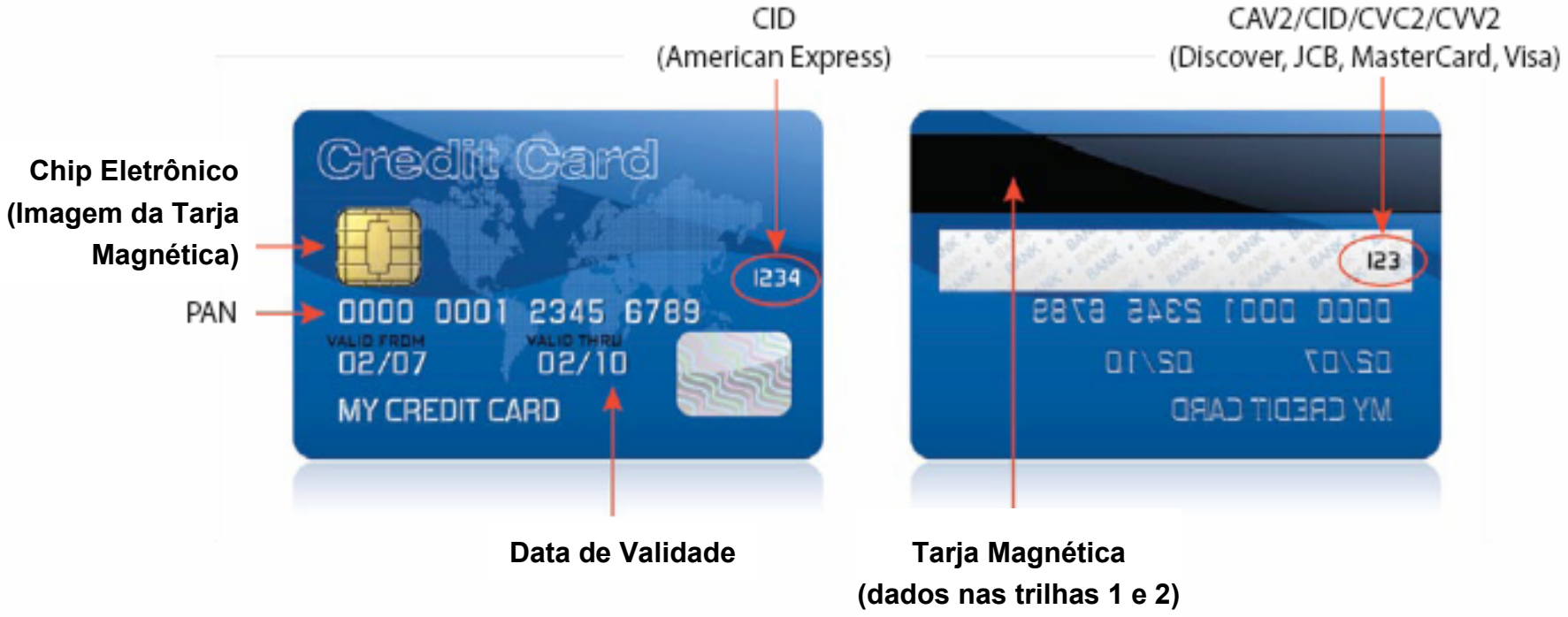
As 12 Exigências do PCI DSS

Construa e Mantenha uma Rede Segura	
1.	Instale e mantenha uma configuração de firewall para proteger os dados do portador de cartão
2.	Não use as senhas padrão de sistema e outros parâmetros de segurança fornecidos pelos prestadores de serviços.
Proteja os Dados do Portador de Cartão	
3.	Proteja os dados armazenados do portador de cartão
4.	Codifique a transmissão dos dados do portador de cartão nas redes públicas e abertas
Mantenha um Programa de Administração de Vulnerabilidades	
5.	Use e atualize regularmente o software ou programas antivírus
6.	Desenvolva e mantenha sistemas e aplicativos seguros
Implemente Medidas Rígidas de Controle de Acesso	
7.	Restrinja o acesso aos dados do portador de cartão a apenas aqueles que necessitam conhecêl-os para a execução dos trabalhos
8.	Atribua um ID único para cada pessoa que possua acesso ao computador
9.	Restrinja o acesso físico aos dados do portador de cartão
Acompanhe e Teste Regularmente as Redes	
10.	Acompanhe e monitore todo o acesso aos recursos da rede e dados do portador de cartão
11.	Teste regularmente os sistemas e processos de segurança
Mantenha uma Politica de Segurança da Informação	
12.	Mantenha uma política que atenda à segurança da informação para funcionários e prestadores de serviços

PCI DSS versão 1.2

Dados protegidos pelo PCI DSS

Dados em uma cartão de pagamento



Dados protegidos pelo PCI DSS

	Elemento do Dado	Armazenagem Permitida	Proteção Exigida	PCI DSS Req. 3.4
Dado do Portador de Cartão	Número Primário da Conta (PAN)	SIM	SIM*	SIM
	Nome do Portador do Cartão*	SIM	SIM*	NÃO
	Código do Serviço*	SIM	SIM*	NÃO
	Data de Vencimento*	SIM	SIM*	NÃO
Dados Confidenciais de Autenticação**	Tarja Magnética Completa*	NÃO	NÃO	N/A
	CVC2/CVV2/CI	NÃO	NÃO	N/A
	PIN / Bloqueador de PIN	NÃO	NÃO	N/A

** Estes elementos dos dados devem ser protegidos se forem armazenados em conjunto com o PAN. Esta proteção deve ser consistente com as exigências do PCI DSS para a proteção geral do ambiente do portador de cartão. Adicionalmente, outra legislação (por exemplo, relacionada à proteção dos dados pessoais do cliente, privacidade, identidade, roubo ou segurança dos dados) pode exigir uma proteção específica destes dados ou divulgação adequada das práticas da companhia se os dados pessoais relacionados ao cliente estão sendo coletados durante o curso do negócio. O PCI DSS; entretanto, não se aplica se os PANs não forem armazenados, processados ou transmitidos.*

*** Não armazene dados confidenciais de autenticação subseqüentes à autorização (mesmo se codificados).*

Datas para Conformidade

- **As datas para conformidade com o PCI segundo a VISA Inc., são:**
  - ✓ **30 de setembro de 2009**
    - o **Todos estabelecimentos que operam em mais que uma região Visa**
    - o **Todos Prestadores de serviço Nível 1**
  - ✓ **30 de setembro de 2010**
    - o **Todos estabelecimentos e prestadores de serviço devem comprovar conformidade através da apresentação do RoC.**

Fonte: Comunicado Visa Inc. de 10 de novembro de 2008 em http://corporate.visa.com/md/nr/press873.jsp

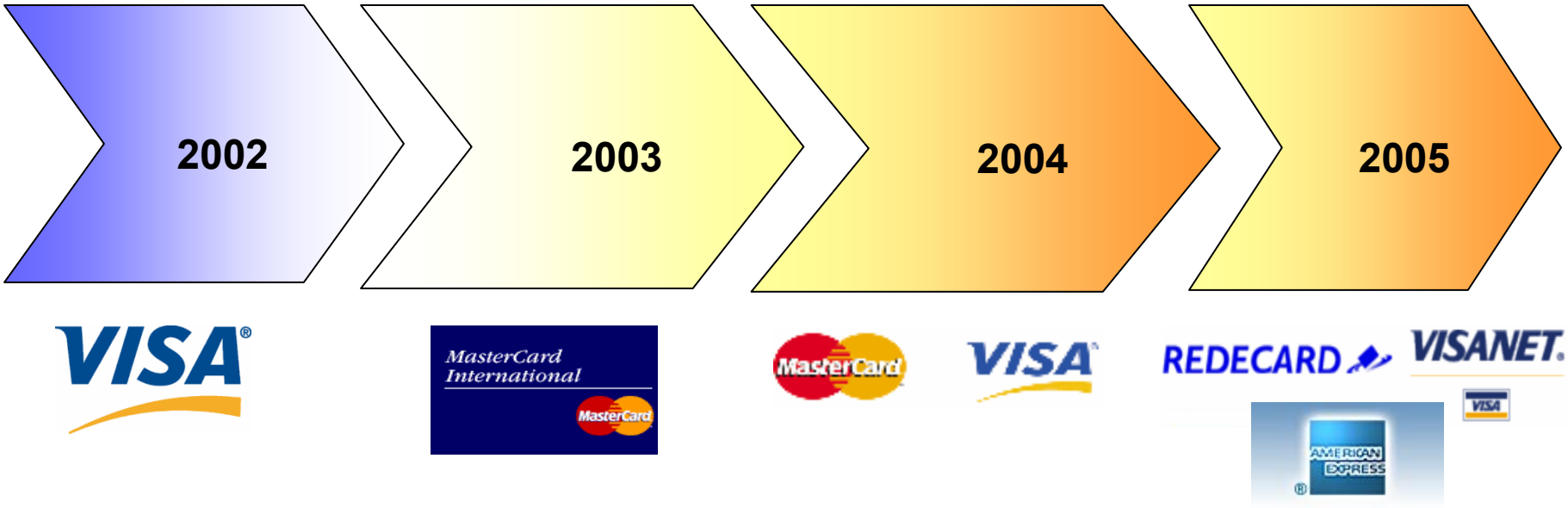
Multas para não Conformidade

- **As multas para a não conformidade ainda não foram definidas pela Visa ou Mastercad para a região, mas nos EUA e Europa as multas praticadas eram:**
  - ✓ **Até US$ 500.000,00 por incidente**
  - ✓ **Até US$ 25.000,00 por mês por não conformidade**
    - **A Mastercard considera a data para conformidade, 30 de junho de 2004 – cobrando multas retroativas até esta data.**
  - ✓ **De US$ 5,00 a US$ 25,00 por cartão comprometido**

Estabelecimentos – Critério para os níveis

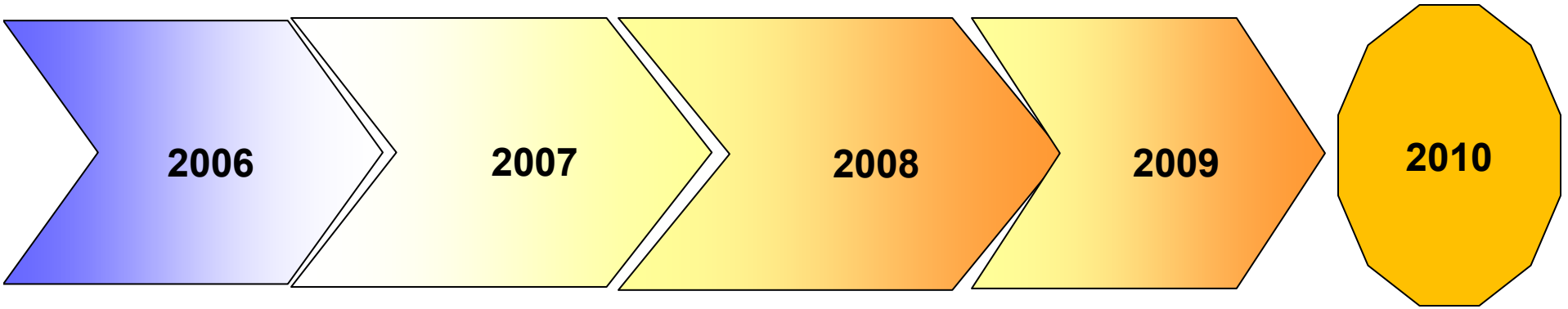
Nível do Estabelecimento	Critérios
Nível 1	▪ Qualquer estabelecimento, com volume anual de transações com cartões superiores a 6 milhões. ▪ Estabelecimentos que sofreram ataques bem sucedidos no ano anterior
Nível 2	▪ Qualquer estabelecimento com volume transacional anual com cartões entre 1 e 6 milhões.
Nível 3	▪ Estabelecimentos de comércio eletrônico, com volume transacional com cartões entre 20.000 e 1 milhão.
Nível 4	▪ Os demais estabelecimentos que não se enquadram nos critérios acima

Implementação do PCI no Brasil – Linha de tempo



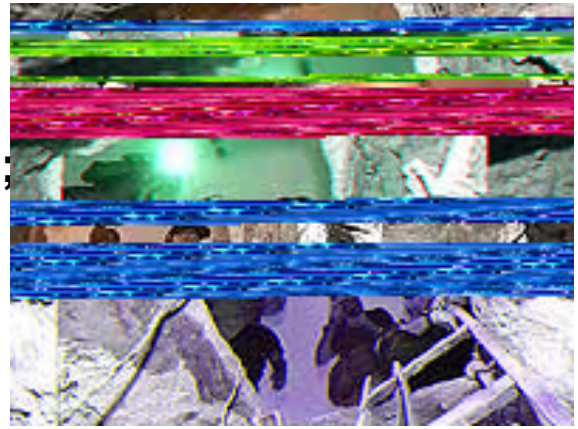
- **2002 – Visa lança o programa VISA AIS – *Account Information Security***
- **2003 - MasterCard lança o programa SDP - *Site Data Protection***
- **2004 – *Payment Card Industry – Data Security Standard* definido**
- **2005 – Ações colaborativas entre os adquirentes, para sinergia dos programas. Formação de grupo de trabalho.**

Implementação do PCI no Brasil – Linha do tempo

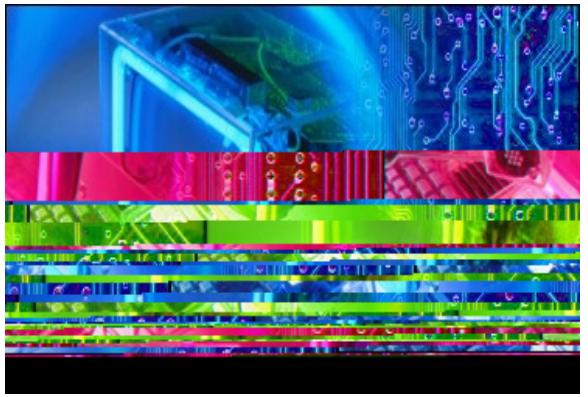


- **2006 – Qualificação de fornecedores e alinhamento de programas / Lançamento da versão 1.1 do PCI-DSS. Formação do PCI SSC.**
- **2007 – Implementação (Auditorias) e Conscientização do PCI no Brasil. Adesão de Adquirentes *Private Label*. Formação de Grupo de Trabalho na ABECS.**
- **2008 – Expansão da implementação e *follow-up* dos planos de remediação. *Target* (Dez/08) para conformidade dos bancos emissores postergado para 2010. Lançamento da versão 1.2**
- **2009 – *Target (Dez/09)* para conformidade dos estabelecimentos *tier*/nivel 1, processadoras e prestadores de serviços. Estabelecido grupo na ABECS para elevar exigências do PCI PED para o Brasil**
- **2010 - Target (Dez 10) Bancos emissores e demais membros da cadeia.**

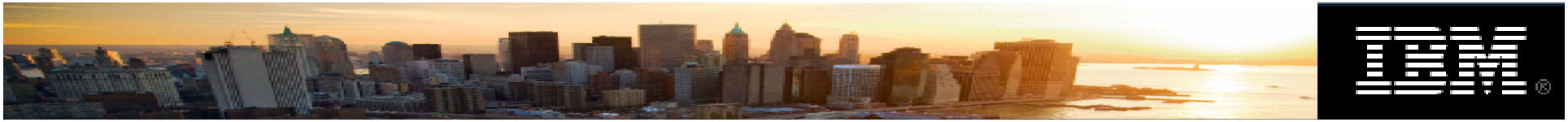
2005 – Roubo do Banco Central do Brasil em Fortaleza



- **62 milhões de Dólares (133 milhões de Reais);**
- **Segundo maior roubo a banco da história;**
- **Túnel de 80 metros de extensão;**
- **Parede de concreto de 2 metros;**
- **3,5 toneladas em notas de R$ 50,00;**
- **Câmeras de Segurança;**
- **Sensores de movimento, etc.**



2005 – Fraudes em meio eletrônico causam prejuízo de 300 milhões de Reais (Febraban)



InfoWorld Log-in | Register

HOME | NEWS | TECHNOLOGIES | BLOGS | COLUMNS | TEST CENTER | AUDIO/VIDEO | CAREERS | IT EXEC-CONNECT

Retailer TJX reports massive data breach

Credit, Debit data stolen. Extent of breach still unknown

By Paul F. Roberts
January 17, 2007

Talkback E-mail Printer Friendly Reprints Text Size A A

ARTICLE TOOLS SPONSORED BY hp

The TJX Companies, a large retailer that operates over 2,000 retails stores under brands such as Bob's Stores, HomeGoods, Marshalls, T.J. Maxx and A.J. Wright said on Wednesday that it suffered a massive computer breach on a portion of its network that handles credit card, debit card, check, and merchandise transactions in the U.S. and abroad.

Related Stories

TJX stolen data used in Florida crime spree

Visa summit will counter data breach hype

The company does not know the extent of the breach, which was first discovered in December, 2006. However, hackers may have made off with credit and debit information from transactions in the U.S., Canada, and Puerto Rico in 2003 as well as transactions between May and December, 2006, according to a company statement.

Banking officials in Massachusetts say that the TJX breach is behind a recent warning by Visa to banks in Massachusetts, which have contacted customers in recent days and had to reissue thousands of ATM and debit cards. In the end, the hack may affect a wide range of credit card companies and thousands of consumers in the U.S. and in countries like the U.K. and Ireland, experts say.

TJX said it is working with IBM and General Dynamics to investigate the breach, which is believed to have occurred on computer systems that process and store information on customer transactions for T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright. Transactions from T.K. Maxx in the U.K. and Ireland may have also been exposed in the breach.

TJX said it knows of "a limited number of credit card and debit card holders whose information was removed from the system," and has provided that information to credit card companies. TJX is also working with law enforcement, including the U.S. Department of Justice, U.S. Secret Service, and Royal Candian Mounted Police, TJX said in its statement.

- **Estimativa Inicial: 46 Milhões, entre débito e crédito**
- **Confirmado: 94 Milhões, entre débito e crédito**
- **A TJX não seguia princípos básicos de segurança e do padrão PCI-DSS;**

NETWORKWORLD

News | Blogs & Columns | Clear Choice Tests | Videos | Events | More

Security | LANs & WANs | VoIP | Net Management | Wireless | Software | Data Center | SMB | T

Anti-Malware | Compliance | Firewalls / VPN | NAC | Security Management | Clear Choice Tests | IT Buyer's Guides |

Details emerging on Hannaford data breach

Malware loaded onto Hannaford servers let attackers intercept credit card data

By Ellen Messmer , Network World , 03/28/2008

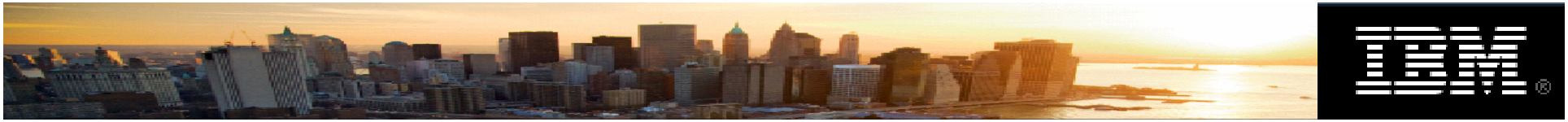
Share/Email | Buzz up! | 2 Comments | Print | IT Buyer's Guides

Hannaford Brothers Cos, which earlier this month disclosed a data breach involving credit cards at its supermarket stores, this week shared more information with Massachusetts regulators about the ongoing investigation into the incident.

In a letter to Massachusetts Attorney General Martha Coakley and Gov. Deval Patrick's Office of Consumer Affairs, Hannaford's general counsel Emily Dickinson shared details that Hannaford is uncovering in its investigation.

The letter stated that malware loaded onto Hannaford servers allowed attackers to intercept card data stored on the magnetic stripe of payment cards as customer's used them at the check-out counter, according to information Hannaford provided to the Massachusetts Attorney General. That information, taken in transit from the point of sale, included card number and expiration date but not the customer's name. The attack resulted in card data being transferred overseas and has resulted in 2,000 known cases of fraud.

- **Estimativa Inicial: + 4 Milhões, entre débito e crédito**
- **A Hannaford era certificada nos princípos básicos de segurança e do padrão PCI-DSS;**
- **Causa: Malware**



Address http://tecnologia.terra.com.br/interna/0,,OI3464245-EI4805,00-Malware+expoe+milhoes+de+cartoes+de+credito+e+debito.html

terra | Buscar na internet | Conheça o Sonora | shopping | e-mail | chat | índice

tecnologia

› Tecnologia › Vírus & Cia

Vírus & Cia

Imprimir Enviar Rss Celular

Quarta, 21 de janeiro de 2009, 21h34 Atualizada às 23h29

Malware expõe 100 milhões de cartões de crédito e débito

Uma contaminação por **malware** na rede da empresa americana Heartland Payment Systems pode ter levado à maior exposição de registros de cartões de crédito e débito até hoje: 100 milhões de números.

» **Novo vírus atinge mais de 800 hospitais britânicos**
» **Vírus Downadup já infectou quase 9 milhões de PCs**

A Heartland Payment Systems processa o pagamento de mais de 250 mil empresas, e os números são estimativas baseadas nas transações mensais da companhia, noticiou o **site** Heise Security.

Em nota oficial publicada em seu site, a Heartland explicou que a empresa foi contaminada por um malware, possivelmente por uma operação internacional de **ciberfraude**, e que está trabalhando com o Serviço Secreto americano e o Ministério de Defesa.

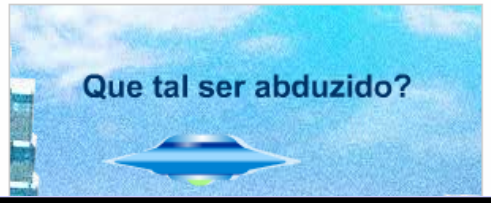
Ainda que os dados possam ter sido expostos, a companhia informou que nenhum dado confidencial pessoal esteve envolvido. Todavia, entre os dados roubados estava a informação digital codificada na fita magnética empregada nos cartões, com a qual seria possível clonar os cartões, noticiou o site *Washington Post*.

Últimas notícias

14h11 » **Vírus Conficker já infecta mais de 15 milhões de PCs**
12h06 » **Hacker que invadiu Pentágono pode evitar extradição**
21h34 » **Malware expõe 100 milhões de cartões de crédito e débito**

Busque outras notícias no Terra

BUSCAR



- **Estimativa Inicial: + 100 Milhões, entre débito e crédito**
- **A Heartland era certificada nos princípos básicos de segurança e do padrão PCI-DSS;**
- **Causa: Malware**

08/02/2009 - 09h53

Invasão de hacker faz Citibank recolher cartões no Brasil

TONI SCIARRETTA
da **Folha de S.Paulo**

Uma invasão de hackers em uma empresa americana que faz processamento de pagamentos eletrônicos levou o Citibank a cancelar e a recolher cartões de crédito em vários países, inclusive no Brasil.

O Citi suspeita de que os hackers tenham obtido dados como nome, número e data de expiração de cartões de crédito Citicard e Credicard Citi no país. O banco não revelou o número de clientes expostos ao problema, mas afirmou que eles estão sendo contatados.

Mesmo com dúvida se os dados foram, de fato, roubados, o Citi afirma que decidiu, preventivamente, recolher os cartões dos clientes que tiveram dados processados pela prestadora de serviço americana.

O processamento dos dados era feito pela Heartland Payments Systems, de Nova Jersey (EUA), que sofreu ataque a seus sistemas entre maio e novembro de 2008. A empresa processa 100 milhões de transações mensais para mais de 250 mil estabelecimentos nos EUA e no Canadá. Os clientes mais expostos são os que viajaram a esses países no período.

Maior violação de dados

O incidente é visto como a maior violação de dados da história e colocou em alerta as principais empresas de processamento de dados do mundo. Especialistas estimam que 50 milhões de pessoas tenham ficado com seus dados vulneráveis. A Heartland criou um hotsite (www.2008breach.com) para esclarecer as principais dúvidas dos clientes.

Conseqüências de Não Cumprimento do PCI-DSS

- Custo da publicidade negativa para o valor das ações
- Multas das Bandeiras ou dos Adquirentes
  - As empresas podem sofrer multas de até to US$500.000 por violação
- Em incidentes que resultam em perda de dados do portador do cartão:
  - Exigência de pagar todos os testes periciais
  - Responsabilidade por perdas das Bandeiras ou dos Adquirentes
  - Custos de resolução de disputas
- Até agora:
  - As Maiores perdas monetárias sofridas pelas Bandeiras, Adquirentes ou Emissores
  - Em segundo lugar, custo pericial e compensações correspondentes
  - Multas representam menor parte das perdas sofridas
  - Em 2006, a Visa impôs multas de $4.6 milhões; em 2005 foram $3.4 milhões.
  - Estima-se que a TJX já perdeu aproximadamente US$ 1 bilhão entre multas, indenizações, perícias, etc.

CNNMoney.com

TJX disse que violação de segurança terá um ônus

COMPUTERWORLD

Violação de segurança no Sam's Club expõe cartões de crédito

NORWICH UNION
an AVIVA company

O Consórcio Britânico de Varejo estima que a fraude de cartões de crédito tenha custado 2,2 bilhões aos varejistas no ano passado

The Register®

Falhas de segurança no varejo de UK expõem 2.000 cartões de crédito

FEDERAL TRADE COMMISSION
FOR THE CONSUMER

Agência diz que a empresa falhou na proteçã de dados sensíveis de clientes

THE WALL STREET JOURNAL

Grande Varejista Revela Incidente de Violação de Dados de Clientes Pode Afetar Milhões de Consumidores de T.J. Maxx, Marshalls e Outras Lojas da TJX

USA TODAY

Dados da MasterCard roubados da Polo Ralph Lauren

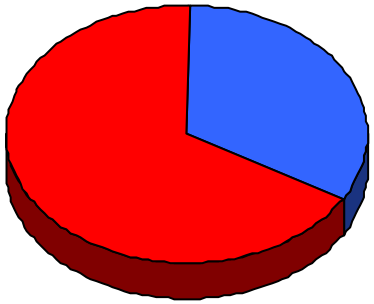
MSNBC

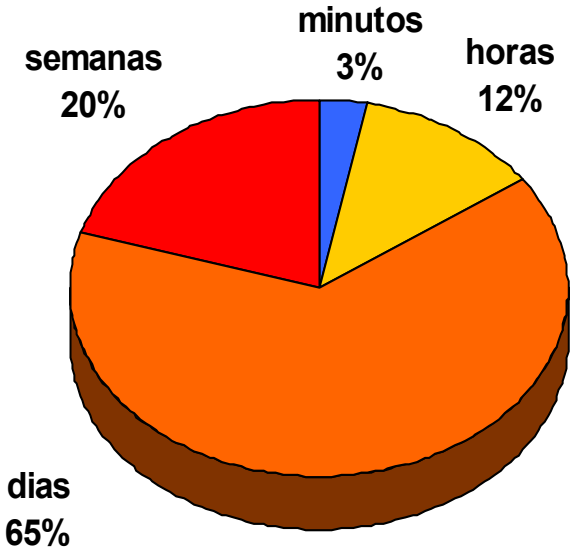
1,4 milhões expostos em violação de dados de sapataria

Outra ameaça a considerar…

Utilização Incorreta dos Dados Corporativos

- **59% dos trabalhadores que deixaram seus cargos levaram consigo informações confidenciais**
- **67% utilizaram informações confidenciais de sua antiga empresa para conseguir um novo emprego**





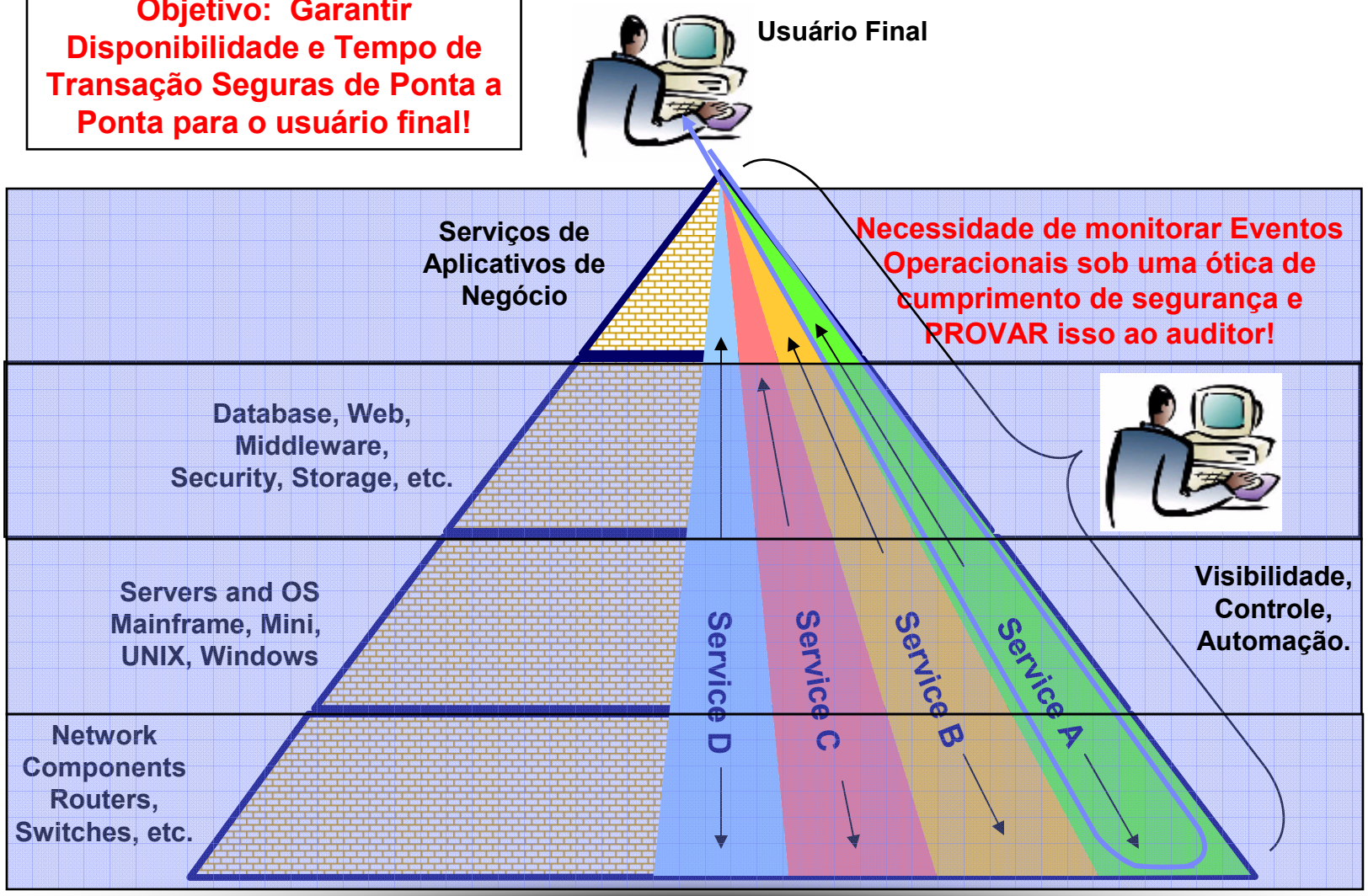
Tempo para encerrar o acesso

- **24% ainda tem acesso aos sistemas corporativos**

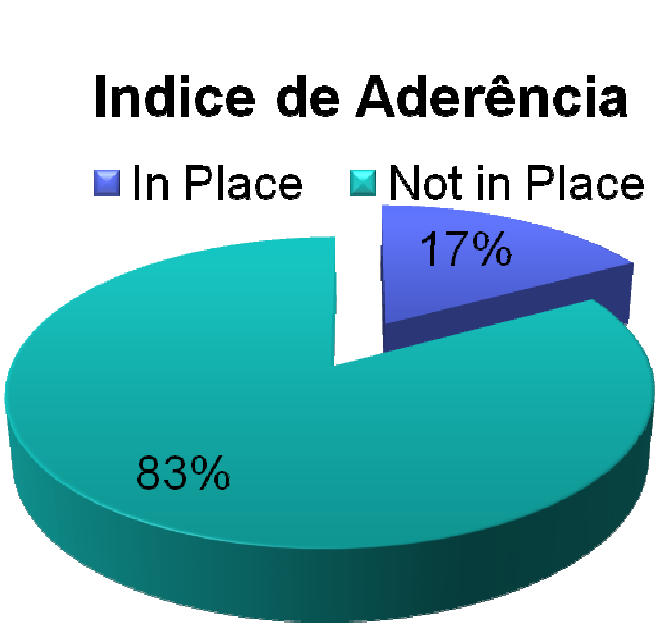
Fonte: “Data Loss Risks During Downsizing”, Ponemon Institute LLC, 23 de fevereiro de 2009

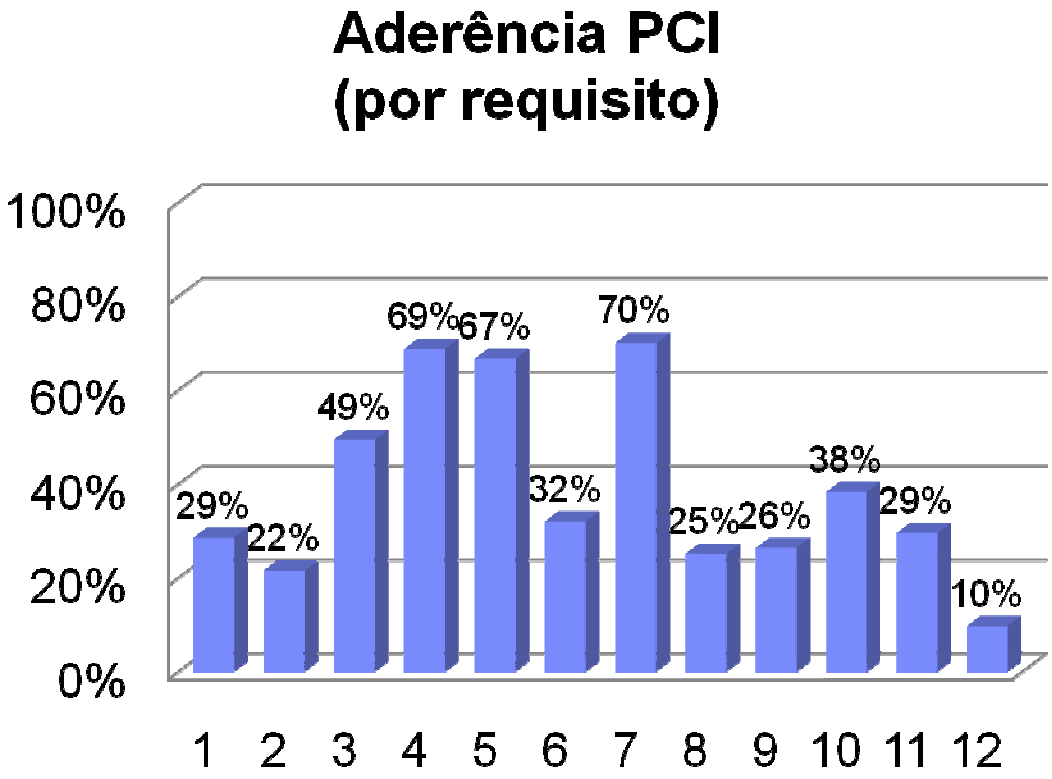
Por que cumprimento é tão difícil?

Objetivo: Garantir Disponibilidade e Tempo de Transação Seguras de Ponta a Ponta para o usuário final!



Aderência Média ao PCI no Brasil





Fonte: Relatórios de Conformidade (RoC) dos estabelecimentos.

Análise de Aderência

Principais Itens para não conformidade:

- Redes *wireless* abertas
- Desconhecimento do risco
- Guarda de informações sem criptografia
- Transmissão de informações sem criptografia
- Descarte de mídias eletrônicas ou não
- Controles internos ineficientes
- Falta de planos de continuidade/contingência

Fonte: Relatórios de Conformidade (RoC) dos estabelecimentos

Serviços, Software e Hardware da IBM para Conformidade PCI

Cumprindo as Exigências do PCI DSS "*Digital Dozen*"

IBM PROFESSIONAL SERVICES

IBM SOFTWARE SOLUTIONS

IBM MANAGED SERVICES

IBM HARDWARE

1 FIREWALL TO PROTECT CARDHOLDER DATA

- IBM Proventia Server Intrusion Prevention System (IPS)
- IBM Proventia Network (IPS)
- IBM Global Services

2 NO DEFAULT PASSWORDS OR SECURITY PARAMETERS

- IBM Tivoli Access Manager
- IBM Proventia Network Multi-Function Security

3 PROTECT STORED CARDHOLDER DATA

- IBM Storage Manager
- IBM Data Encryption of IMS and DB2
- IBM Proventia Server IPS
- IBM PKI Services
- IBM Global Services

4 ENCRYPT TRANSMISSION

- IBM Data Encryption of IMS and DB2
- IBM Websphere
- Proventia Network Intrusion Prevention System
- DataPower XML Security Gateway

5 USE & UPDATE ANTI-VIRUS SOFTWARE

- IBM Proventia Desktop Endpoint Security
- IBM Proventia Network Enterprise Scanner
- IBM Global Services

6 SECURE SYSTEMS & APPLICATIONS

- IBM Software Development Platform
- IBM Tivoli CCMBD
- IBM Global Services
- IBM Rational AppScan

7 RESTRICT ACCESS

- IBM Tivoli Access Manager
- IBM Tivoli zSecure Admin
- IBM Tivoli Compliance Insight Manager
- IBM Global Services

8 UNIQUE IDs

- IBM Tivoli Identity Manager
- IBM Tivoli Federated Identity Manager
- IBM Global Services

9 RESTRICT PHYSICAL ACCESS

- IBM Digital Video Surveillance
- IBM Biometric Access Control
- IBM Global Services

10 MONITOR ACCESS

- IBM Tivoli Compliance Insight Manager
- IBM Tivoli Security Operations Manager
- IBM Proventia Server IPS
- IBM Global Services

11 TEST SECURITY SYSTEMS AND PROCESS

- IBM ISS Products & Services
- Tivoli Security Compliance Manager
- IBM Proventia Network Anomaly Detection System (ADS)
- IBM Global Services
- IBM Rational AppScan

12 SECURITY POLICY FOR EMPLOYEES & CONTRACTORS

- IBM Global Services
- Tivoli Console Insight Manager

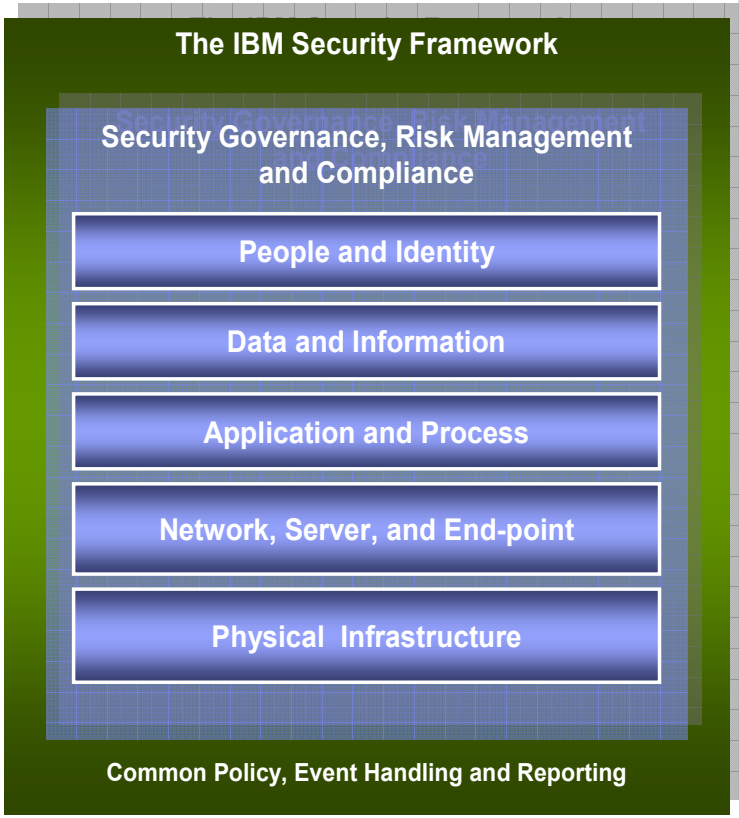
SECURE & PROTECT CARDHOLDER DATA

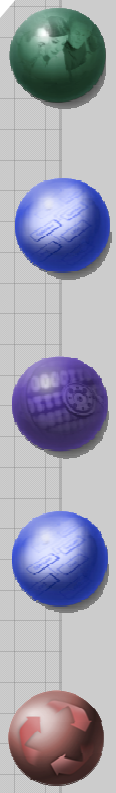
The IBM Security Framework
Compelling Reasons to Act

Serviços Profissionais

Serviços de Segurança Gerenciados

Hardware e Software de Segurança





- **CONFORMIDADE EM SEGURANÇA**
  - Mantenha uma Política de Segurança da Informação
- **GER. DE IDENTIDADES E ACESSOS(USUÁRIOS)**
  - Implemente Medidas Rígidas de Controle de Acesso
- **SEGURANÇA DE DADOS**
  - Proteja os Dados do Portador de Cartão
- **SEGURANÇA DE APLICAÇÕES**
  - Mantenha um Programa de Gerenciamento de Vulnerabilidades
- **SEGURANÇA DE INFRA-ESTRUTURA**
  - Construa e Mantenha uma Rede Segura
  - Monitore e Teste as Redes Periodicamente

The IBM Security Framework

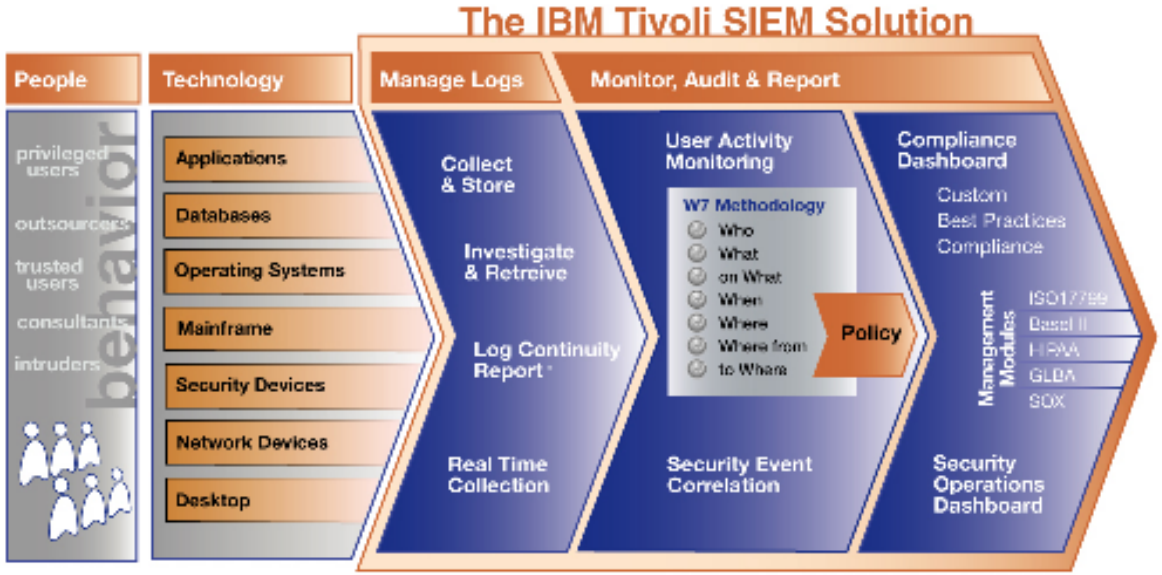
De uma empresa reativa para uma empresa orientada à risco

Conformidade em Segurança

Alinhando Segurança de TI com as prioridades de negócio

Nosso valor

- Rapidamente provamos que somente as pessoas certas estão acessando as informações sensíveis para o negócio.
- Efetivamente coletamos e reportamos todos os eventos relevantes de auditoria, alertas e logs gerados na sua infra-estrutura diariamente.
- Validamos que todos os sistemas, **includindo o System z**, estão configurados de forma segura



Soluções Chave:

- **Tivoli Security Information & Event Manager (TSIEM)**
- **Tivoli Compliance Insight Manager (TCIM)**
- **Tivoli Security Operations Manager (TSOM)**
- **Tivoli zSecure Suite**
- **Tivoli Security Compliance Mgr**
- **Rational (Watchfire) Portfolio**
- **ISS Proventia Portfolio**

Gerenciamento de Acessos e Identidades

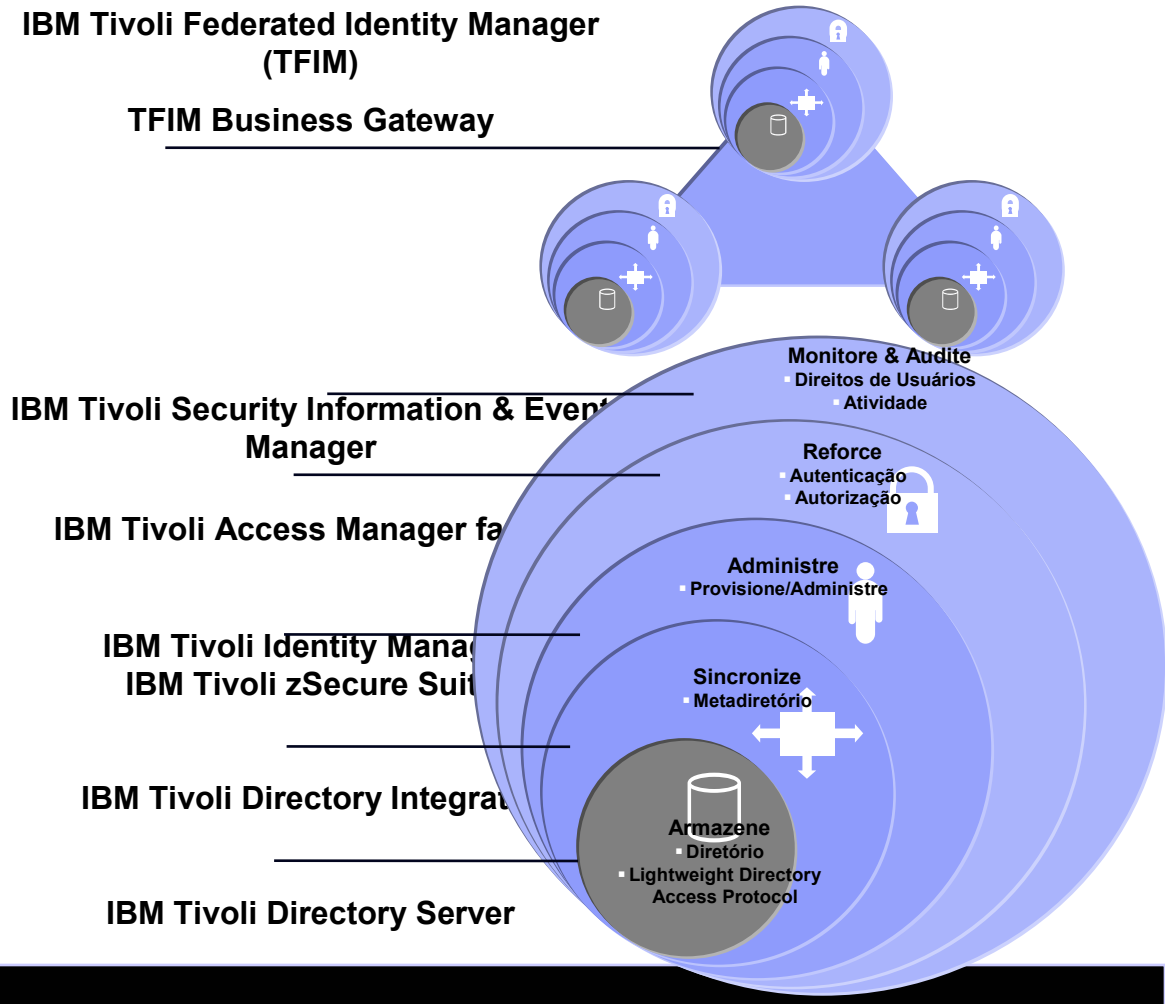
Gerencia usuários, identidades, direitos de acesso, reforça e monitora as atividades dos usuários em todos os sistemas de TI

Nosso valor

- Provisionamento: Rapidamente atribua ou certifique as contas de acesso dos usuários em todas as plataformas, incluindo System z
- Rapidamente localize e gerencie as contas de usuários

- Produtividade: Aumente a produtividade dos usuários através do conveniente mas seguro, suporte à *single sign-on.*

- Acesso e Auditoria: Controle o acesso consistentemente em aplicações corporativas, web, ou SOA-based.

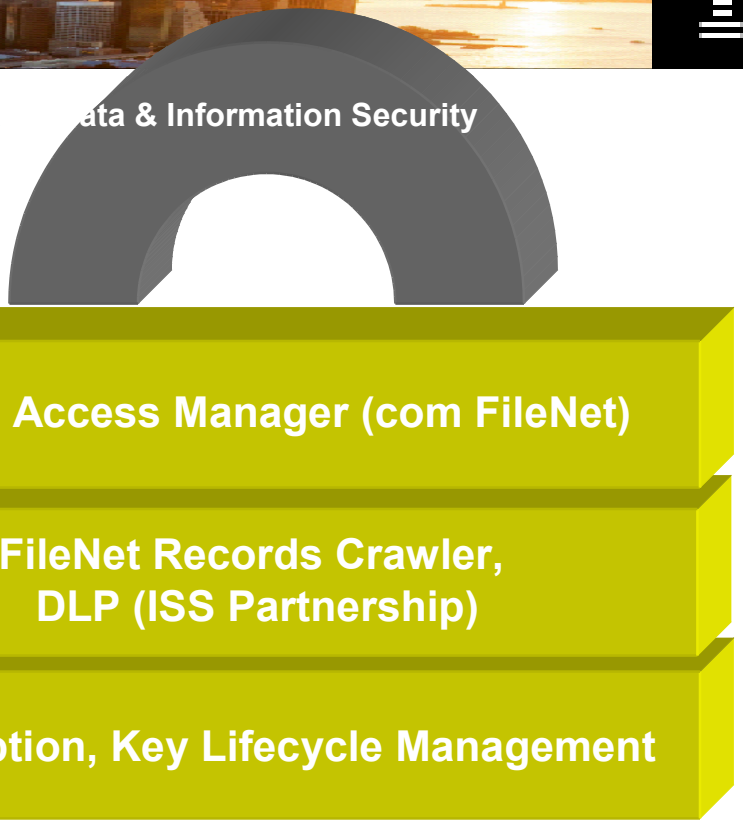


Segurança de Dados

Protegendo ativos críticos da empresa

Nosso Valor

- Consistentemente controle dados estruturados e não estruturados em todas as plataformas, incluindo o System z.



Soluções Chave:

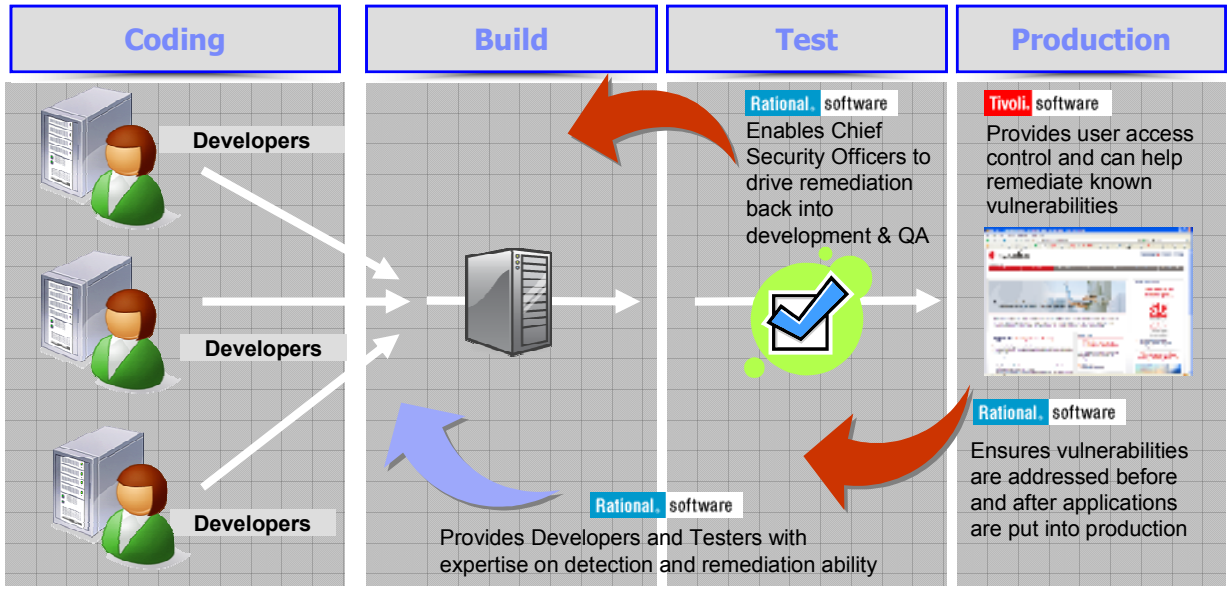
- **Tivoli Access Manager family**
- **ISS DLP Partnerships**
- **DB2 and STG Encryption**

Segurança em Aplicações

Gerenciamento da Política de Segurança em uma aplicação desde a concepção até a entrada em produção.

Nosso Valor

- Proteção contra as vulnerabilidades de aplicações mais comuns.
- Audita e controla o acesso à todas aplicações consistentemente – corporativas, web, e SOA-based
- Blinda os desenvolvedores das mudanças da Política de Segurança (autenticação, etc.)



Soluções Chave:

1. Vulnerabilidades de Aplicações
   - Rational AppScan e Tivoli Access Manager
2. Federated ESB ('identity-aware')
   - Tivoli Federated Identity Manager com WebSphere ESB (incluindo DataPower), WebSphere Service Registry and Repository, and Tivoli Composite Application Manager for SOA

Gerenciamento de Segurança da Infra-estrutura

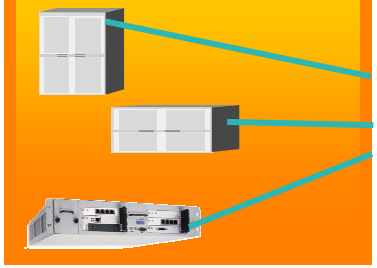
Comprehensive threat and vulnerability management across networks, servers and end-points

Nosso Valor

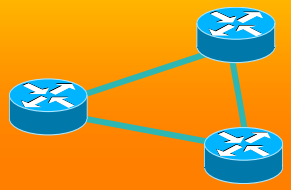
- Detectar e gerenciar ameaças e intrusões em redes, Hosts e endpoints
- Gerenciar e monitorar as operações de Segurança de forma Centralizada.

Gerenciamento de Eventos e Informações de Segurança

Perímetro



Rede Local (LAN)



Ambiente de Hosting

Web server
Mail server

Soluções Chave:

- **ISS Proventia portfolio**
- **Tivoli Security Information & Event Management**
  - **Tivoli Compliance Insight Manager**
  - **Tivoli Security Operations Manager**
- **Tivoli Security Compliance Mgr**

Pensamento

O Problema não vai ser resovido fazendo com que os dados sejam difíceis de se roubar. A forma de resolvermos o problema é fazendo com que os dados sejam difíceis de usar.

"We're not going to solve this by making data hard to steal. The way we're going to solve it is by making the data hard to use.."

Bruce Schneier, Autor, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World"

Conclusão

O mercado Brasileiro tem uma oportunidade muito grande para evoluir em aspectos importantes de segurança:

- Conscientização
- Prevenção
- Falsa sensação de segurança

O PCI não é a solução mágica ou total para a proteção das transações eletrônicas. Mas representa uma grande evolução para a confiança do sistema, e se adotado de forma consciente e responsável, pode tornar-se um padrão de fato.

Ou alguém quer ser a próxima TJX,Hannaford ou Heartland ?

Perguntas?

Obrigado!

Ed Wilson Menezes, CISSP, CISM
emenezes@br.ibm.com
11-2132-5875