Melhores Práticas de Segurança Cibernética

ANBIMA

MELHORES PRÁTICAS DE SEGURANÇA CIBERNÉTICA

ANBIMA

TIMELINE

JUL | OUT | 2014 | JAN | ABR | JUL | OUT | 2015 | JAN | ABR | JUL | OUT | 2016 | JAN | ABR

Jul 2013

IOSCO e WFE publicam resultados de pesquisa com 45 bolsas de valores

Dez 2013

Financial Stability Oversight Council organiza reunião para falar sobre Cybersecurity no sistema financeiro

Dez 2013

Target Corp anuncia Cyber ataque violando info 40 mi de clientes

Fev 2014

CFTC publica Guia sobre Práticas de Segurança de Dados

Jan 2014

FINRA Cybersecurity é prioridade na supervisão

Mar 2014

US SEC promove mesa redonda para discutir Cybersecurity

Abr 2014

US SEC promove iniciativa em Cybersecurity

Mar 2014

SEC Chair Mary Jo White

"SEC have been focused on cybersecurity-related issues for some time"

Aug 2014

JP Morgan reporta ataque que violou 83 milhões de contas e estabelece gastos anuais de **US$ 250 mi**

Nov 2014

Sony Pictures Custo divulgado foi de US$ 15 mi , podendo chegar a US$ 100 mi

Jan 2015

FINRA Cybersecurity continua prioridade na supervisão

Jan 2014

US SEC Estabelece Cybersecurity prioridade na supervisão

Fev 2015

FINRA Relatório de Práticas de Cybersecurity

Fev 2015

US SEC publica resultados de revisão temática

Jun 2015

OCC/FFIEC lança a ferramenta Cybersecurity Risk Assessment

Jun 2015

FFIEC estabelece Cybersecurity prioridade

Jan 2016

FINRA Cybersecurity continua prioridade na supervisão

Out 2015

US Senate aprova Lei Cybersecurity Info Sharing

Ago 2014

ANBIMA Supervisão foca em Cybersecurity

Mai 2016

CPI de Crimes Cibernéticos recomenda mudanças no SFN

Mai 2016

ANBIMA Promove debate sobre o assunto

Abr 2016

IOSCO publica Cyber Security in Securities Market

Jun 2016

Robert Van Dijk Presidente da ANBIMA

"Cybersecurity é tema relevante no mercado"

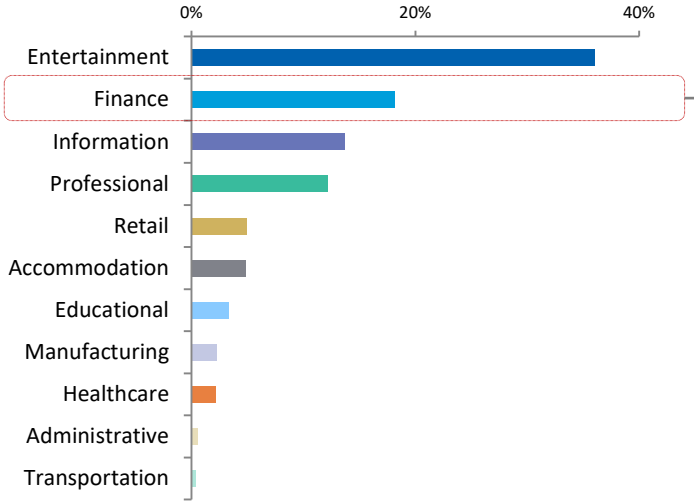
ANBIMA

Lança Guia de Cybersecurity

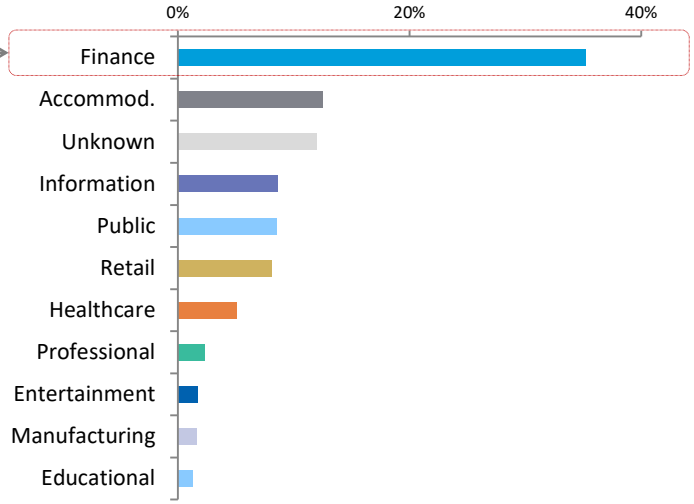
Posição do setor financeiro em violações de dados

Violações tem sido financeiramente motivadas

1. Incidentes por Setor[1]



2. Violação de Dados por Setor



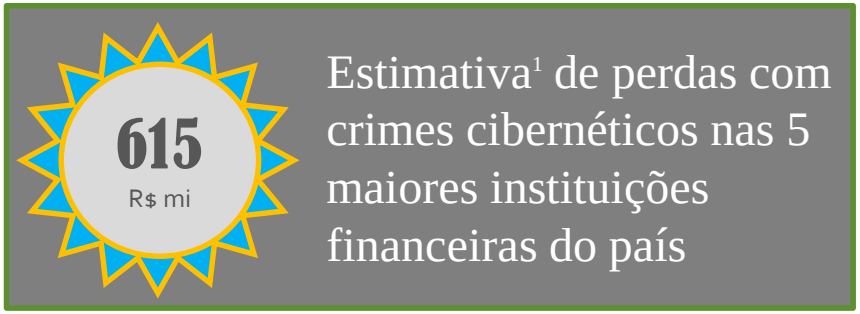
- 64.199 acidentes de violação de dados avaliados
- O Setor Financeiro vem sendo listado entre os 3 maiores alvos nos últimos anos
- 80% das violações de dados foram motivadas por questões financeiras
- Espionagem esta em segundo lugar das motivações para violação de dados com 15%

- 5% dos incidentes resultaram em violação, exposição de dados
- Setor financeiro apresenta maior percentual de violação de dados
- 63% das violações envolveram questões com senhas fracas, comprometidas ou padrões

1. 2016 Data Breach Investigations Report. Visando uma melhor visualização dos dados relativos por setores, foram retirados das estatísticas os dados do setor público e os não categorizados (“unkown”) por computarem aproximadamante 74% (47,237) e 15% dos incidentes respectivamente.

Tendências Regulatórias

O mercado financeiro atualmente necessita de iniciativas dos reguladores



Código Penal (Decreto-Lei 2.848/40)

Já prevê o crime de invasão de dispositivo informático (computador ou celular)

CVM cria FinTech Hub (13/06/16)

Núcleo que considera a intensificação do monitoramento das mudanças tecnológicas, mitigando eventuais riscos decorrentes e avaliar judiciosamente a necessidade de ajustes na regulação e na supervisão de mercado

CVM publica pesquisa "Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários" (Julho de 2017)

O risco cibernético consiste num tópico cada vez mais presente na academia e nos fóruns de reguladores internacionais de mercado de capitais, além de mais recentemente aparecer nas pautas regulatórias dos diversos países.

RELATÓRIO FINAL CPI DOS CRIMES CIBERNÉTICOS

NECESSIDADES DE REGULAMENTAÇÃO

- Normatização para exigir das instituições financeiras o reporte compulsório da ocorrência de crimes cibernéticos
- Banco Central do Brasil deve criar mecanismos para contabilizar de maneira segregada o risco cibernético

VARAS ESPECIAIS

- A criação de Varas Judicias Especializadas em Crimes Eletrônicos deverá dar maior celeridade ao tratamento desses crimes através da criação de equipes especializadas no âmbito da justiça
- Bloqueio e confisco de bens de criminosos cibernéticos

PARCERIAS

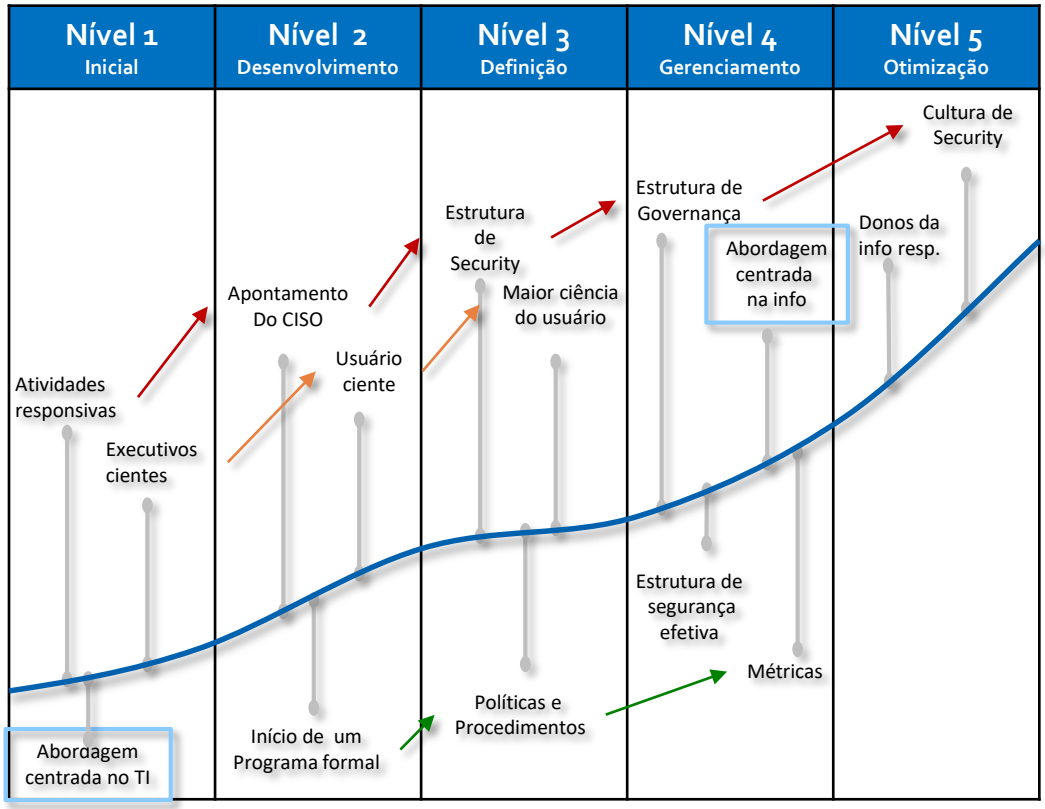
- Banco Central do Brasil e Polícia Federal devem estabelecer relacionamento para compartilhar informações e manter bancos de dados

1. Relatório Final CPI dos Crimes Cibernéticos

Avaliando a maturidade da sua governança

Evolução dos aspectos relevantes na construção de uma estrutura

8. ITScore Maturity Levels for Information Security [1]



PONTOS RELEVANTES [1]

- Leva 1 ano para passar de um nível para outro, salvo casos de esforços extraordinários
- Um dos grandes obstáculos ainda é a questão cultural
- Comprometimento dos executivos seniores, das linhas de negócios e outros stakeholders é um fator crítico para aumentar a maturidade

1. **Gartner** (February 2016) – ITScore for Information Security

Tendências Regulatórias Globais

Abordagens regulatórias para segurança cibernética de Basiléia

Serviços Financeiros e Risco Cibernético

Os serviços financeiros têm uma grande interface com os clientes e assim é vulnerável a ataques cibernéticos. Consequentemente o risco cibernético é uma dos principais preocupações para a maioria dos supervisores bancários.

Duas Abordagens Distintas

Duas diferentes visões sobre a necessidade de regulamentar o risco cibernético.

1. Pode ser gerenciado com a regulamentação atual sobre tecnologia e risco operacional.

2. Há necessidade de regulamentação para lidar com a natureza distinta do risco cibernético e devido as crescentes ameaças sobre o setor financeiro altamente digitalizado.

Nas jurisdições que já apresentam requerimentos específicos, há ainda debates sobre o nível adequado prescritivo de um normativo vis-à-vis um normativo baseado em princípios.
Apesar das diferenças há alguns pontos em comum para se iniciar uma estrutura regulatória de segurança cibernética.

PONTOS COMUNS DE UMA ESTRUTURA REGULATÓRIA

+ comuns

- Implementar políticas e/ou programas de segurança cibernética
- Definição clara de responsabilidades
- Inventário de ativos / informações críticas
- Execução de testes de vulnerabilidade e resiliência em riscos cibernéticos
- Reporte de eventos/incidentes cibernéticos

- comuns

- Compartilhamento de inteligência (cyber-threat intelligence sharing)
- Diligência de provedores terceirizados de serviços

Tendências Regulatórias Globais

Abordagens regulatórias para segurança cibernética de Basiléia

Abordagens de Supervisão

1. Revisões temáticas;

2. Uso de *threat intelligence* (inteligência de ameaça / ataque) para desenhar e simular ataques cibernéticos

3. Supervisores estão certificando seus profissionais

4. Aumento no nível de cooperação e coordenação entre os supervisores de diferentes jurisdições.

Considerações Relevantes

1. Incorporar o risco cibernético, assim como qualquer outro risco que instituições financeiras possuem, nas estruturas, matrizes e governança de gerenciamento de riscos.

2. Requerer que as IFs desenvolvam uma estrutura efetiva de controle e resposta para riscos cibernéticos, assegurando a implementação de práticas gerais e sólidas para gestão de riscos ("*general sound risk management practices*") no contexto de risco cibernético;

3. Considerar como ponto de partida os padrões técnicos existentes;

4. Alocação de maior foco na conscientização sobre riscos cibernéticos;

5. Beneficiar-se da colaboração futura com indústria no fortalecimento da segurança cibernética

6.Buscar cooperação e consistência *cross-border* regulatória e na abordagens de supervisão.

Alguns desenvolvimentos significantes recentes

2016 – O *Financial Stability Institute* (BIS) conduziu uma pesquisa com supervisores de 73 jurisdições fora da Basiléia e a maioria dos respondentes mencionou *fintech* e risco cibernético como os maiores desafios.

Junho de 2016 – IOSCO emite as Diretrizes sobre Resiliência Cibernética para as Infraestruturas do Mercado Financeiro.

Outubro de 2016 - G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR (out16) – ministros de economias e presidentes de banco centrais.

Novembro de 2016 - FSB inclui no plano de trabalho para 2017 uma ação para se monitorar os riscos cibernéticos oriundos do surgimento das *fintech* e identificar questões de supervisão e regulamentação sobre riscos cibernéticos da perspectiva de estabilidade financeira.

Julho de 2017 – FSB reporta para o G20 que a mitigação do impacto do risco cibernético na estabilidade financeira está entre as 3 maiores prioridades para futura cooperação internacional.

Tendências Regulatórias Globais

Alguns requerimentos regulatórios chave segundo Basiléia e IOSCO

Política ou Programa - O ponto de partida usual é a documentação de um programa ou política de segurança cibernética. Os requerimentos devem seguir os padrões de gestão de riscos do Comitê de Pagamentos e Infraestrutura de Mercado do BIS:

- **governança, identificação, proteção, detecção, resposta e recuperação.**

Assim sendo são requerimentos gerais sobre governança e supervisão, responsabilidade e papeis em gestão de riscos, estabelecimento de medidas e indicadores (*patch management procedures, access controls, identity management* etc), avaliação periódica e monitoria dos controles de segurança cibernética, resposta a incidentes e plano de recuperação.

Inventário de Ativos/Informações Críticas - IFs devem identificar ativos/informações críticas. No plano nacional os governos devem identificar as estruturas e instituições críticas. As IFs devem fazer o mesmo para priorizar os esforços em sistemas críticos.

Testes - Execução de testes de vulnerabilidade e resiliência

Reporte de Incidentes - Reporte de eventos/incidentes cibernéticos (sujeito a materialidade?). O FINCEN (COAF dos EUA) já exige o reporte de eventos cibernéticos em relatórios de atividade suspeita.

Inteligência sobre Ameaças Cibernéticas - Não demandam necessariamente uma norma mas podem ser encorajadas pelo regulador. O material do G7 inclui o compartilhamento de informações. Em algumas jurisdições o regulador é responsável pela plataforma de compartilhamento das informações.

Definição Clara de Papeis e Responsabilidades - Apesar da expectativa pela definição clara de papeis e responsabilidades: deve-se designar um CISO? Ele Deve reportar para o CRO ou para o CIO?

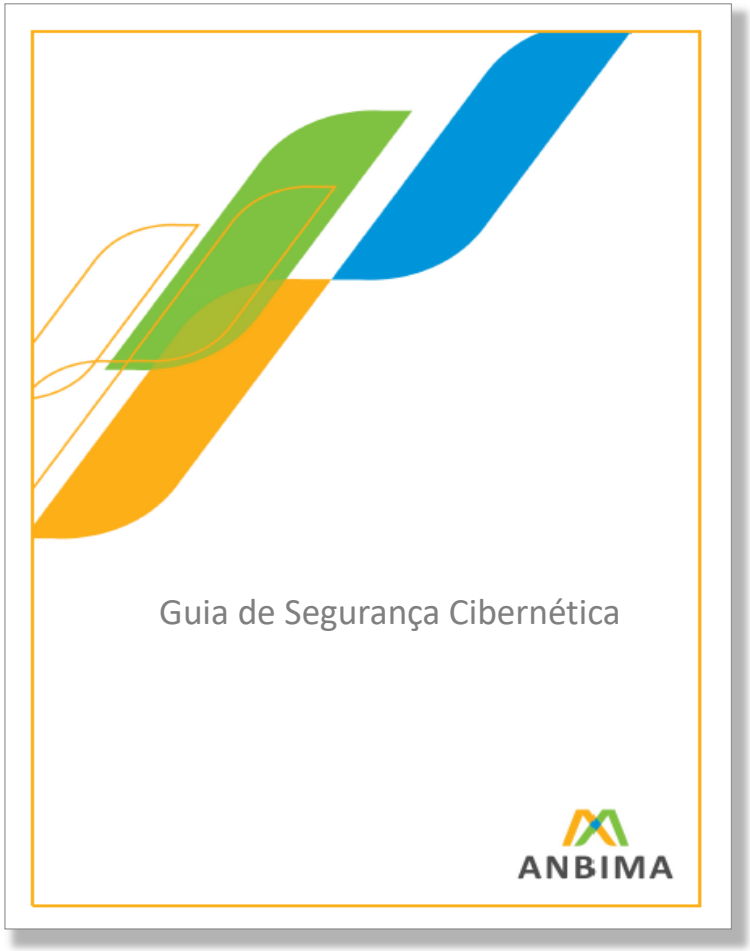
Gestão de Terceiros - As capacidades de gestão de riscos cibernéticos pelos provedores de serviços para terceiros são um elemento crítico de uma estrutura de gestão.

Certificação de Profissionais – Os profissionais devem ser certificados?

Treinamento – Programas de treinamento para todos os funcionários

Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos



- OBJETIVOS DESTE GUIA
- RISCO CIBERNÉTICO
- COMO COMEÇAR
- SEGURANÇA CIBERNÉTICA

PROGRAMA

- GOVERNANÇA CORPORATIVA
- CONTROLE DOS USUÁRIOS
- CONTROLES TECNOLÓGICOS
- PLANO DE RESPOSTA A INCIDENTES
- PROCESSO DE INVESTIGAÇÃO
- DIÁLOGO COM PARTES EXTERNAS
- PREVENÇÃO DOS ATAQUES INTERNOS

- DIVULGAÇÃO
- TRATATIVAS

Melhores Práticas de Segurança Cibernética

Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos

Risco Cibernético

Resultados negativos potenciais de um ataque cibernético-tentativas de comprometer a confidencialidade, intergridade e disponibilitidade de dados ou sistemas.

Segurança Cibernética

Conceito amplo que embarca todas as atividades para mitigação do risco cibernético, sendo a identificação, proteção, detecção, resposta e recuperação de um ataque cibernético.

Avaliação do Risco

Programa baseado em necessidades, elaborando e mantendo um **risk assessment** atualizado que deve ser compatível com as características e tamanho da instituição e os recursos de defesa e respostas, proporcionais aos riscos identificados.

MOTIVAÇÕES

- Ganho financeiro
- Roubo de informações
- Vantagem competitiva
- Fraudes
- Exposição de fragilidade
- Terrorismo e pânico

PILARES

- Identificação
- Prevenção
- Detecção
- Proteção
- Tratativas
- Reciclagem

CHECK-LIST

- Identificação dos ativos e riscos
- Mensuração dos riscos
- Segurança dos dados
- Processos
- Contingência
- Qualificação dos profissionais
- Identificação de ameaças
- Vulnerabilidades
- Impactos

ANBIMA

Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos

Governança Corporativa

- Definição das responsabilidades
- Criação de um comitê
- Realização de auditoria
- Plano de continuidade de negócios
- Classificação das informações mais sensíveis
- Definição do ciclo de vida das informações

Controle de Usuário

- Políticas de controles de acesso para trabalhos fora do escritório
- Troca periódica de senhas
- Definição do perfil de acesso dos Colaboradores e administradores de rede
- Definição do perfil de acesso dos prestadores de serviços,
- Gerenciamento e controle dos acessos privilegiados
- Treinamento
- Canais de comunicação e divulgação das políticas e procedimentos internos

Controles Tecnológicos

- Proteção dos dados
- Rastreamento das informações nas nuvem
- Inventários dos hardwares e softwares
- Atualização dos sistemas
- Prevenção de ameaças com firewalls, antivírus
- Detecção de ameaças
- Inclusão das preocupações de segurança no desenvolvimento
- Controles de auditoria
- Utilização de dados fictícios em ambientes não produtivos
- Segregação dos ambientes de desenvolvimento, teste e produção
- Mesmo nível de segurança e proteção às aplicações que se utilizem de informações críticas

Controle Físico

- Perfis de acesso às instalações do escritório
- Gerenciamento e controle dos acessos
- Espaço físico adequado e seguro para a guarda dos equipamentos
- Restrição de acesso físico das áreas com informações críticas/sensíveis
- Segurança e controles de acesso nas instalações de contingência
- Acesso remoto por usuários devidamente identificados e autenticados
- Uso exclusivo de equipamentos homologados

ANBIMA

Guia ANBIMA de Segurança Cibernética

Reguladores e autorreguladores têm voltado maior atenção para assuntos relacionados a riscos cibernéticos

Resposta Incidentes

- Critérios para classificação
- Lista de ativos críticos
- Procedimentos de detecção e investigação
- Plano de acionamento dos Colaboradores-chaves e contatos externos relevantes
- Tomada de decisões e ações técnicas de acordo com vários cenários possíveis de ataques
- Plano de comunicação
- Medidas de remediação; e
- Plano de continuidade dos negócios.

Investigação

As investigações de cibersegurança incluem a coleta, a análise e a preservação de dados (conforme aplicável) com o objetivo de identificar a origem e as características de uma invasão/ataque cibernético. Para êxito nas investigações, é recomendável definir o protocolo que direcione a análise com a interrupção ou não do ataque e utilizar técnicas forenses que suportem a preservação das provas em caso de requerimentos legais.

É recomendável manter o histórico das análises com o objetivo de obter indicadores que permitam identificar, de forma preditiva, tendências e comportamentos.

Diálogo Externo

Fornecedores, prestadores de serviços e parceiros (“Partes Externas”) podem representar uma fonte significativa de riscos para as instituições.

Recomenda-se que as instituições discutam com as Partes Externas os controles estabelecidos por eles a respeito da cibersegurança antes de celebrar um contrato de prestação de serviços e durante sua execução. Em geral, o nível de diligência desejável depende do risco que a relação com o fornecedor pode criar para a instituição.

Ataques Internos

Boas práticas na prevenção dos ataques internos juntam ferramentas tecnológicas (por exemplo, de monitoramento das redes) com o conhecimento interno dos fatores humanos das instituições. Alguns indicadores podem revelar comportamentos duvidosos (fracassos repetidos no login, downloads massivos de dados etc., mas, também, conflitos entre Colaboradores ou ameaças).

Fotografia do Mercado Brasileiro

Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários

Política ou Programa

43% dos agentes fiduciários de pequeno porte não possuem nenhum programa para gerenciamento do risco cibernético.

Matriz de Segregação de Funções

Um dos itens que normalmente é constante de uma política de riscos cibernéticos é a instituição de uma matriz de segregação de funções em relação às responsabilidades de gerenciamento de risco cyber, isto é, a prática de se adotar divisões de funções e definição de segregações sobre processos pertinentes a gestão e governança cibernética.

68% dos pequeno possuem tal segregação.

Plano de Recuperação

Formalmente estabelecido: **57%** dos administradores fiduciários possuem.

Certificação de Profissionais – 86% não é requisito possuir nenhuma certificação dos profissionais de segurança da informação.

Treinamento – 60% possuem treinamento para toda instituição. Nos pequenos **26%** não possuem ações de treinamento voltadas a segurança da informação.

Processos operacionais e partes afetadas - primazia dos processos relativos a cadastros de clientes e de processos de movimentação financeira, ambos com uma percepção de riscos muito próxima e bem a frente dos demais processos.

Formas de ataque - Numa análise de percepção de risco com relação aos pares e parceiros comerciais diretos, a mesma tende a ser um pouco maior para a invasão/exploração de vulnerabilidades, ao passo que em relação às próprias atividades, a percepção de risco tende a ser um pouco maior para *phishing* e negação de serviço do que para invasão/exploração de vulnerabilidades.

Conclui-se ainda que exista um viés de porte, devido à preocupação mais acentuada com a questão da engenharia social nas instituições grandes em relação às pequenas, levando novamente a crer que em instituições maiores o fator "pessoas" pode possuir um pouco mais de criticidade do que o fator "sistemas" na percepção de riscos.

1. Relatório Final CPI dos Crimes Cibernéticos

Fotografia do Mercado Brasileiro

Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários

Governança e gerenciamento de riscos cibernéticos - Quais das cinco funções principais seriam prioritárias:

identificação de riscos, proteção, detecção de vulnerabilidades, resposta às ameaças e recuperação de ativos

Estruturas e políticas formais são chaves ficando em primeiro.

Em segundo lugar, ficariam os processos de identificação de possíveis vulnerabilidades, depois seguidos por processos de detecção de vulnerabilidades, proteção de ativos, recuperação de ativos e resposta às ameaças detectadas.

Proteção contra ameaças - As medidas de controle de acesso são a principal prática.

Pequeno porte - Armazenamento e backup de informação e da existência de um plano de gerenciamento de vulnerabilidades desenvolvido e implementado.

Detecção de ameaças - Os processos de comunicação são os menos prioritários, depois dos papeis e responsabilidades bem definidos.

→ Pode haver deficiências no processo de comunicação quando da detecção de uma ameaça, inclusive aos órgãos reguladores, o que no limite poderia prejudicar os procedimentos de resposta.

Papeis e responsabilidades bem definidas não são prioridade na detecção de ameaças. Por fim, instituições grandes aparentam conferir maior valor à tempestividade da detecção de uma ameaça do que instituições pequenas.

Resposta a ameaças e recuperação de ativos - planos de resposta e recuperação definidos, consiste no processo principal, seguido pela contenção e isolamento da ameaça e da realização de testes nos planos de resposta.

O processo de reporte voluntário aos stakeholders, por sua vez, foi o menos prioritário.

Portanto, conclui-se que no que tange à respostas a ameaças e recuperação de ativos, uma medida de caráter mais estratégico consiste no processo principal. Além disso, o processo de comunicação, inclusive aos órgãos reguladores, novamente não é prioritário, podendo consistir numa vulnerabilidade.

Plataformas de negociação e pós-negociação - Ou seja, o questionário fornece evidências de que as plataformas de negociação e pós-negociação não ensejam percepções críticas em termos de risco cibernético aos participantes do mercado de capitais brasileiro.

1. Relatório Final CPI dos Crimes Cibernéticos

Rio de Janeiro
Av. República do Chile, 230 13º andar
20031-170 Rio de Janeiro RJ Brasil
+ 55 21 3814 3800

São Paulo
Av. das Nações Unidas, 8.501 21º andar
05425-070 São Paulo SP Brasil
+ 55 11 3471 4200

ANBIMA