Questões Atuais Sobre Seguros e Gestão de Riscos Cibernéticos

MATTOS FILHO >

Mattos Filho, Veiga Filho,
Marrey Jr e Quiroga Advogados

MATTOS FILHO > Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

Questões Atuais Sobre Seguros e Gestão de Riscos Cibernéticos

Camila Leal Calais

Agenda

- Anatomia do risco cibernético
- Danos causados por incidentes cibernéticos
- Reputação e imagem
- Algumas considerações sobre como abordar o risco cibernético

MATTOS FILHO >

Anatomia do risco cibernético

- **Definição:**

"Risco cibernético refere-se aos potenciais resultados negativos associados a ataques cibernéticos. Por sua vez, ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas computacionais"

O Global Risks Report de 2019 do **World Economic Forum** classifica os riscos cibernéticos como a **quarta maior ameaça** à economia mundial.

Fontes: **IOSCO**, in Percepção de riscos cibernéticos nas atividades de administradores fiduciários e intermediários, CVM (Link: http://www.cvm.gov.br/export/sites/cvm/menu/acesso_informacao/serieshistoricas/estudos/anexos/Percepcao_de_riscos_ciberneticos_nas_atividades_de_administradores_fiduciarios_e_intermediarios.pdf)
Global Risks Report 2019, **Word Economic Forum** (Link: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf)

I. Quem são as principais vítimas dos incidentes?

- **Setor público**: 16%
- **Organizações de saúde**: 15%
- **Instituições financeiras**: 10%
- **Pequenos negócios**: 43%

II. Quem são os autores dos incidentes?

- **Agentes externos**: 69%
- **Agentes internos**: 34%
- **Organizações criminosas**: 39%
- **Nações ou agentes governamentais**: 23%

III. Quais os motivos dos incidentes?

- **Motivações financeiras:** 71%
- **Vantagens estratégicas (por exemplo, espionagem)**: 25%

IV. Como se deram os incidentes?

- **Phishing**: 32%
- **Roubo de credenciais**: 29%

Fonte: Verizon Data Breach Investigations Report 2019, **Verizon** (Link: https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/)

Danos causados por incidentes cibernéticos

Responsabilidade Civil

- Danos a dados da própria empresa
- Danos a dados de terceiros
- Danos a dados de empregados
- Danos a dados em arquivos inativos
- Danos a bens de terceiros
- Danos à integridade física de terceiros

Outros Danos

- Comprometimento de *softwares, hardwares* e infraestrutura física
- Lucros Cessantes

Exemplos de reparações a danos previstas em leis (tais como Código Civil, Lei das S.A. e LGPD):

- Por prejuízos de terceiros originados em vazamento de dados (corporativos ou pessoais)
- Por prejuízos de terceiros originados em manipulação de dados (publicação de dados confidenciais não autorizada)
- Por prejuízos originados em violação de dados que implique infração de propriedade intelectual
- Por prejuízos originados em violação de dados que resulte em publicação de conteúdos de mídia que causem dano a terceiros
- Por prejuízos originados em violação de dados na prestação de serviços de empresas de assessoria em tecnologia
- Por danos morais oriundos da veiculação de dados sem autorização do titular

The New York Times

"Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say"
6/7/2017

BBC

"Hackers breached a dozen US nuclear plants, reports say"
7/7/2017

FOLHA DE S.PAULO

"Ciberataque interrompe a impressão e entrega de jornais nos EUA"
30/12/2018

Forbes

"Cyberattack on LAPD Confirmed: Data Breach Impacts Thousands of Officers"
30/7/2019

The New York Times

"A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try"
15/3/2018

REUTERS

"Hackers halt plant operations in watershed cyber attack"
14/12/2017

Reputação e imagem

Estudo realizado pela **Comparitech** demonstra que, a longo prazo, as ações de companhias que sofreram incidentes cibernéticos tiveram um desempenho inferior comparado ao desempenho observado no mercado em geral:

Após **1** ano da data de divulgação do incidente cibernético, o preço médio das ações das companhias aumentou em **8,53%** em média, mas apresentou um desempenho médio inferior ao NASDAQ em **-3,7%**;

Após **2** anos da data de divulgação do incidente cibernético, o preço médio das ações das companhias aumentou em **17,78%** em média, mas apresentou um desempenho médio inferior ao NASDAQ em **-11,35%;** e

Após **3** anos da data de divulgação do incidente cibernético, o preço médio das ações das companhias aumentou em **28,71%** em média, mas apresentou um desempenho médio inferior ao NASDAQ em **-15,58%**.

Fonte: How data breaches affect stock market share prices, Comparitech (Link: https://www.comparitech.com/blog/information-security/data-breach-share-price-2018/#Long_term_effects_of_data_breach_on_share_price)

Algumas considerações sobre como abordar o risco cibernético

- Riscos cibernéticos devem figurar entre os pontos de maior atenção da alta administração da empresa (sensibilização);

- Usando metodologia e processos, riscos cibernéticos devem ser (i) abordados junto a todos os departamentos da empresa e (ii) tratados nos mais diversos documentos da empresa, desde políticas a contratos;

- Gestão de riscos cibernéticos: constância e ritmo; ferramentas; pessoas (incluindo terceiros); envolvimento de toda a organização;

- Realização periódica de auditorias e testes internos e externos;

- Elaboração de procedimento para incidente cibernético (resposta);

- Elaboração de programa de continuidade de negócios; e

- **Seguro de riscos cibernéticos** (atentar para *silent cyber*).

www.mattosfilho.com.br

SÃO PAULO – PAULISTA
Al. Joaquim Eugênio de Lima 447
01403 001 São Paulo SP Brasil
T 55 11 3147 7600

SÃO PAULO – FARIA LIMA
Rua Campo Verde 61 3º andar
01456 010 São Paulo SP Brasil
T 55 11 3035 4050

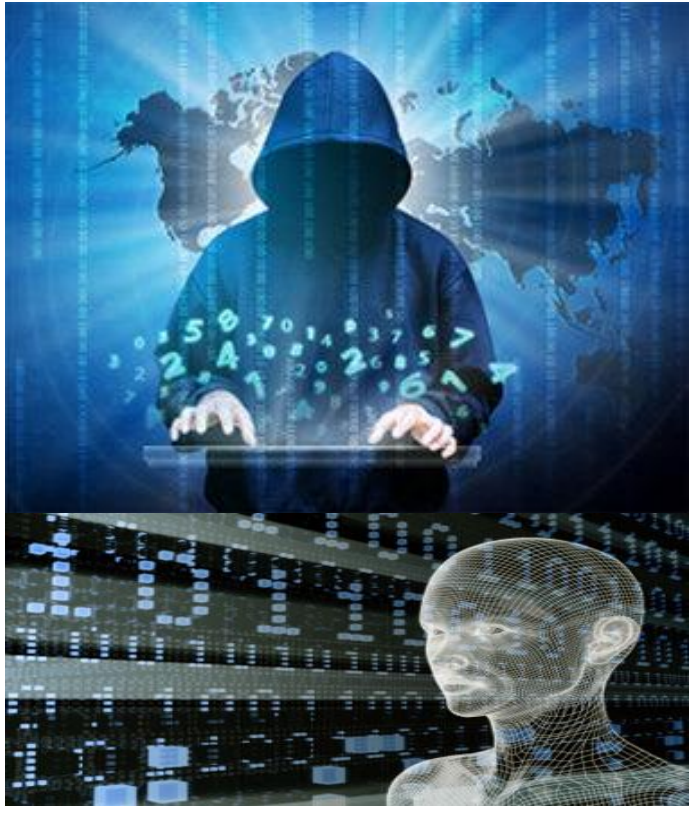
BRASÍLIA
SHS Q6 Bloco C Cj. A sala 1901
70322 915 Brasília DF Brasil
T 55 61 3218 6000

RIO DE JANEIRO
Praia do Flamengo 200 11º andar
22210 901 Rio de Janeiro RJ Brasil
T 55 21 3231 8200

NEW YORK
34 East 51st Street, 12th floor
New York, NY 10022 U.S.A.
T 1 646 695 1100

LONDON
5th floor, 32 Cornhill
London UK EC3V 3SG
T 44 (0)20 7280 0160

Questões Atuais Sobre Seguros e Gestão de Riscos Cibernéticos



1. ISACA - Apresentação Institucional
2. Ataques e Incidentes Cibernéticos
3. Frameworks e Padrões

Information Systems Audit & Control Association

Contact: news@isaca.org
Kristen Kessinger, +1.847.660.5512
Joanne Duffer, +1.847.660.5564
Jay Schwab, +1.847.660.5693

ISACA Fact Sheet
www.isaca.org

About ISACA

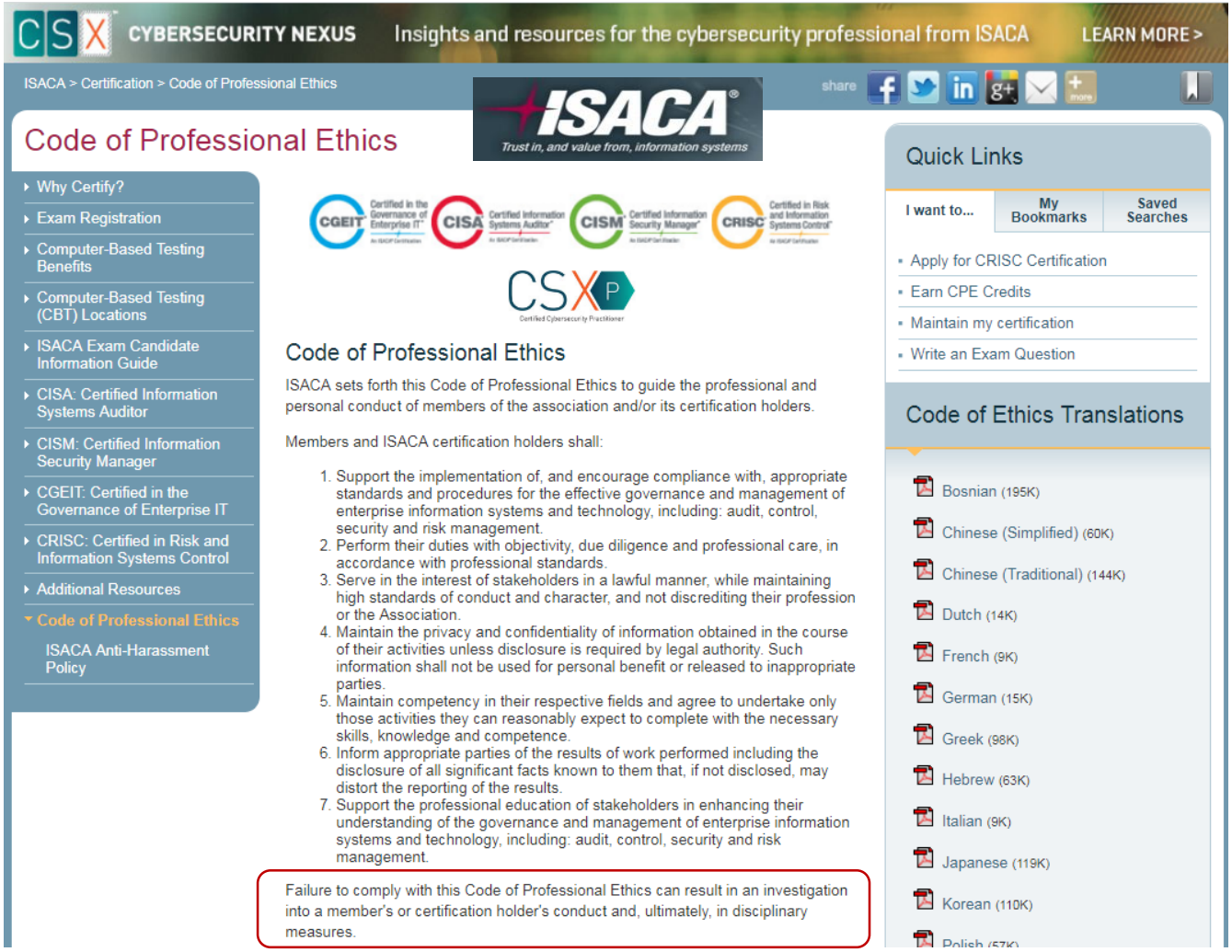
ISACA® is the voice of the information systems audit, IT governance, risk management and cybersecurity professions. For nearly 50 years, ISACA has helped enterprises develop strong IT workforces by inspiring and equipping individuals to be more capable, valuable and successful in the fast-changing world of information technology and business.

By offering industry-leading knowledge, standards, credentialing and education, ISACA enables professionals to apply technology in ways that instill confidence, address threats, drive innovation and create positive momentum for their organizations.

ISACA is the creator of the COBIT framework, which helps organizations effectively govern and manage their information and technology. Through its Cybersecurity Nexus (CSX), ISACA helps organizations develop skilled cyber workforces and enables individuals to grow and advance their cyber careers.

ISACA Membership and Chapters

Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 187 countries. Its members include internal and external auditors, CEOs, CFOs, CIOs, educators, information security and control professionals, business managers, students, and IT consultants. ISACA has more than 210 chapters in more than 80 countries.



CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA LEARN MORE >

ISACA > Certification > Code of Professional Ethics

share

ISACA Trust in, and value from, information systems

Code of Professional Ethics

- Why Certify?
- Exam Registration
- Computer-Based Testing Benefits
- Computer-Based Testing (CBT) Locations
- ISACA Exam Candidate Information Guide
- CISA: Certified Information Systems Auditor
- CISM: Certified Information Security Manager
- CGEIT: Certified in the Governance of Enterprise IT
- CRISC: Certified in Risk and Information Systems Control
- Additional Resources
- Code of Professional Ethics
  - ISACA Anti-Harassment Policy

CGEIT Certified in the Governance of Enterprise IT™ · CISA Certified Information Systems Auditor™ · CISM Certified Information Security Manager™ · CRISC Certified in Risk and Information Systems Control™

CSXP Certified Cybersecurity Practitioner

Code of Professional Ethics

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

Quick Links

I want to... | My Bookmarks | Saved Searches

- Apply for CRISC Certification
- Earn CPE Credits
- Maintain my certification
- Write an Exam Question

Code of Ethics Translations

- Bosnian (195K)
- Chinese (Simplified) (60K)
- Chinese (Traditional) (144K)
- Dutch (14K)
- French (9K)
- German (15K)
- Greek (98K)
- Hebrew (63K)
- Italian (9K)
- Japanese (119K)
- Korean (110K)
- Polish (57K)

Trust in, and Value from, Information Systems

CGEIT Certified in the Governance of Enterprise IT

CISM Certified Information Security Manager

CISA Certified Information Systems Auditor

CRISC Certified in Risk and Information Systems Control

20 YEARS COBIT 5 AN ISACA FRAMEWORK

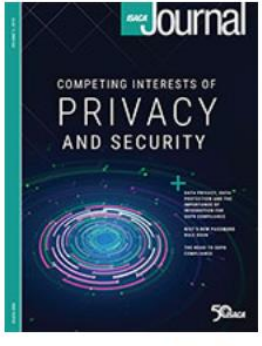
CSX CYBERSECURITY NEXUS

- Current Issue
- Practically Speaking Blog
- CPE Quizzes
- Submit an Article
- Advertise
- Editorial Calendar
- Read More on COBIT
- Archives
  - 2019
  - 2018
  - 2017
  - 2016
- Journal Print Opt-In Steps

Join ISACA and enjoy these

2019

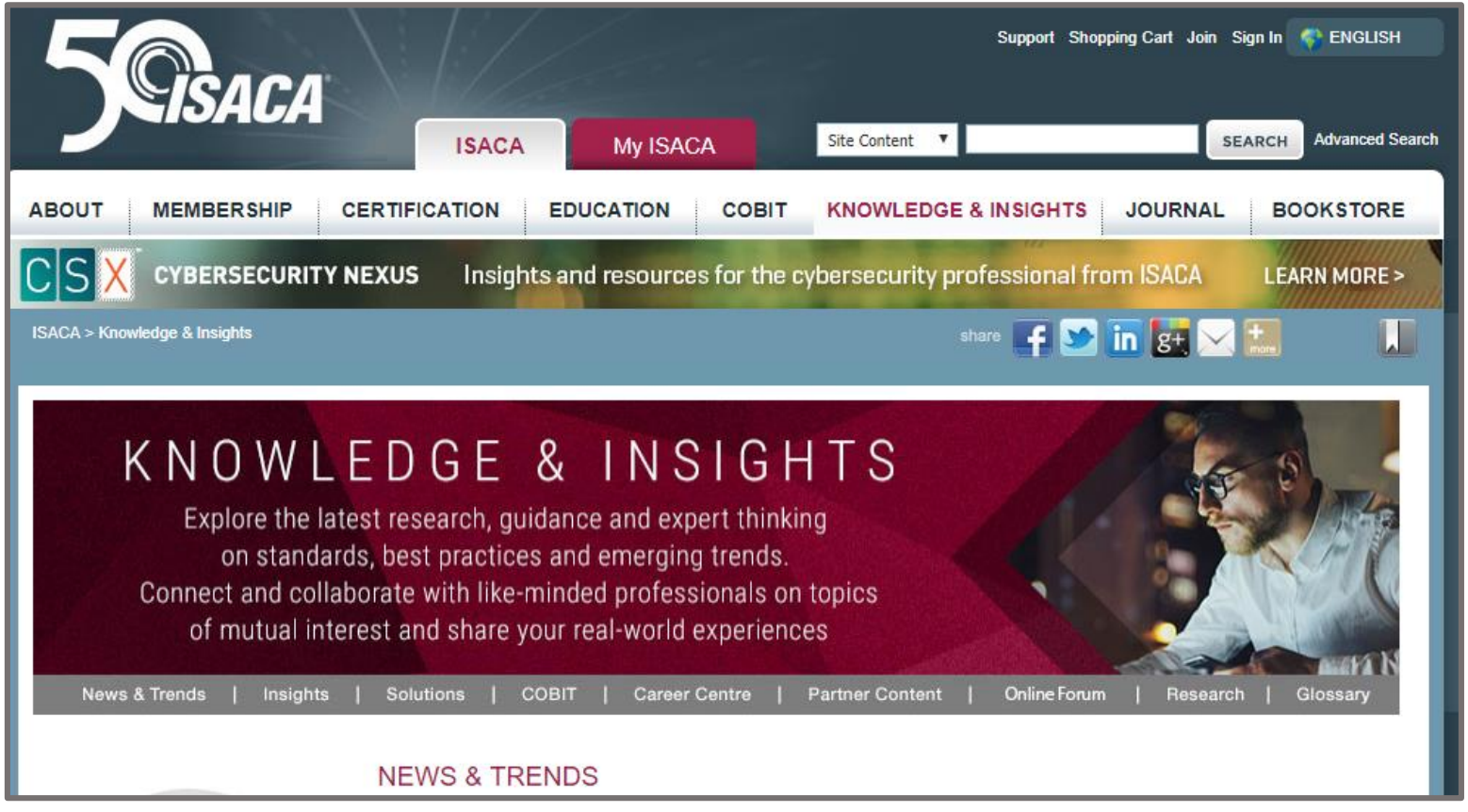
Volume 2, 2019
Tomorrow's Security Today



Volume 1, 2019
Competing Interests of Privacy and Security

Volume 1, 2018
The Future of Data Protection

Knowledge Center



Segurança

- ✓ CID – **Confidencialidade, Integridade, Disponibilidade**

  Independente do formato

- ✓ Documentos em papel e digitais
- ✓ Comunicação verbal e visual
- ✓ Propriedade Intelectual

- ➢ **Proteção dos Ativos Digitais** : CID + Autenticidade + Não Repudio => PPTs
- ➢ Tratamento das Ameaças e Riscos Cibernéticos
- ➢ Ataques sofisticados, intencionais, direcionados
- ➢ Informações processadas, armazenadas e transmitidas
- ➢ Sistemas de Informação **Interconectados em Rede**

Segurança - Domínios

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communication and Network Security
5. Identity and Access Management
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

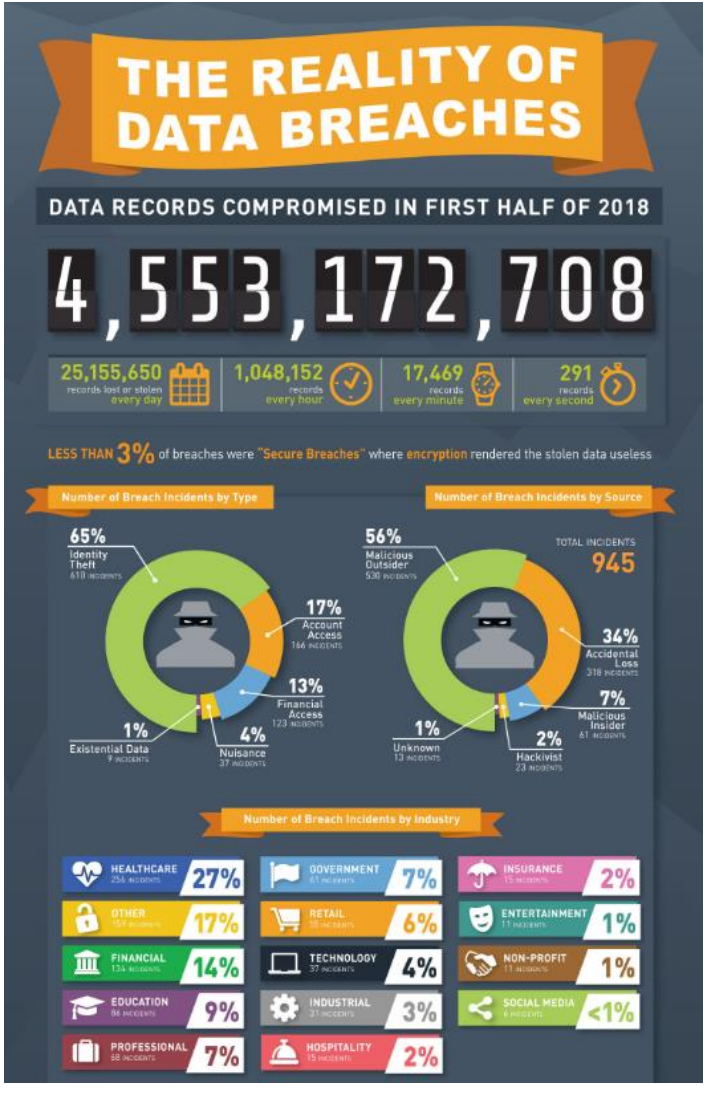
CISSP – Certified Information Systems Security Professional CBK

$(ISC)^2$ - International Information System Security Certification Consortium

Risco Cibernético

Ataques e Incidentes Cibernéticos

CONHECIDOS

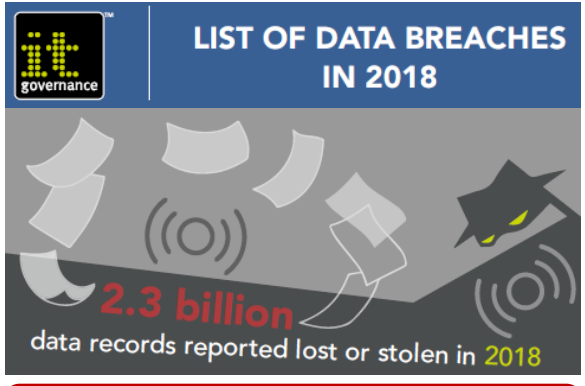


PC NEWS All Re

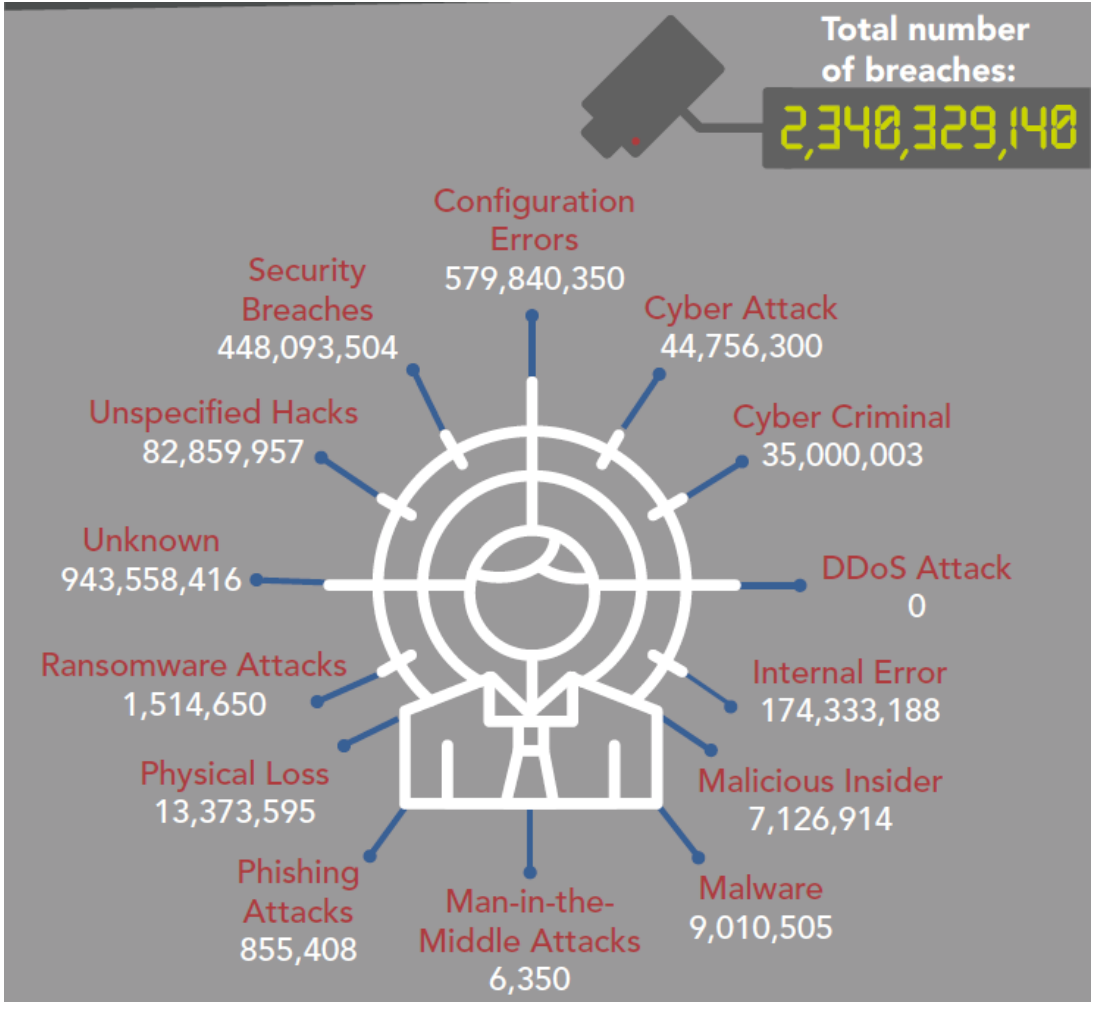
2018 - 1º. Semestre

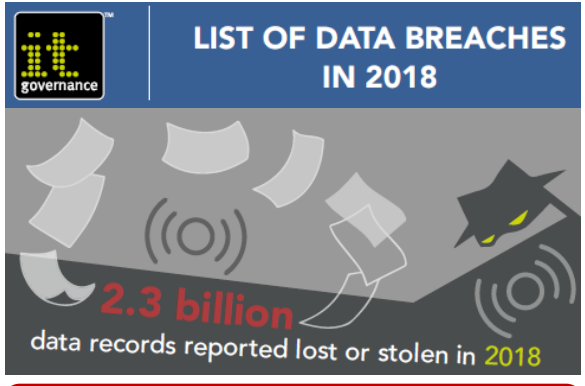
759 M / mês

~ 10 x mais - 2017

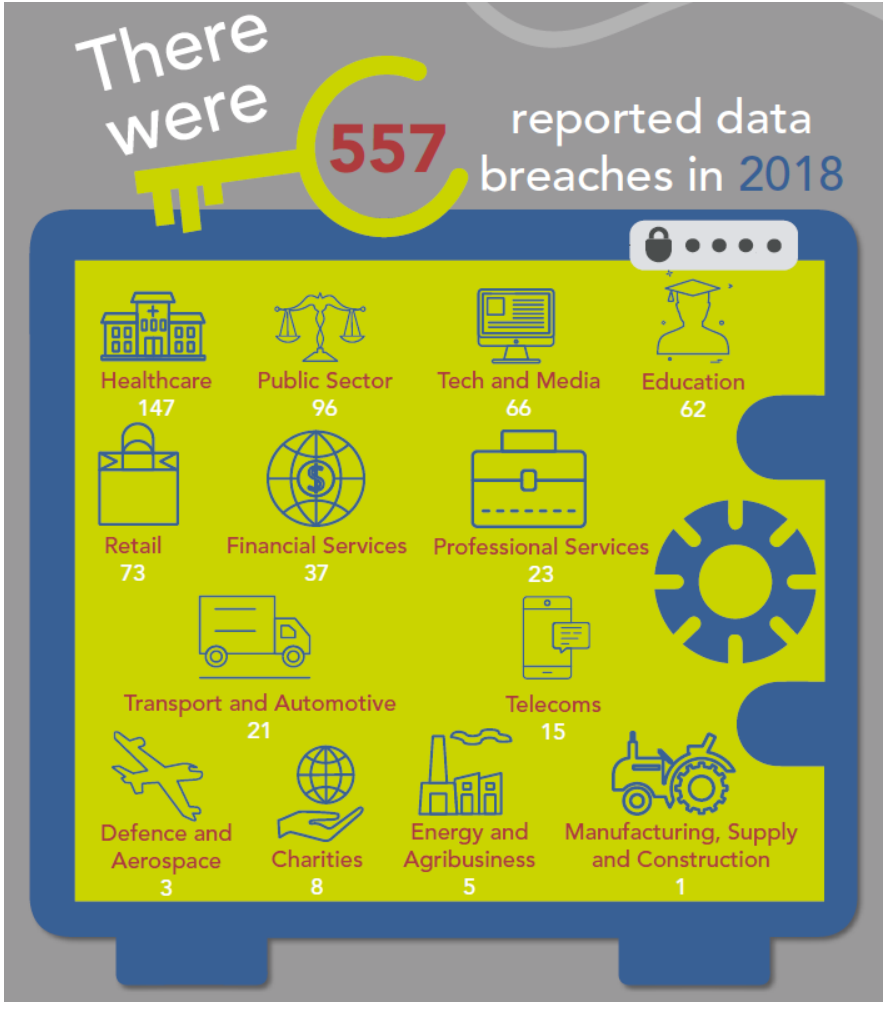

LIST OF DATA BREACHES IN 2018
2.3 billion
data records reported lost or stolen in 2018

CONHECIDOS


Total number of breaches:
2,340,329,140
Configuration Errors
579,840,350
Security Breaches
448,093,504
Cyber Attack
44,756,300
Unspecified Hacks
82,859,957
Cyber Criminal
35,000,003
Unknown
943,558,416
DDoS Attack
0
Ransomware Attacks
1,514,650
Internal Error
174,333,188
Physical Loss
13,373,595
Malicious Insider
7,126,914
Phishing Attacks
855,408
Man-in-the-Middle Attacks
6,350
Malware
9,010,505

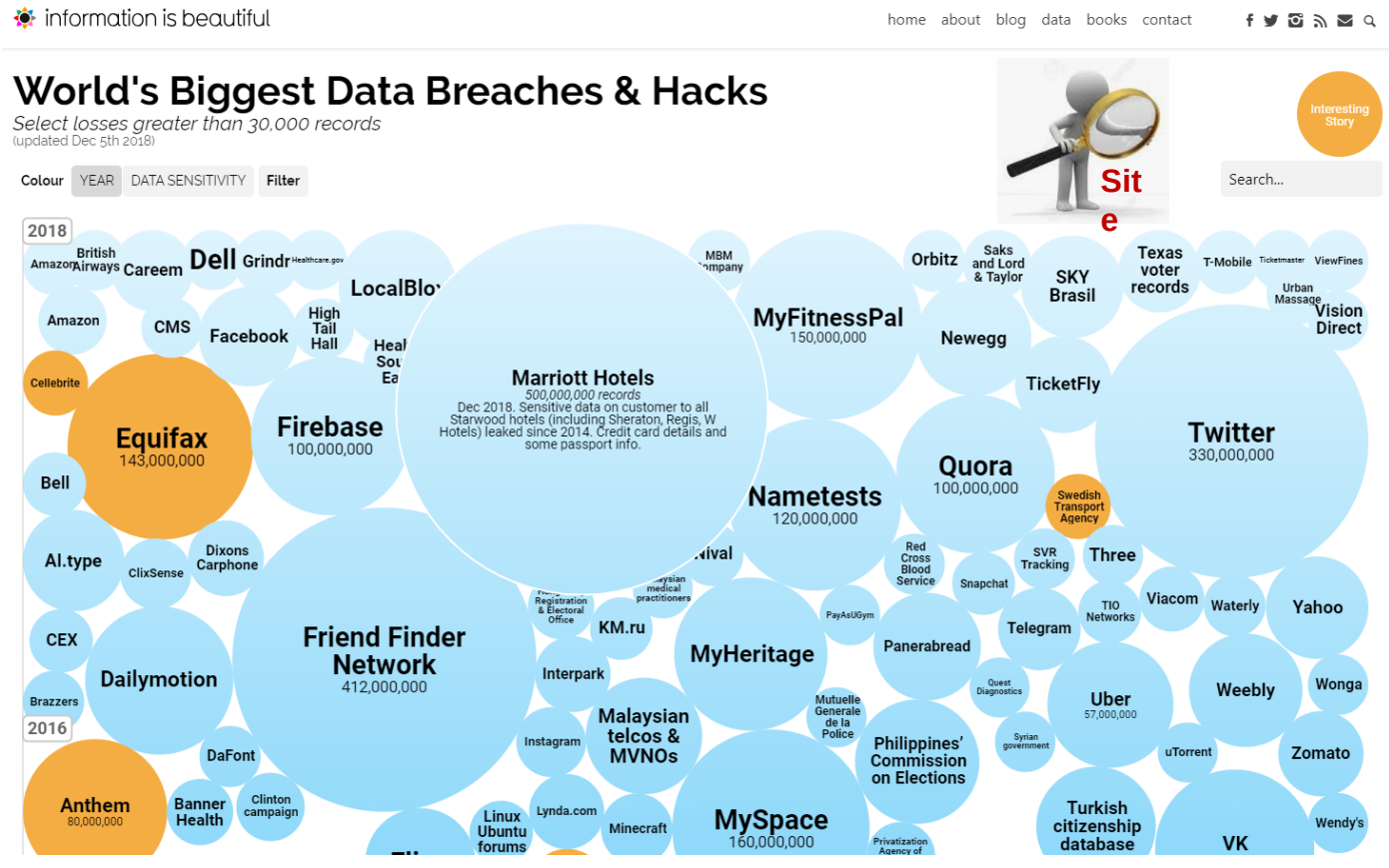

LIST OF DATA BREACHES IN 2018
2.3 billion
data records reported lost or stolen in 2018

CONHECIDOS


There were 557 reported data breaches in 2018
Healthcare 147
Public Sector 96
Tech and Media 66
Education 62
Retail 73
Financial Services 37
Professional Services 23
Transport and Automotive 21
Telecoms 15
Defence and Aerospace 3
Charities 8
Energy and Agribusiness 5
Manufacturing, Supply and Construction 1

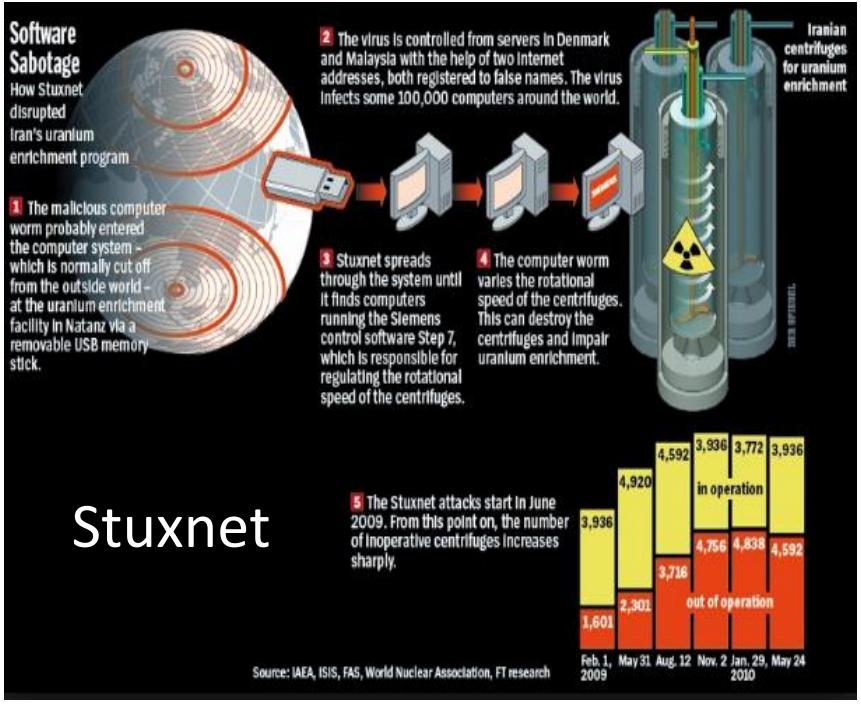
Ataques e Incidentes Cibernéticos

CONHECIDOS



Risco Cibernético

2010 | 03/16 | 07/17 | 12/17



Stuxnet

- + 15 Sites Industriais
- Destruição de 984 Centrífugas de Enriquecimento de Urânio
- 30% Redução na capacidade de enriquecimento de Urânio

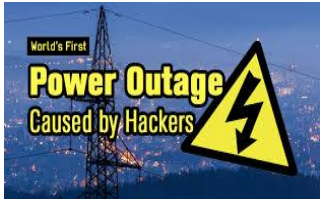
Stanford University, Winter 2015

Risco Cibernético

2010 | 03/16 | 07/17 | 12/17


KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID



O que ?

- Acesso remoto a rede SCADA sem 2FA
- Alteração do Firmware de dispositivos críticos em 16 subestações (conversores Serial-Ethernet para envio de comandos para a rede SCADA)
- Impossibilidade de execução de comandos pelos Operadores das subestações
- Reconfiguração das UPS (Energia de Backup)
- T-DoS – ataque de negação de serviços no SAC/Call Center (excesso de ligações falsas)

Risco Cibernético

2010 | 03/16 | 07/17 | 12/17

Como ?

- Phishing para 3 empresas com Doc. Word malicioso
- Solicitação de habilitação de Macros no Word Doc. (técnica anos 90)
- Infecção com BlackEnergy3 – variante de versões anteriores ocorridas na Europa e EUA
- Uso do KillDisk – limparam os HDs dos computadores dos Operadores e o MBR, impedindo o reboot

Risco Cibernético

2010 | 03/16 | 07/17 | 12/17

Impacto ?

- 60 subestações
- 2 centros de distribuição de energia
- Blackout => 230.000 residências
- Completa recuperação : + 2 Meses

Risco Cibernético

2010 | 03/16 | 07/17 | 12/17

Risco Cibernético

2010 | 03/16 | 07/17 | 12/17

Ataque hacker faz usina ser desativada

18-Dez-2017

Um **ataque hacker fez uma usina ser desativada**. Apesar da infraestrutura dessas instalações já ter sido alvo de cibercriminosos no passado, **é a primeira vez que um ataque hacker força a paralisação das atividades da usina**.

O acontecimento foi relatado pela **empresa de segurança FireEye**, que não detalhou local nem tipo de usina envolvido no ataque. Segundo a Reuters, especialistas acreditam que tenha sido no Oriente Médio, provavelmente na Arábia Saudita.

Avaliação do Risco Cibernético

Estrutura Organizacional e Report Line

Menor Risco

- CISO – Chief Information Security Officer
- Gerente de Segurança da Informação (SI)
- Arquiteto de SI
- Gestor de Incidentes de SI
- Políticas, Processos, Padrões, Controles de SI

Maior Risco

- CIO – Chief Information Officer
- Gerente de Tecnologia da Informação (TI)
- Arquiteto de TI
- Gestor de Incidentes de TI
- Políticas, Processos, Padrões, Controles de TI

Avaliação do Risco Cibernético

Encarregado de Proteção de Dados Pessoais

As atividades do Encarregado consistem em (LGPD, Art. 41)

1. **aceitar reclamações** e comunicações dos Titulares, prestar esclarecimentos e **adotar providências**;

2. receber comunicações da Autoridade Nacional e **adotar providências**;

3. **orientar os funcionários e os contratados** da entidade a respeito das **práticas a serem tomadas em relação à proteção** de dados pessoais; e

4. **executar as demais atribuições determinadas pelo Controlador** ou estabelecidas em normas complementares.

Avaliação do Risco Cibernético

DPO - Data Protection Officer

ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken | About the ICO

For organisations /

Guide to the General Data Protection Regulation (GDPR)

Share | Download options

Search this document

- Introduction
- What's new
- Key definitions
  - What is personal data?
- Principles
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)

Introduction

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

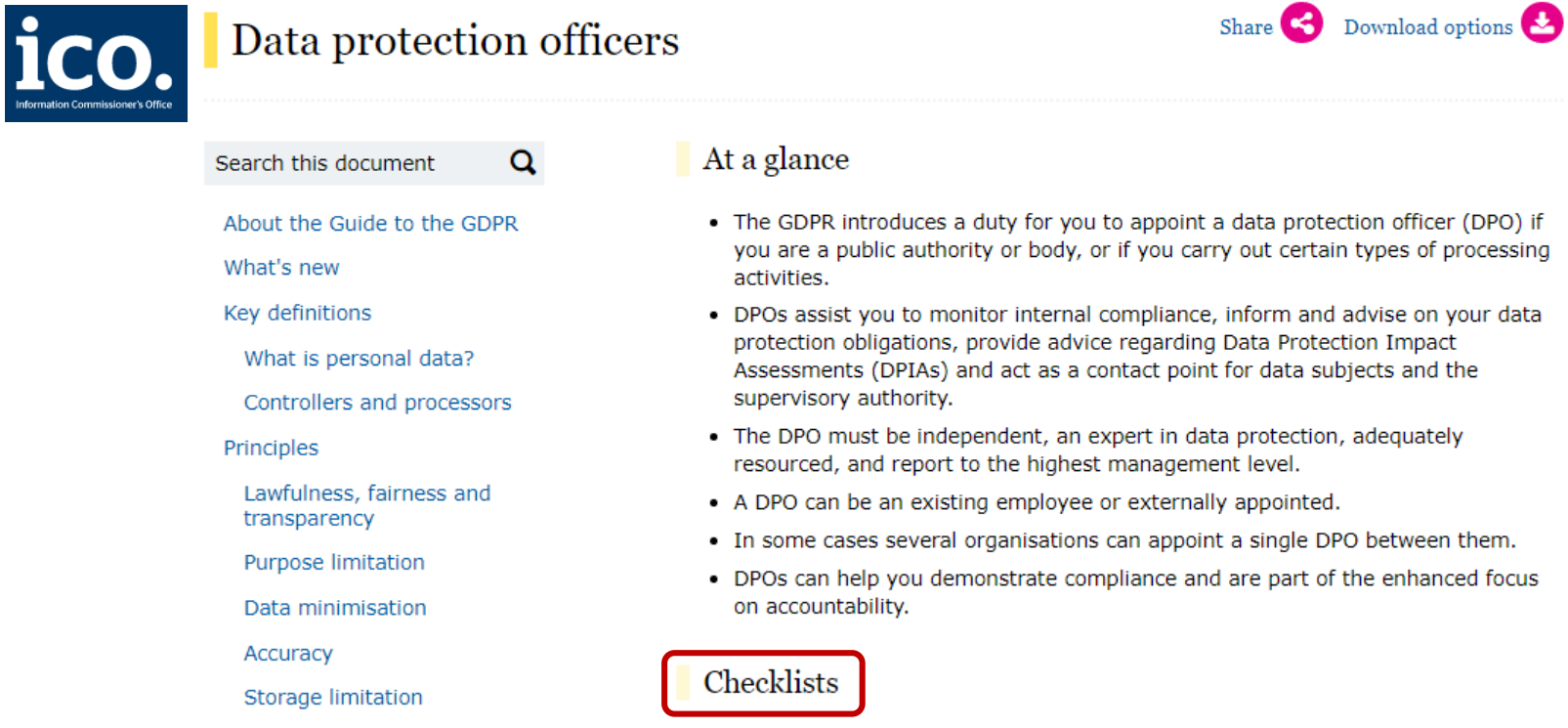
This guide refers to the DPA 2018 where it is relevant includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party - now the European Data Protection Board (EDPB).

We intend the guide to cover the key points that organisations need to know. From now we will continue to develop new guidance and review our resources to take into account what organisations tell us they need. In the longer term we aim to publish more guidance under the umbrella of a new Guide to Data Protection, which will cover the GDPR and DPA 2018, and include law enforcement, the applied GDPR and other relevant provisions.

Further reading

Avaliação do Risco Cibernético

DPO - Data Protection Officer



ico. Information Commissioner's Office

Data protection officers

Share Download options

Search this document

At a glance

- The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.
- DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
- The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.
- A DPO can be an existing employee or externally appointed.
- In some cases several organisations can appoint a single DPO between them.
- DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability.

Checklists

Avaliação do Risco Cibernético

ico. DPO - Checklist

Appointing a DPO

☐ We are a public authority or body and have appointed a DPO (except if we are a court acting in our judicial capacity).

☐ We are not a public authority or body, but we know whether the nature of our processing activities requires the appointment of a DPO.

☐ We have appointed a DPO based on their professional qualities and expert knowledge of data protection law and practices.

☐ We aren't required to appoint a DPO under the GDPR but we have decided to do so voluntarily. We understand that the same duties and responsibilities apply had we been required to appoint a DPO. We support our DPO to the same standards.

Position of the DPO

☐ Our DPO reports directly to our highest level of management and is given the required independence to perform their tasks.

☐ We involve our DPO, in a timely manner, in all issues relating to the protection of personal data.

☐ Our DPO is sufficiently well resourced to be able to perform their tasks.

☐ We do not penalise the DPO for performing their duties.

☐ We ensure that any other tasks or duties we assign our DPO do not result in a conflict of interests with their role as a DPO.

Tasks of the DPO

☐ Our DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.

☐ We will take account of our DPO's advice and the information they provide on our data protection obligations.

☐ When carrying out a DPIA, we seek the advice of our DPO who also monitors the process.

☐ Our DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

☐ When performing their tasks, our DPO has due regard to the risk associated with processing operations, and takes into account the nature, scope, context and purposes of processing.

Accessibility of the DPO

☐ Our DPO is easily accessible as a point of contact for our employees, individuals and the ICO.

☐ We have published the contact details of the DPO and communicated them to the ICO.

Avaliação do Risco Cibernético

Estrutura Organizacional e Report Line

ISACA Now | INFORMATION EXCHANGE
BUSINESS. TECHNOLOGY. VALUE.

As CISOs' Roles Evolve, So Do the Reporting Lines

Michel Lambert, CISA, CISM, CRISC, CGEIT, CISO, Québec Ministry of Agriculture, Fisheries and Food
| Posted at 3:03 PM by ISACA News | Category: Security | Permalink | Email this Post | Comments (1)

Author's note: *This post was inspired by the discussions among CISOs attending ISACA's 2016 CISO Forums, plus additional readings and personal experience. The opinions are my own. For more*

"**The main trend** has been a tendency **to establish a Corporate Information Security** function **outside of the IT organization**." **Gartner**

The CISO will achieve this by ensuring that the information security posture is commensurate with the risk appetite and compliant with industry requirements.

Avaliação do Risco Cibernético

Estrutura Organizacional e Report

What's The Best Reporting Structure for the CISO?

APR 29, 2018 / by Stephanie Overby

As cybersecurity risk management has emerged as a top strategic priority for companies across industries, the question of whom the CISO should report to has likewise risen in importance. Historically, the CISO reported to the CIO, but companies are increasingly considering a number of alternatives—from placing the CISO in the risk or enterprise data groups to having them report directly to the CEO or the board. Although there is no one-size-fits-all answer, we can provide guidance for companies about the pros and cons of the various options.

Estrutura Organizacional – Menor Risco

Certificações	Qtd Prof.

Linkedin - Julho /2018

Brasil

- CGEIT – Certified in the Governance of Enterprise IT
- CISM – Certified Information Security Manager
- CRISC – Certified in Risk & Information Systems Controls
- CISSP – Certified Information Systems Security Professional
- COBIT5 – The Leading Framework for the Governance and Management of Enterprise IT

Avaliação do Risco Cibernético

National Institute of Standards and Technology
U.S. Department of Commerce

Processos Críticos

Gestão de Segurança

da Informação e

Cibernética

Avaliação do Risco Cibernético

ISO	Conteúdo (+40 Normas de SI)
27.000	Visão Geral e Vocabulário de Segurança da Informação (SI)
27.001	Requisitos para um SGSI (“o que tem que ter”, p.e. PSI)
27.002	Controles de SI – Detalhamento e Recomendações (“o que deve conter”, a PSI)
27.003	Guia de Implementação do SGSI
27.004	Medição do SGSI
27.005	Gestão de Riscos de SI
27.006	Requisitos para Realização de Auditoria e Certificação de SGSIs

ISO 29.134 – Proteção de Dados Pessoais

ISO 29.151 – Avaliação de Impacto de Privacidade

Avaliação do Risco Cibernético

ISO 27.000 - 114 Controles de Segurança da Informação		
01	A.05	Política de Segurança da Informação
02	A.06	Organização de SI
03	A.07	Segurança em Recursos Humanos
04	A.08	Gestão de Ativos
05	A.09	Controle de Acesso
06	A.10	Criptografia
07	A.11	Segurança Física do Ambiente
08	A.12	Segurança nas Operações
09	A.13	Segurança nas Comunicações
10	A.14	Aquisição, Desenvolvimento e Manutenção de Sistemas
11	A.15	Relacionamento na Cadeia de Suprimento
12	A.16	Gestão de Incidentes de SI
13	A.17	Aspectos de SI na Gestão da Continuidade do Negócio
14	A.18	Conformidade

Avaliação do Risco Cibernético

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures			
Risk Management Strategy	Maintenance			
	Protective Technology			

NIST National Institute of Standards and Technology
U.S. Department of Commerce

SP 800

https://www.nist.gov/

Series/Number:	NIST Special Publication 800-82
Title:	Guide to Industrial Control Systems (ICS) Security

Mitigação do Risco Cibernético

Avaliação As-Is

- Sistemas de Informação
  - ERP, CRM, SCM, SFA
  - HR, M&S, Departamentais
  - SCADA / PCS / ICS / IACS
- Apps, Mobile, IoT, Cloud
- E-mail, Intranet, Extranet
- EUC – End User Computing
- Infraestrutura, Redes e Telecom
- Treinamento e Conscientização
- Políticas, Processos, Procedimentos, Padrões
- Fornecedores, Outsourcings

Programa Corporativo - SIC

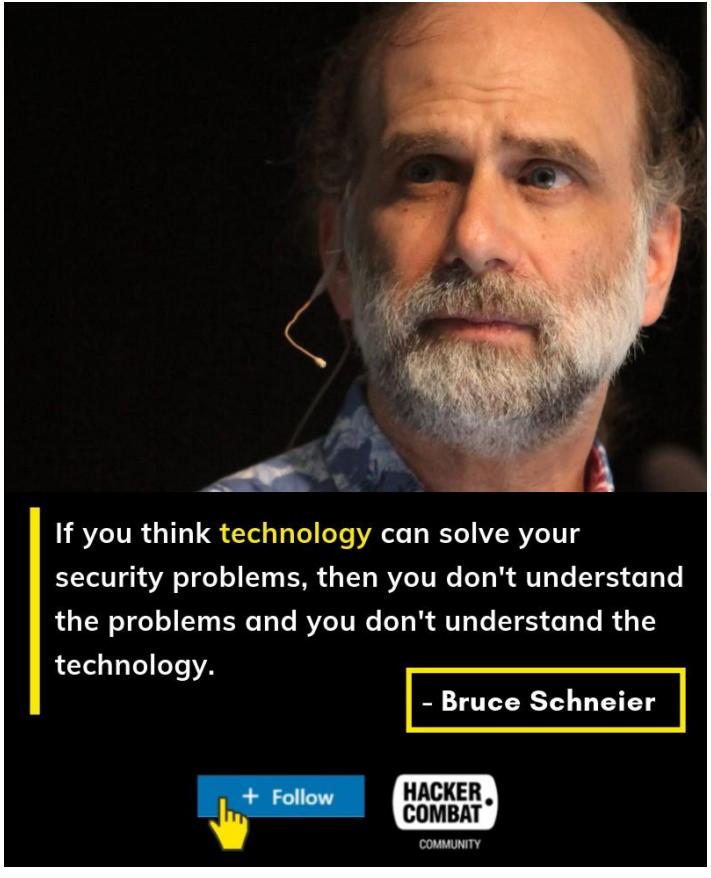
- Melhores Práticas, Padrões e Frameworks
- Pessoas
- Processos
- Tecnologias
- Controles
- Ambientes Interno e Externo
- **Nível Risco Seg. Cibernética**

✓ SIEM
✓ DLP
✓ MDM
✓ UBA
✓ SOC

Risco Cibernético – To-Be

- Sistemas de Informação
  - ERP, CRM, SCM, SFA
  - HR, M&S, Departamentais
  - SCADA / PCS / ICS / IACS
- Apps, Mobile, IoT, Cloud
- E-mail, Intranet, Extranet
- EUC – End User Computing
- Infraestrutura, Redes e Telecom
- Treinamento e Conscientização
- Políticas, Processos, Procedimentos, Padrões
- Fornecedores, Outsourcings

Mitigação do Risco Cibernético => PPT



C-Level Sleeping Positions

Risco Cibernético

Segurança “100%”

Se pensas que sua Empresa 100% Segura está !

Muito de Segurança Cibernética tens ainda que aprender !

Empresas Cyber-Secure Ready, nosso Grande Desafio !

Risco Cibernético - 1520

Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas.

Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota.

Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.

José Fontenelle

https://www.linkedin.com/in/josefontenelle/

20 anos de experiência em Governança, Gestão de Riscos e Compliance (GRC) de Tecnologia, Segurança da Informação e Cibernética, em empresas nacionais e de atuação global, como Furnas, Eletronuclear, Petrobras, Nissan, Vale, Orange Business Services. Condução de +10 projetos internacionais, sendo um global. Implementação de programas de Gerência de Qualidade Total e Reengenharia de Processos Organizacionais.

Diretor Secretário - ISACA-RJ
Gerente Sr - Segurança Cibernética – EY Brasil
Professor - GRC de TI, Segurança da Informação e Cibernética – IBEF-Rio
Professor - Gestão de Riscos Cibernéticos – Escola Nacional de Seguros - Rio
Instrutor - COBIT 5 – ISACA-RJ

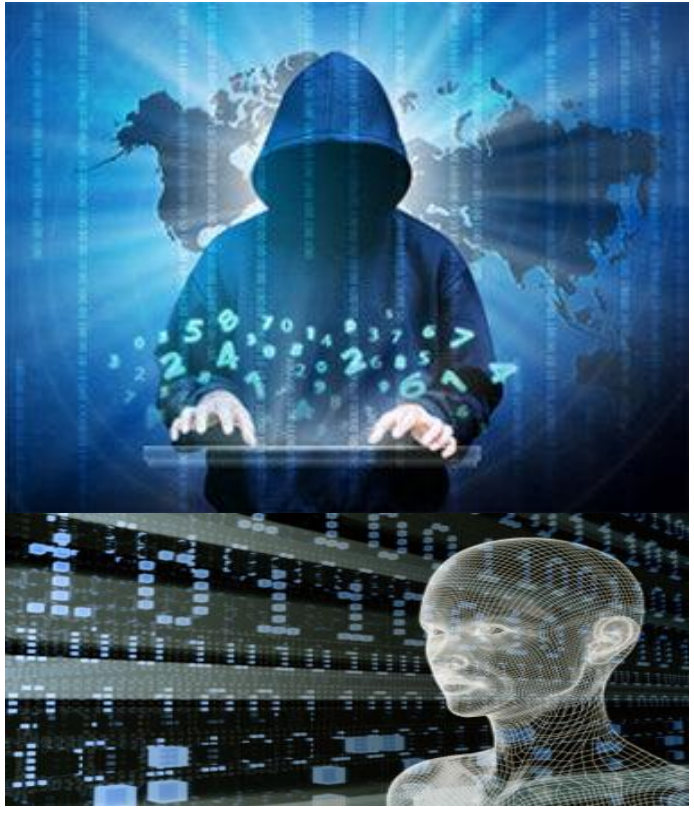
- ✓ Analista de Sistemas – PUC-RJ
- ✓ Engenheiro Eletrônico e de Telecomunicações - UGF-RJ
- ✓ MBAs : Executivo - Coppead/UFRJ
  Gestão Estratégica de TI - NCE/UFRJ
- ✓ Máster em Gerenciamento de Projeto – Projectlab

Certificações :

- ✓ CGEIT – Certified in the Governance of Enterprise IT
- ✓ CISM – Certified Information Security Manager
- ✓ CRISC – Certified in Risk & Information Systems Controls
- ✓ CISSP – Certified Information Systems Security Professional
- ✓ CSX Cyber Security Fundamentals
- ✓ Cobit 5, ITIL V3 Foundations, ITIL Service Manager

Treinamentos em **Advanced Hacking and Incident Response** (2004) e **Segurança Ofensiva de Redes de Computadores** (2017)

Como Avaliar o Risco Cibernético ?



Linkedin

Muito Obrigado !

José Fontenelle

CGEIT, CISM, CRISC, CISSP, CSX, COBIT 5, ITIL V3

Certified in the Governance of Enterprise IT (CGEIT)

Certified Information Security Manager (CISM)

Certified in Risk & Information Systems Controls (CRISC)

Certified Information Systems Security Professional (CISSP)

Cyber Security CSX, ITIL Service Manager

jose.fontenelle@isaca.org.br

21 99999-0095

MARSH

Riscos Cibernéticos

20 de agosto de 2019

Marta Helena Schuh
Líder Riscos Cibernéticos

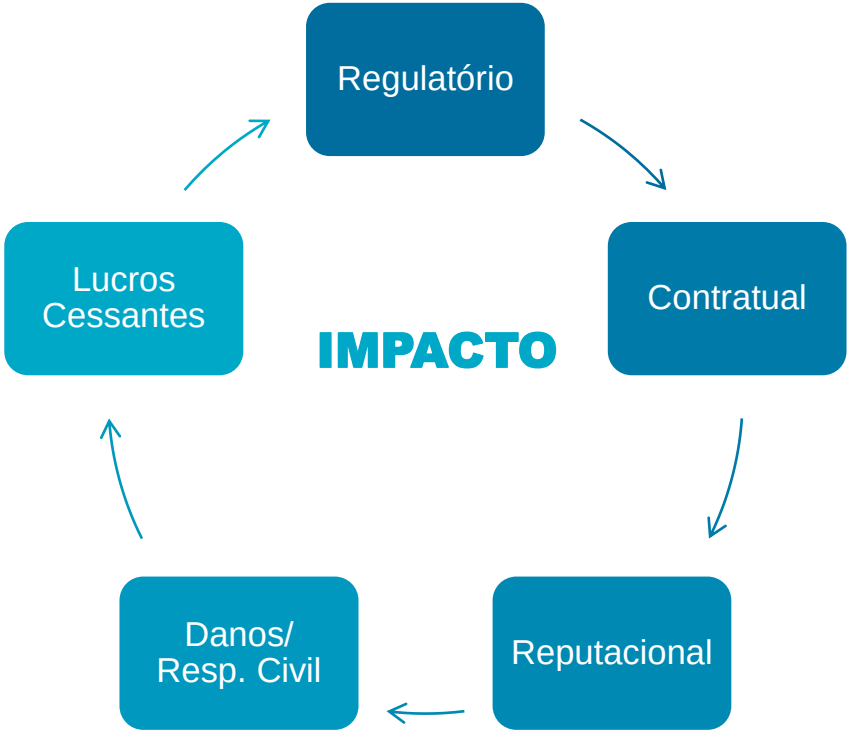
MARSH & McLENNAN COMPANIES

Impactos de um Acidente

O que é um incidente Cyber

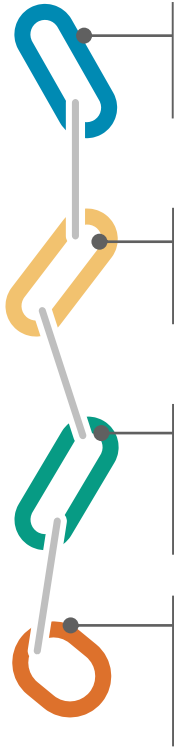
Um evento que ou potencialmente ou totalmente compromete:

- A confidencialidade, integridade ou disponibilidade de informações, banco de dados ou configuração sistêmica operacional; ou
- Os dados que o sistemas processa, armazena ou transmita, ou
- Constitui uma ameaça confirmada ou iminente de violação de segurança, procedimentos de segurança tecnológicas de uma organização.



Nossa crescente dependência de tecnologias digitais integradas e abrangentes também aumenta o impacto dos riscos cibernéticos

Fatores Chaves que aumentam os riscos cibernéticos nas organizações



1. Uso amplo de Tecnologia para Inovação

As empresas estão inovando em um esforço para transformar a experiência do cliente e melhorar a eficiência e eficácia

2. Ataques sofisticados

Assim como a tecnologia evolui, os hackers estão cada vez mais organizados e usam técnicas mais sofisticadas; vetores de ataque estão mudando constantemente

3. Complexidade Tecnológica

A superfície de ataque está aumentando à medida que as empresas engajam com fornecedores e se tornam mais conectadas por meio de tecnologias baseadas em nuvem e arquitetura baseada e integração de TA

4. Data sharing

A interconexão crescente e a velocidade, o volume e a variedade de dados aumentam a vulnerabilidade ao

Cyber Segurança
Uma necessidade para toda empresa

A dependência cibernética cada vez mais complexo faz com que as organizações enfrentem maiores desafios ao equilibrar prioridades

Atores de ameaças aprenderam a contornar a segurança de rede tradicional

- Os ataques cibernéticos são geralmente conduzidos em vários vetores e usando mecanismos diferentes, como vírus, spyware, spear phishing, anexos de e-mail, códigos maliciosos e downloads drive-by; ataques
- A maioria das medidas tradicionais, como software antivírus, firewalls e proteção por senha, não detecta ou bloqueia "ataques de entrada" – não existe ferrramentas 100% efetivas

Novo cenário regulatório

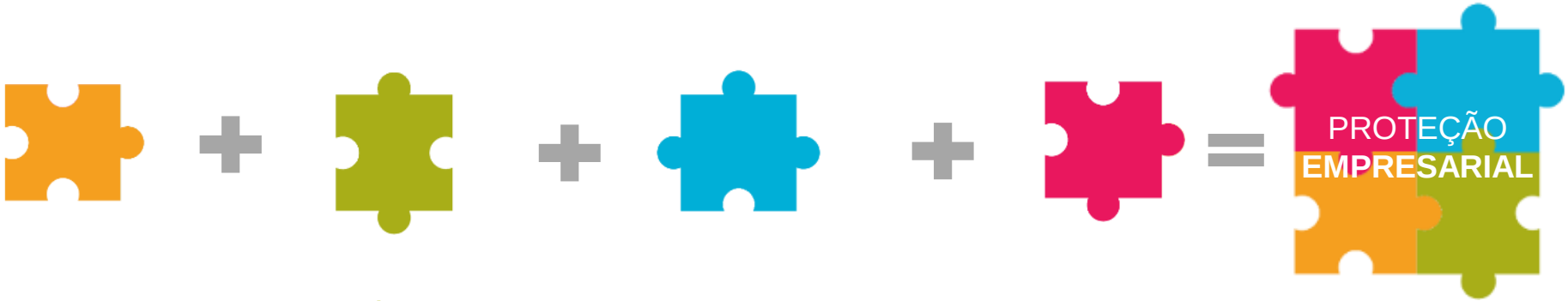
- A digitalização rápida e coleta de dados amplifica as ameaças cibernéticas, o que leva a mais regulamentações e políticas cibernéticas.
- Com os novos regulamentos cibernéticos, as empresas podem se encontrar em um novo cenário em como tratar de incidentes e ações que não estavam anteriormente vislumbradas

Corpo Diretivo da empresa desempenham um papel crucial no gerenciamento de ameaças cibernéticas

- As perspectivas, atitudes, valores, objetivos morais e sistemas legados compartilhados dentro de uma organização têm um impacto direto sobre como as ameaças cibernéticas são percebidas e gerenciadas.
- Para estabelecer uma cultura de resiliência cibernética, todos na organização - de liderança e gestão executiva a área comercial- têm um papel igual e importante a desempenhar na defesa.

Cyber Segurança
Uma necessidade para toda empresa

Nós não queremos que o seguro seja um substituto para a segurança



PROCESSOS
Políticas de Segurança Cibernética
Plano de Resposta a Incidentes
Controles
Segurança Física

PRÁTICAS
Acompanhar novas ameaças
Gerenciamento de Fornecedores
Treinamento
Testes de Segurança

TECNOLOGIA
Segurança de Aplicações
Segurança de Dados
Segurança de Rede
Segurança Operacional
Ferramentas e Sistemas

SEGURO

Coberturas do Seguro Cibernético

Coberturas do Seguro Cibernético

Perda de Receita
Receita perdida durante o período de interrupção de negócios decorrente de um incidente cibernético.

Responsabilidade e Mídia
Planejar, implantar, executar e gerenciar uma campanha de relações públicas para opor-se a ou minimizar eventuais efeitos prejudiciais, reais ou previstos, da publicidade negativa de tal Ato de violação de Privacidade, ou para proteger a reputação comercial do Segurado como forma de reação à publicidade negativa após tal Ato de Violação de Privacidade.

Perda de Ativo de Dados
Custos para recriar, restaurar ou recuperar dados de qualquer tipo, confidenciais ou não, incluindo; restaurar ou comprar novas licenças de software e o custo de investigar sua capacidade de restaurar a partir do backup.

Ramnsonware Sequestro de Dados
Custos relacionados com a investigação e pericia e até mesmo o pagamento do resgate.

Despesas Extras
Despesas extras relacionadas a uma falha do sistema ou um incidente cibernético

Coberturas do Seguro Cibernético

Gerenciamento de Crise
- Pericia Forense.
- Monitoramento de Credito
- Custos de notificação a terceiros
- Consultor de Relações Públicas
- Call Center
- Investigação e resgate de Extorsão/Ransomware

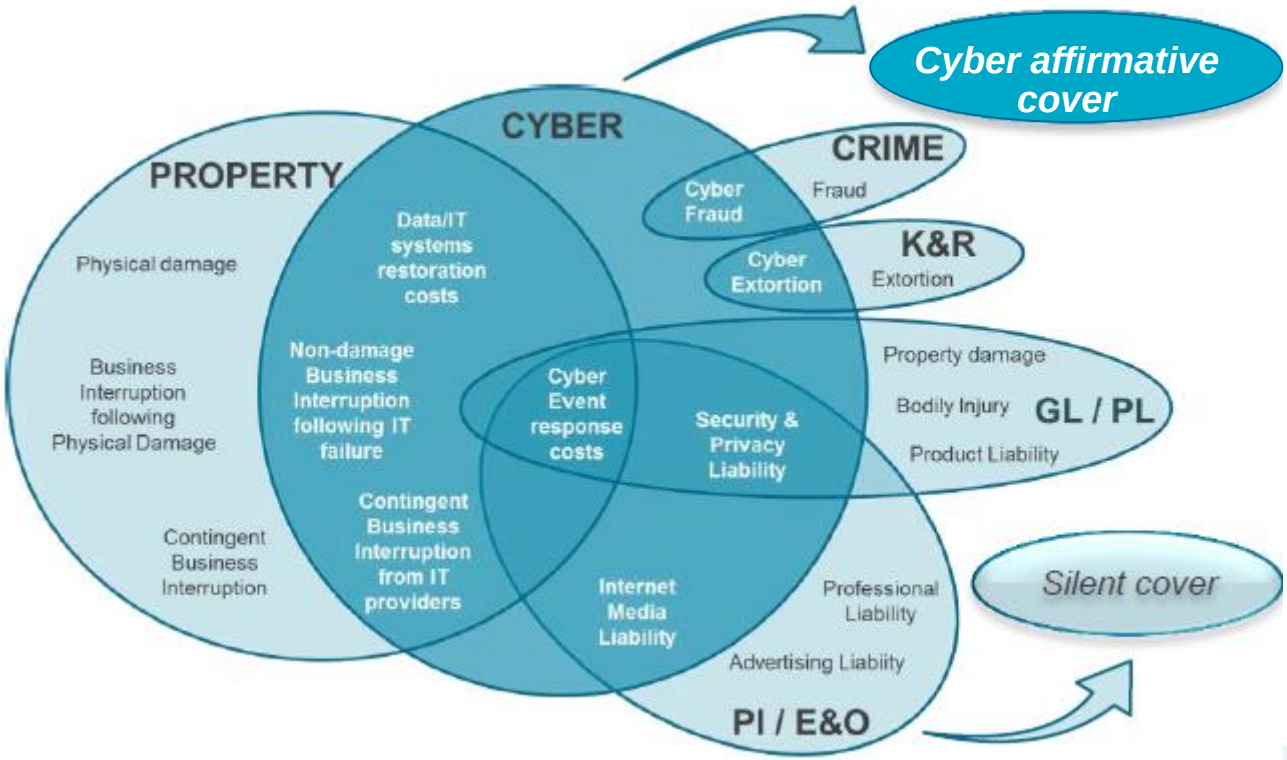
Penalidades Regulatórias
Penalidades cobradas pelos reguladores sob leis de privacidade estaduais ou federais (incluindo leis de privacidade como a Lei Geral de Proteção de Dados que incluirá multas de até 2% do faturamento ou 50 milhões de reais) na medida do direito legal.

Responsabilidade
Danos ou indenizações a terceiros decorrentes de uma violação de privacidade

Custos de Defesa
Custos de defesa contra litígios ou uma investigação ou ação por órgão regulador relacionada a um incidente cibernético.

Exclusões Chave
- Atos Dolosos
- Negligência
- Eventos antes da contratação

Apólice Cyber versus Apólices Tradicionais



Vale a Pena Contratar um Seguro Cyber?

https://www.insuranceage.co.uk/insurer/4136831/cyber-insurance-payout-rates-at-99-claims-abi

INSURER

Cyber insurance payout rates at 99%, claims ABI

Sian Barton

@InsuranceSian

08 Aug 2019

PRICE

Case

Hospital do Câncer de Barretos & Banco Inter

Case
Hospital do Câncer de Barretos

Pagamento do resgate

Despesas emergenciais

Custos com pericia digital

Lucros cessantes

Custos de Perdas de ativos Digitais

Outros Custos:

- Danos a terceiros
- Danos de Imagem

O ataque cibernético que paralisou o hospital foi causado por uma variante do vírus Petya, que em junho infectou computadores com o sistema Windows no mundo todo em troca de "resgates", a serem pagos em moedas digitais - nesse caso, a bitcoin. Chamados de ransomware, vírus de resgate invadem sistemas em que há vulnerabilidades.

Uma vez que rompe as barreiras de proteção, o software malicioso embaralha dados das máquinas infectadas e os criptografa, paralisando os computa e, que fica de poss de um resgate.

No caso do 00 por máquina, o equivalente pital conseguiu e exames foram cancelados e 350 pacientes ficaram sem radioterapia por conta da invasão no dia 27 de junho. Outras unidades do hospital, localizadas em Jales (SP) e Porto Velho (RO), também foram afetadas.

"Trabalhamos em regime de 24 horas, nos revezando, para restabelecer o sistema do hospital. Todo mundo virou técnico, foi um trabalho braçal. O problema mais grave foi o 'sequestro' das máquinas", afirma Douglas Vieira, gerente do departamento de TI da instituição. Em três dias, a equipe conseguiu recuperar 800 dos 1200 computadores da instituição. Mas o atendimento aos pacientes só seria completamente normalizado seis dias depois.

Fonte G1 - 2017

SEGURO APLICABILIDADE DE COBERTURAS

CASE STUDY – BANCO INTER

MPDFT ajuíza ação contra o Banco Inter por vazamento de dados pessoais

A Comissão de Proteção dos Dados Pessoais do Ministério Público do DF e Territórios (MPDFT) ajuizou nesta segunda-feira, 30 de julho, **ação civil pública por danos morais coletivos contra o Banco Inter S/A**. Na ação, **o Ministério Público pede a condenação do banco ao pagamento de R$ 10 milhões**, a título de indenização, em razão de não ter tomado os cuidados necessários para garantir a segurança dos dados pessoais de seus clientes e não clientes. O valor, no caso de condenação, será revertido ao Fundo de Defesa de Direitos Difusos (FDD).

"As tentativas de encobrir o incidente de segurança, promovidas pelo Banco Inter, geraram prejuízos morais e insegurança aos clientes, não clientes, investidores, acionistas, ecossistemas de Fintechs e Startups brasileiros de dados, bem como na confiabilidade da migração dos serviços de processamento, armazenamento e de computação em nuvem das instituições financeiras", ressaltou o coordenador da Comissão, promotor de Justiça Frederico Meinberg.

Custos regulatórios, inclui defesa, procedimentos envolvidos a investigação e algumas seguradoras ofertam cobertura de multa

Cobertura de Gestão de crise/ danos a imagem

Responsabilidade de privacidade. Danos decorrentes de uma violação de dados

Custos de notificação

Cobertura de extorsão e sequestro


CANALTECH

Banco Inter alega sofrer extorsão de hacker com dados de 300 mil clientes

"**Ainda segundo o que o hacker haveria informado ao site, uma tentativa de extorsão** foi feita junto ao Banco Inter, expondo o ocorrido e pedindo como resgate dos dados uma quantia não revelada, em troca da garantia que o vazamento não seria levado ao público. Na hipotética negativa do Banco Inter, John teria optado, então, por trazer o caso à imprensa."

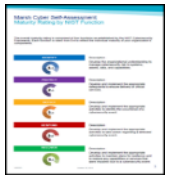
Outros custos não divulgados e que estariam contemplados pela apólice:
- Custos de investigação e pericia digital
- Custos de reconstrução de ativos digitais (sistemas e banco de dados)
- Despesas emergências

Fonte: MPDFT e Terra 2018

Contratação da Apólice

Como avaliar o seu risco?

Avaliação do Risco



Avaliação de controles de segurança - Marsh SelfAcessment Rating

Fornece uma análise de maturidade do programa de segurança cibernética da empresa

- Utiliza elementos-chave de várias estruturas de segurança cibernéticas, incluindo o NIST, ISO 27001 e outras
- Fornecer uma pontuação de segurança da empresa
- Usado no lugar de questionarios padrões de seguradora

Análise do Risco Cibernético

- Usando métodos não invasivos, o Cyence coleta dados sobre indicadores de comprometimento e higiene cibernética geral.
- Fornece feedback sobre vulnerabilidades percebidas.
- Avalia o risco cibernético geral da empresa e fornece uma comparação com empresas semelhantes em seu setor.
- Históricos de violação de dados

Frequency and Severity of Claims

Currency: BRL	Frequency	Severity	Annual Loss		
			1 in 100 Year Loss	1 in 250 Year Loss	1 in 1000 Year Loss
Description:	Probability of a claim happening each year	Average claim amount	A loss equal to or greater than this amount will happen once every 100 years	A loss equal to or greater than this amount will happen once every 250 years	A loss equal to or above above this amount will happen once every 1,000 years
Data Breach (including liability defence, incident response, PCI related liability, and regulatory investigations)	10.76%	18.09M	41.01M	88.73M	226.14M
PCI DSS Non-Compliance Fines	1.25%	2.22M	0.13M	1.17M	5.67M
Cyber Business Interruption	6.07%	1.30M	0.88M	2.55M	10.60M
Cyber Extortion	1.80%	0.01M	0.00M	0.01M	0.05M
Data Asset Loss	4.80%	0.27M	0.29M	0.70M	1.87M
Combined*	17.24%	11.98M	42.63M	91.60M	231.79M

*Combined values are not the summation of the losses above, but a combination of losses that would result in an overall annual average loss.

Estimated Number of Unique PII Records	9,000,000
Economic Sector	Info Tech
Type of Company	Private
Number of Employees	350
Revenue (R$)	1,056,924,884
Profit Margin %	50%
Security Rating	3.5
PCI Data	Yes

Perguntas

Obrigada!

Marta Helena Schuh

Marta_Schuh@jltbrasil.com

+55 11 3156 3975