



# Data Protection Risks in the Health Care Industry

Presenters:

Dirceu Santa Rosa

Erick Pérez

# Data Protection in Latin America

## Background

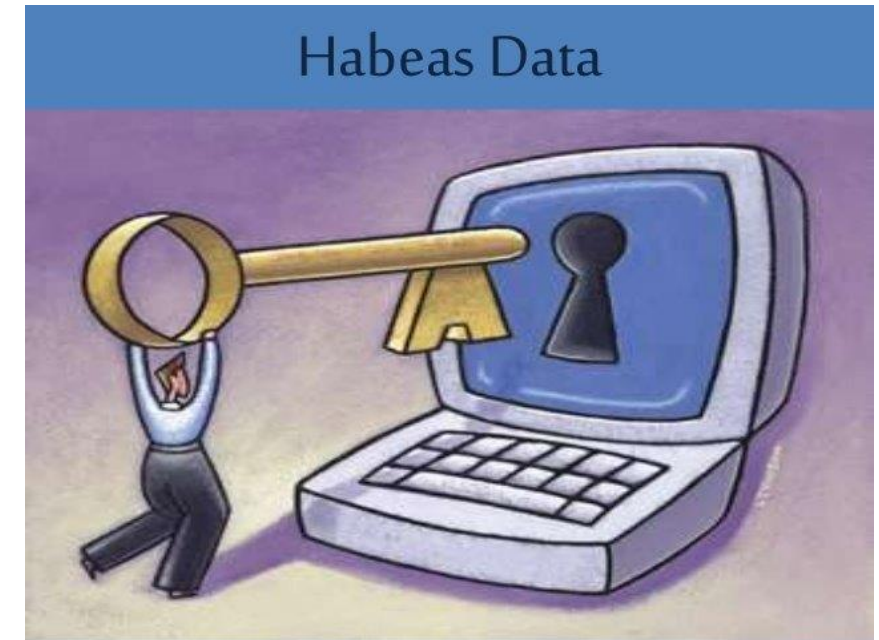
- 1985 first constitutional amendment in Latin America to include data protection was in Guatemala.
- 1987 Nicaragua also included a section in their constitution regarding data protection.

The dangers that have always entailed the compilation and systematization of personal data for individual liberties were strongly increased with the creation of internet.

The right to the protection of personal data, that began to develop autonomously in the European context, begins to be introduced in Latin America through the institution of habeas data, in the 90s.



# Data Protection in Latin America



- The habeas data is a jurisdictional action of the law, usually constitutional, which confirms the right of any individual or legal entity to request and obtain the existing information about their person, and request its removal or correction if it is false or outdated

# Argentina

- Habeas data protection is included in the political constitution.
- Is the only latin american country together with Uruguay to be considered by the European Comission that it offered good data protection control.
- They have an autonomus government entity to control data privacy issues.





# Brasil

- Brazil Federal Senate passed in Mid August a “Data Protection Bill of Law”, it was inspired by the EU General Data Protection Regulation.
- Non compliance with the bill can led to fines to up to two percent of gross sales it will be inforced in 2020.
- Applicable to any public or private organization collecting and processing data in Brazil, the new regulations foresee that organizations would need to inform users when information is collected and delete it after the relationship between the parties has ended - or if the user has not requested to be contacted afterwards.



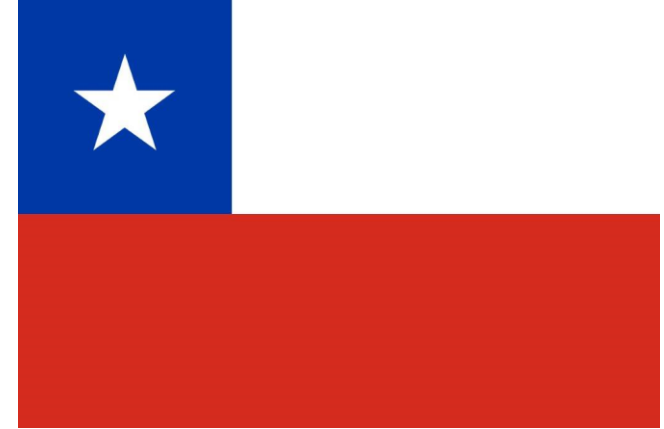
# Mexico

- Mexico habeas data is included in the constitution, and is considered a fundamental right for every citizen.
- Mexico has its own local laws regarding data protection.
- Mexico has its own organism to review data privacy deviations called INAI.
- Mexico was one of the first countries to create an organism in charge of data privacy issues.



# Chile

- June 16, 2018, constitutional amendment to include data privacy rights.
- Entities must obtain a previous and detailed consentment to use personal data of citizens.



# GDPR

- Multinationals that have some form of operations within the EU will be majorly affected by the new General Data Protection Regulation.
- In what will be a major upheaval to many multinationals there will be expanded territorial scope for the new Regulation.





# More risks

- Different Industry experts see dangers in the unrestricted use of data and in possible cybersecurity breaches related to new technologies.
- Cybersecurity and related technologies, are expanding.





# Data Protection Risks on a Health Care Environment

Dirceu Pereira de Santa Rosa

September, 2018

# Today's topics

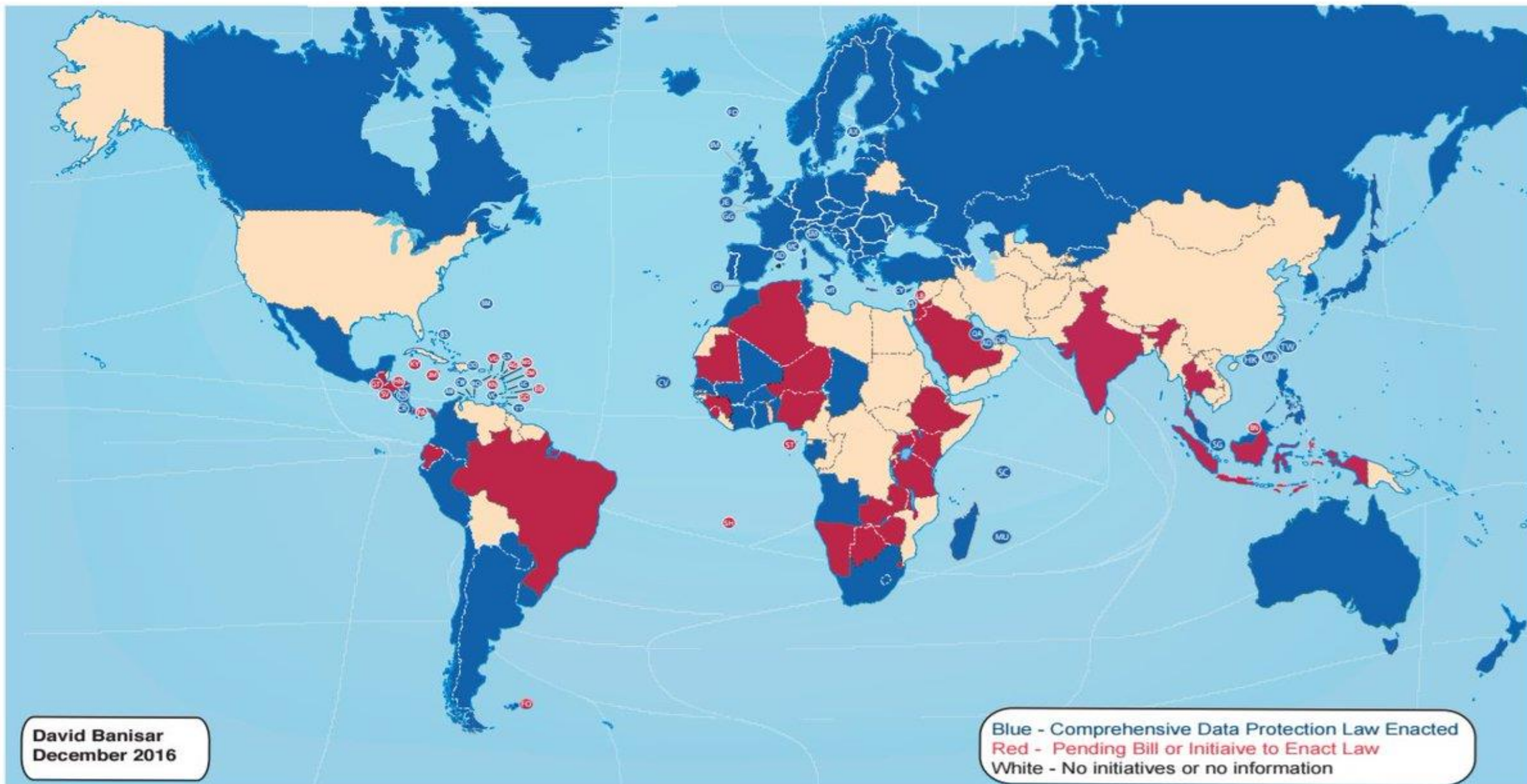
- Brazil's new Data Protection Law ( #LGPD );
- Current Data Security Incidents in Brazil (and some abroad);
- Actual risks, and costs, of a Data Breach incident;
- A Compliance perspective on Data Protection & Health care;
- Building your “game plan”.



## Brazil's Data Protection Law - LGPD



# National Comprehensive Data Protection/Privacy Laws and Bills 2016

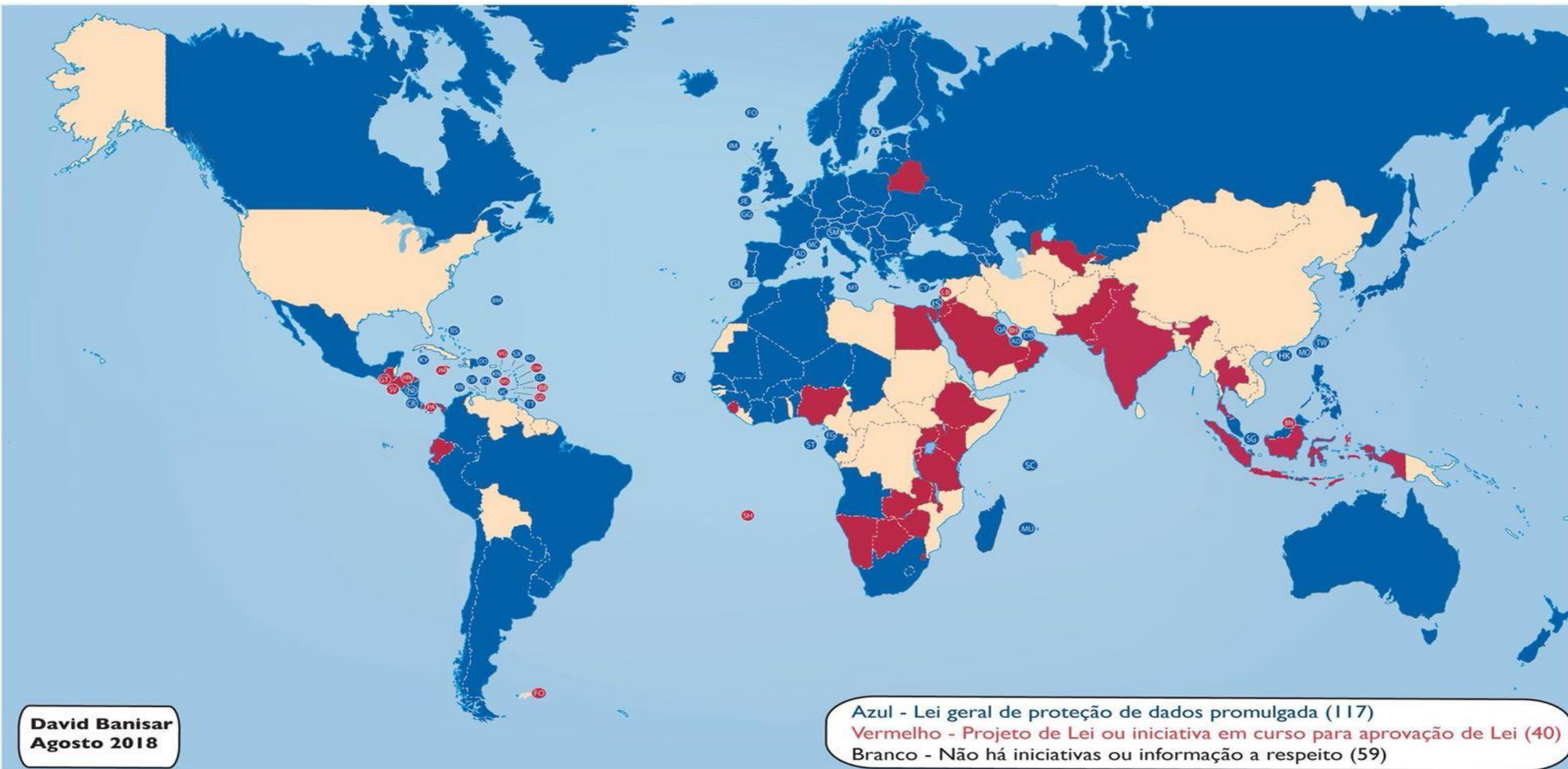








## Leis e Projetos de Lei gerais sobre proteção de dados e privacidade em 2018



# Law 13.709/98 ( LGPD ) on a Nutshell 1/2

- LGPD establishes strict rules on processing personal data, both online and offline, in the private and public sectors;
- Law has extraterritorial scope, such as the GDPR, covering even data collected outside of Brazil ( Art.3o. );
- Significant fines and penalties for non-compliance with the LGPD might reach R\$ 50.000,00 per each incident.



# Law 13.709/98 ( LGPD ) on a Nutshell 2/2

- Allows International data transfers under specific conditions;
- Requires companies to adopt the “Privacy By Design” concept;
- Companies should maintain a DPO, and perform Privacy Impact Assessments regularly; Officer’s duties are similar to the ones in the GDPR, and involve being a focal point for data protection issues with authorities and clients.
- Provides restrictions for collecting sensitive data, **which includes health information**;



LGPD has  
Horizontal  
Scope

# Consent

## I agree



# It is not all about the consent (art.7)

- Compliance with a statutory or regulatory obligation by the controller;
- Execution of public policies;
- Research studies, anonymized whenever possible;
- Performance of agreements to which the data subject is a party, at his/her request;
- Lawsuits, administrative or arbitration proceedings;
- For protection of health, in procedures carried out by health professionals;
- Legitimate interests of the controller or third parties; or
- Credit protection.



## Consent Is:

A “**clear affirmative action**”

**Freely given**

**Specific, informed** and **unambiguous**

**Documented**

**Easily withdrawn**

## Consent Is Not:

Implicitly assumed from pre-ticked boxes, inactivity, or silence

A condition to use a service (unnecessarily)

Asked for with vague or confusing language (no legalese!) or bundled with other terms and conditions

Defensible, if the details are not recorded and accessible (date, time, language)

Hidden (hard to withdraw)

# OPT - OUT

Do you want  
to receive  
additional  
information ?  
Yes (X) No ( )

(X) Please  
send me  
additional  
information.

( ) click here  
if you do not  
want to  
receive  
additional  
information.

# OPT IN

Do you want to  
receive additional  
information about  
our products of  
services ?

- ( ) Yes
- ( ) No



A close-up photograph of a medical professional's hand signing an 'INFORMED CONSENT' form. The form is held by a silver clip on a black clipboard. A stethoscope is visible in the upper right corner, and a portion of a black keyboard is in the upper left. The background is a clean, white surface. The text on the form is in a standard sans-serif font, with the title 'INFORMED CONSENT' in large, bold, black letters. The body of the form consists of several paragraphs of smaller text, which are slightly out of focus. The hand is holding a black pen and is in the process of signing the document.

# INFORMED CONSENT





# Sensitive Personal Data

# Sensitive Data on a Nutshell

- Data relating to racial or ethnical origin, religious beliefs, political opinion, affiliations to trade unions or organizations of a religious, philosophical, or political, **health, sex life, genetical or biometrical data, when linked to an individual.**
- Such data may only be submitted to processing upon specific and **evident** consent of the data subject, for limited purposes (art. 11, I); or under these exceptions:
  - To comply with a legal or regulatory obligation by the controller (art. 11, II, “a”), regularly exercise rights, including in the administrative, judicial, or arbitral spheres (art. 11, II, “d”), or to ensure protection against fraud and security of the data subject (art. 11, II, “g”);
- In case of minors, processing requires specific consent of at least one of the parents or the legal guardian, and the controller must use reasonable technology efforts to confirm that the consent has been obtained properly (art. 14).

# What constitutes Sensitive Data ?

- Health exams;
  - Prescriptions;
  - Hospital files;
  - History of health insurance or HMO usage;
  - DNA and other samples;
  - Fitness device information;
  - Customer data of “health tech”.
- 
- Results of health-based research ??
  - Exchange of information from healthcare plans ??









“Privacy By Design”

## “Privacy by Design” & “Privacy by Default”

- **Privacy by Design** involves embedding privacy measures and privacy enhancing technologies directly into the design of products, services and technologies, involving various organisational and technological components to implement privacy and data protection principles.

It is a Legal obligation for data controllers and processors, in both LGDP and GDPR.

- **Privacy by Default** is a concept adopted by the GDPR, which involves moving a step further into stipulating the protection of personal data (using cryptography, anonymization and pseudonimization, for example) as a default property of any systems and services provided by a corporation.

Wearables powered by IoT

M-Health

01

02

03

04

05

Robotics & Artificial  
body parts

Telemedicine and Remote  
Health monitoring

Artificial Intelligence





HACKERNOON

Follow



Sign in

Get started

HOME

LATEST

DEV

BLOCKCHAIN

PM

CRYPTO TRADING

AI

TECH JOBS



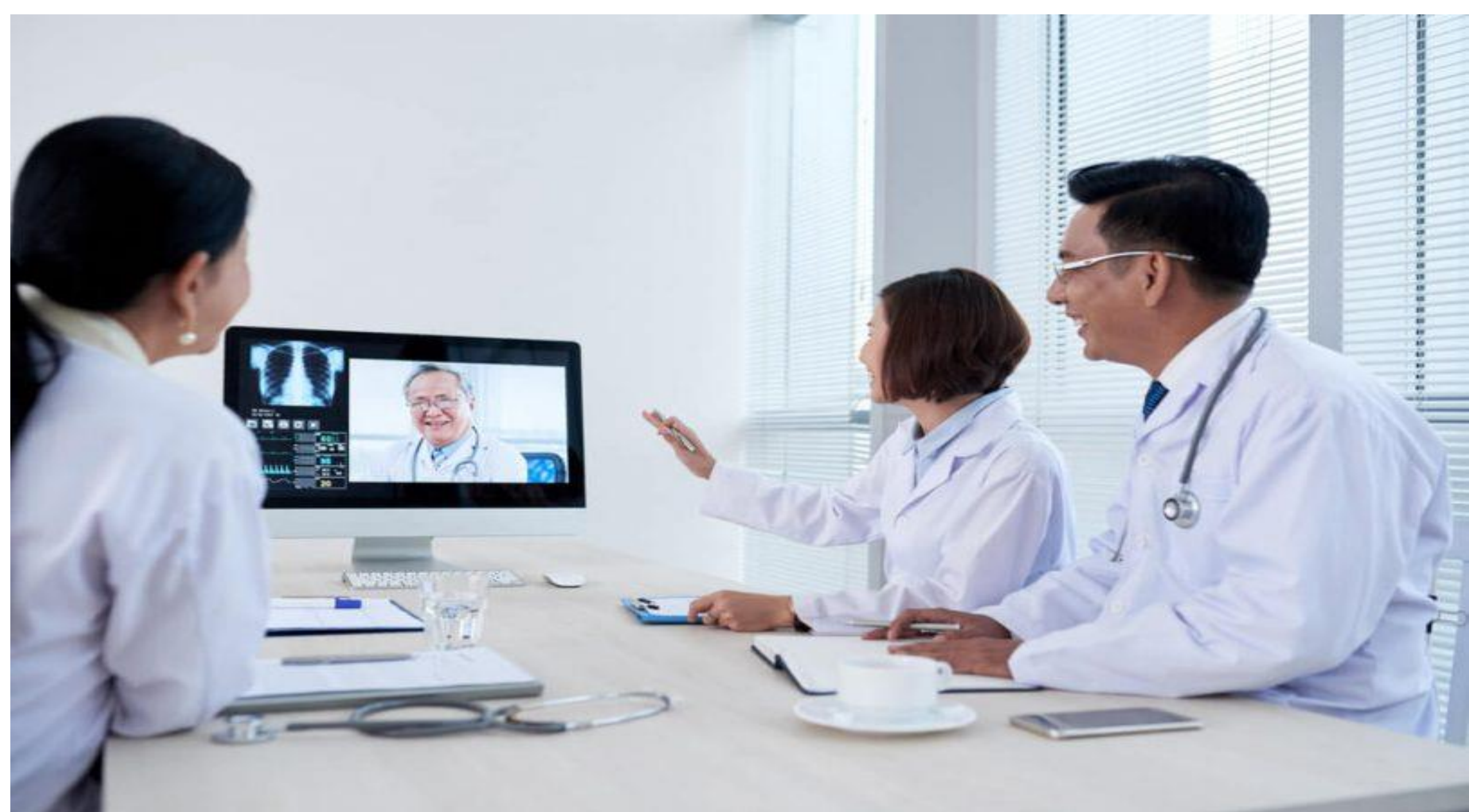
# Privacy, Security Concerns Grow for Wearables



Never miss a story from **Hacker Noon**, when you sign up for Medium. [Learn more](#)

GET UPDATES







# Current Data Breach Incidents



# BA apologises after 380,000 customers hit in cyber attack

Hackers obtained names, street and email addresses, credit card numbers, expiry dates and security codes



Reuters (New Zealand Reseller News)

10 September, 2018 05:30



Distributors | [Aquion](#)

[Comments](#)



FOLLOW US



# Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims

September 11, 2018, Yonathan Klijsma



On September 6th, [British Airways announced it had suffered a breach](#) resulting in the theft of customer data. [In interviews with the BBC](#), the company noted that around 380,000 customers could have been affected and that the stolen information included personal and payment information but not passport information.

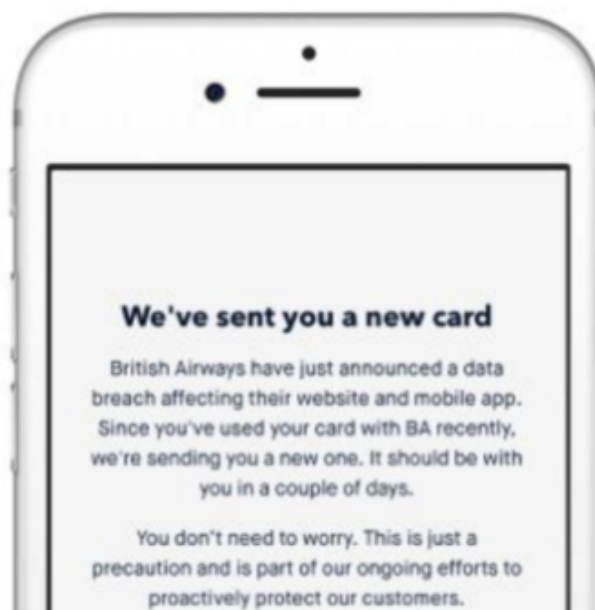
On its website, British Airways placed an article explaining details of the incident that answered as many questions as possible for customers. The technical details were sparse but included the following pieces of information:

- Payments through its main website were affected
- Payments through its mobile app were affected

**Monzo**

@monzo

Last night, we contacted 1,300 customers affected by the British Airways data breach and ordered them new cards as a precaution to protect them from fraud.



### The British Airways data breach: How Monzo responded

Last night British Airways announced that the personal and financial details of their



# Actual Risks in case of a Data Breach

Tarnishment of the company's Market reputation;

Bad media coverage;

Problems with regulators (and other authorities);

Class Action lawsuits or Consumer Lawsuits;

Penalties and limitations to treat data;

Customer backlash;

Stocks lose value;

Financial burden to cover the damages;

Loss of confidential data and trade secrets;

Someone may lose their job / contract.

Breaches come in every shape and form



Grindr

**Support The  
Guardian**

Subscribe

Find a job

Sign in / Register

Search ▾

International edition ▾

**News****Opinion****Sport****Culture****Lifestyle**

More ▾

**The  
Guardian**World UK Science Cities Global development Football **Tech** Business Environment Obituaries**Grindr**

## Grindr shared information about users' HIV status with third parties

Company said sharing data with partners to test and optimise its platform was 'industry practice'

Advertisement

*Staff and agencies*

Tue 3 Apr 2018 05.28 BST



921

This article is over 5 months old





But just because users are comfortable sharing personal information in their profile or chats doesn't mean they want it being shared more broadly.

"Some people's jobs may be in jeopardy if the wrong people find out about their status — or maybe they have difficult family situations," said Chris Taylor of Seattle, who uses Grindr but no longer displays his HIV positive status on his profile. It's "disconcerting," he said, that Grindr is sharing this information with other companies. "It can put people in danger, and it feels like an invasion of privacy."

The disclosure of HIV status also raises questions about the app's [privacy policy](#), which states: "You may also have the option to provide information concerning health characteristics, such as your HIV status or Last Tested Date. Remember that if you choose to include information in your profile, and make your profile public, that information will also become public."

But the average person may not know or understand what they've agreed to in the fine print. Some experts argue that Grindr should be more specific in its user agreements about how it's using their data.

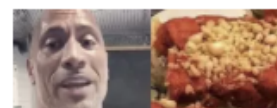
"What the law regards as informed consent is in almost all instances uninformed consent," Ben Wizner, director of the ACLU Speech, Privacy, and Technology Project, told BuzzFeed News.

"I hope that one small silver lining here will be that users and citizens will realize that there are enormous loopholes in the privacy regime," he said, "and that personal information is bought and sold freely on a global market."

#### TRENDING ON BUZZFEED



**23 Delicious Soups You Can Make In A Slow Cooker**



**The Rock Posted His Recent One A.M. "Cheat Meal" And**



[World](#) [UK](#) [Science](#) [Cities](#) [Global development](#) [Football](#) **Tech** [Business](#) [Environment](#) [Obituaries](#)**Opinion**  
Grindr

# Grindr was a safe space for gay men. Its HIV status leak betrayed us

*Brian Moylan*

 @brianjmoylan

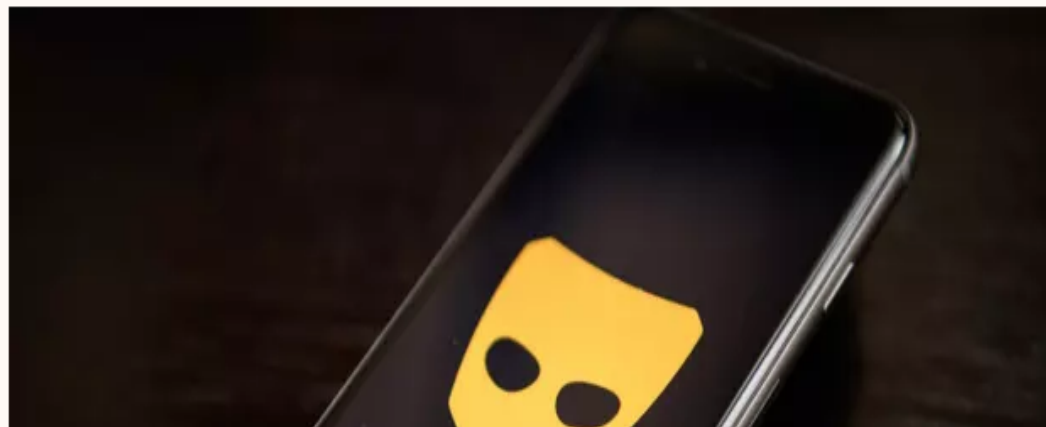
Wed 4 Apr 2018 12.50 BST



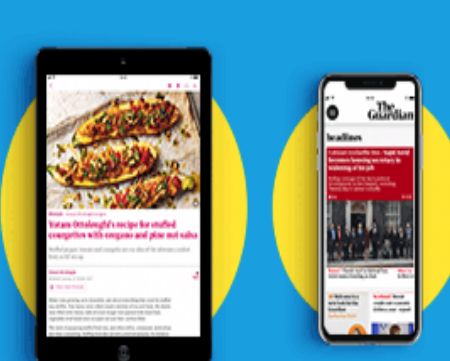
470

314

The app helped revolutionise the community's approach to HIV. Sharing that data undoes all its good work



Advertisement



**Try free for 14 days** ➔

**The Guardian**



# Breaches under LGPD x GDPR

- In case of a security breach involving personal data on the LGPD, the controller should notify authorities **within a reasonable time.** No specific deadline is set, and notifying data subjects may be requested by authorities, after reviewing the breach.
- On the GDPR, a breach must be notified not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. On the GDPR, controller should notify data subjects.



investimentos

***NETSHOES***



**Netshoes** ✓  
@sigaNetshoes



Replying to @sccp1910\_Cicero

Fique tranquilo! Não temos nenhum indício de invasão ao nosso sistema de dados que incluem informações dos nossos clientes. Temos total sigilo por todas as informações que são registradas pelos nossos clientes. E zelamos por isso

4:34 PM - Jan 27, 2018



See Netshoes's other Tweets



**andre** @andresarre · Jan 26, 2018



Certeza que foi a @sigaNetshoes que ferrou meu cartao  
[@nubankbrasil](#) [twitter.com/JornalOGlobo/s...](#)



**Netshoes** ✓  
@sigaNetshoes

Fique tranquilo! Não temos nenhum indício de invasão ao nosso sistema de dados que incluem informações bancárias, de cartões de crédito, ou senhas de acesso. Temos total sigilo por todas as informações que são registradas pelos nossos clientes. E zelamos por isso.

8:51 AM - Jan 29, 2018



1



See Netshoes's other Tweets







# NETSHOES



The online Brazilian retailer known as Netshoes had half a million records compromised from their system posted publicly in December 2017. A media outlet Tecmundo said they had no indications that they had been compromised. However, Netshoes' own systems successfully confirmed the presence of matching identifiers and email addresses from the data set, indicating a high likelihood that the data originated from the company.

**Compromised data:** Dates of birth, Email addresses, Names, Purchases

Sources:

<http://breachlevelindex.com/>

<https://pages.riskbasedsecurity.com/hubfs/Reports>

<https://www.scmagazine.com/>

<https://nakedsecurity.sophos.com>

<https://haveibeenpwned.com/PwnedWebsites>

<http://techgenix.com>

[https://motherboard.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispv-retina-x](https://motherboard.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispv-retina-x)

▼ SEGURANÇA

◀ Voltar para a Home de Segurança

◀ Voltar para a Home do Convergência Digital

# Netshoes, nos EUA, confirma vazamento de dados por ataque hacker no Brasil



Ana Paula Lobo\* ... 27/02/2018 ... Convergência Digital

A Netshoes comunicou à Securities and Exchange Commission (SEC), a CVM norte-americana, que sofreu um ataque cibernético nas operações no Brasil e que houve a divulgação de dados não bancários específicos de alguns clientes.

De acordo ainda com o comunicado da empresa de comércio eletrônico de artigos esportivos, a polícia brasileira está investigando o caso e os clientes atingidos estão sendo notificados sobre o incidente. A expectativa é que todos sejam informados até abril.

“Confirmamos a todos os nossos clientes e partes interessadas que nenhum dado bancário (incluindo senhas e dados de cartão de crédito) de nossos clientes foi comprometido neste incidente”, disse a empresa à Securities and Exchange Commission (SEC), acrescentando que após a conclusão de uma investigação interna, realizada por um especialista independente de segurança cibernética, não houve indícios de que a infraestrutura de TI da empresa tenha sido comprometida.

No Brasil, o **Ministério Público do Distrito Federal e Territórios (MPDFT)** sustentou que esse foi um dos maiores incidentes cibernéticos do País. Foi feita a recomendação, no dia 25 de janeiro, para que a empresa entrasse em contato com todos os clientes afetados. Apesar de não terem sido reveladas informações como cartão de crédito ou senhas, o incidente de segurança, alega o MPDFT, comprometeu dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras. Em comunicado, a **Netshoes não descartou a invasão**, mas sustentou que não houve invasão à área de TI.

\*Com informações da Agência Reuters



CONTEÚDO RETROCEDIDO

**NEC** Orchestrating a brighter world

## Multibiometria: saiba como ela pode cuidar da sua segurança digital

Plataforma Super Resolution, que integra espaços físicos e digitais, será apresentada pela primeira vez no Brasil no Futurecom 2018. Um dos usuários da solução é o OCBC Bank, de Cingapura. A plataforma permite o reconhecimento instantâneo das pessoas à medida que se aproximem da agência.

**Veja todo o conteúdo**

“Opinião”

## Cybersecurity: Cadeado ou Escudo?

Por Mateus Bueno\*

« 1 2 3 4 5 »

10 GB + LIGAÇÕES ILIMITADAS.

EMPRESAS



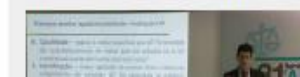
**Apagão de mão de obra exige o uso de robôs na segurança cibernética**



**Fabricantes tornam Internet das Coisas um ambiente sem segurança**



**Defesa nacional fará exercício de guerra cibernética com setores nuclear e financeiro**





# Data Breach Incidents in Healthcare



# Why Health care ?

- Servers usually carries sensitive data or patients personal information;
- Privacy and Data Security is not a priority for investment;
- Medical/ Patient confidentiality is not Technical confidentiality;
- Easier “prey” for extortion or blackmail;
- Patents, Trade Secrets, Reserch Data, Market Data,
- Regulators and authorities are usually harsher.



## Q2, 30% caused by repeat offenders

More than 3 million patient records were breached between April and June, highlighting an even bigger issue: Risk increases over time without proper education or reporting.

By **Jessica Davis** | August 09, 2018 | 04:29 PM



The healthcare sector suffered 142 healthcare data breaches from April through June, impacting 3.14 million patient records – nearly three times the number reported in the first part of the year, according to the latest Protenus Breach Barometer.

### Health 2.0 12<sup>TH</sup> ANNUAL FALL CONFERENCE

Santa Clara Convention Center / CA / September 16 – 18, 2018

Announcing Health 2.0's  
**10 HEALTH TECH  
DISRUPTORS OF 2018**

Hear them live on stage at  
**Launch!**  
this September!



**LEARN MORE!**

**Most Influential**



# The biggest healthcare data breaches of 2018 (so far)

Healthcare continued to be a lucrative target for hackers in 2017 with weaponized ransomware, misconfigured cloud storage buckets and phishing emails dominating the year. In 2018, these threats will continue and cybercriminals will likely get more creative despite better awareness among healthcare organizations at the executive level for the funding needed to protect themselves.

This collection highlights some of the biggest breaches across the industry – and points to some mistakes to avoid in the future.

- Healthcare IT News Staff

## THE ATTACKS

---



# Phishing Attack on Legacy Health Results In Exposure of 38,000 Patients' PHI

[Home](#)[Healthcare Data Privacy](#)[Phishing Attack on Legacy Health Results In Exposure of 38,000 Patients' PHI](#)

Posted By HIPAA Journal on Aug 21, 2018



Share this article on:

[Facebook](#)[Twitter](#)[LinkedIn](#)

## HIPAA Compliance Checklist

Simple Guidelines  
Immediate PDF Download  
Written by HIPAA Journal



**Newsroom**[Search News Releases](#)

## *A Notice to Our Community Regarding a Recent Privacy Incident*

*Posted Aug. 20, 2018*

Legacy Health values the privacy and confidentiality of our patients' information. Regrettably, this notice is regarding an incident that may have involved some of that information.

On June 21, 2018, we learned that an unauthorized third party may have gained access to some employees' email accounts in May, 2018. We immediately began an investigation, including hiring a leading third party forensic firm to assist us. Our investigation determined that some patient information may have been contained in the email accounts, including some patients' name, dates of birth, health insurance information, billing information, medical information regarding care received at Legacy Health and, in some cases, social security numbers and driver's license numbers.

We have no indication that any information has been misused. We began mailing letters to affected individuals on August 20, 2018. Out of an abundance of caution, we are offering credit monitoring to those patients whose social security number was in the affected email accounts. We recommend our patients review any statements they receive related to their healthcare. If they see services they did not authorize, please contact the provider immediately.

We deeply regret any concern or inconvenience this may cause our patients. To help prevent something like this from happening in the future, we are implementing additional access restrictions. Should any of our patients have questions regarding this incident, please call 1-888-277-6762, 6:00 a.m. to 5:00 p.m., Monday through Friday.





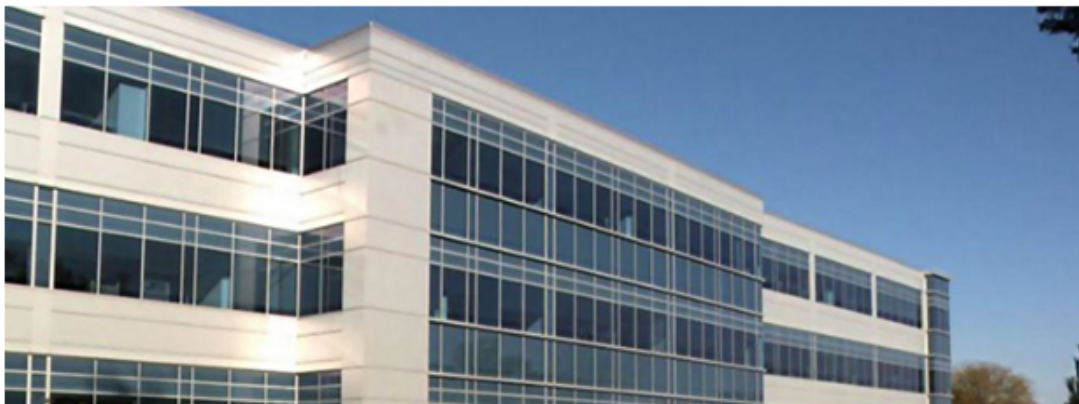
**Himss tv** “We need to *focus* on **people first** when it comes to **cyber security**.”  
- Michael Archuleta, CIO, Mt. San Rafael Hospital

**TUNE IN NOW**

## 5 breaches cost \$3.5 million for national provider in HHS settlement

The first enforcement settlement of the year follows an OCR investigation of Fresenius Medical Care North America that began in 2013, after a string of breaches in its clinics across the U.S. the prior year.

By [Jessica Davis](#) | February 01, 2018 | 02:53 PM



### Health 2.0 12<sup>TH</sup> ANNUAL FALL CONFERENCE

Santa Clara Convention Center / CA / September 16 – 18, 2018

Announcing Health 2.0's  
**10 HEALTH TECH  
DISRUPTORS OF 2018**

Hear them live on stage at  
**Launch!**  
this September!



LEARN MORE

# Five Breaches in 2012 Lead to \$3.5 Million OCR Settlement

February 1, 2018 by Heather Landi

     | [Reprints](#)

Following five separate data breach incidents, Fresenius Medical Care North America (FMCNA) has agreed to pay \$3.5 million to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

FMCNA, based in Waltham, Massachusetts, is a provider of products and services for people with chronic kidney failure with over 60,000 employees that serves over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.


The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced the \$3.5 million settlement, noting that the company failed to heed HIPAA's risk analysis and risk management rules. FMCNA also agreed to adopt a comprehensive corrective action plan. The resolution agreement can be found [here](#).

According to OCR officials, on January 21, 2013, FMCNA filed five separate breach reports for separate incidents occurring between February 23, 2012 and July 18, 2012 implicating the electronic protected health information (ePHI) of five separate FMCNA-owned covered entities.

The five locations of the breaches were Bio-Medical Applications of Florida, Inc. d/b/a Fresenius Medical Care Duval Facility in Jacksonville, Florida (FMC Duval Facility); Bio-Medical Applications of Alabama, Inc. d/b/a Fresenius Medical Care Magnolia Grove in Semmes, Alabama (FMC Magnolia Grove Facility); Renal Dimensions, LLC d/b/a Fresenius Medical Care Ak-Chin in Maricopa, Arizona (FMC Ak-Chin Facility); Fresenius Vascular Care Augusta, LLC (FVC Augusta); and WSKC Dialysis Services, Inc. d/b/a Fresenius Medical Care Blue Island Dialysis (FMC Blue Island Facility).



THE STATE OF NEW JERSEY  
DEPARTMENT OF LAW & PUBLIC SAFETY  
OFFICE OF THE ATTORNEY GENERAL

 Global Navigation

Search



OAG Home

OAG Services from A - Z ▼

Servicios en Español ▼

OAG Contact

News Release

OAG Home

Gurbir S. Grewal  
Attorney General



AG's Executive Leadership Team

AG's Message

Ask the AG

Contact OAG

About OAG

OAG News

OAG FAQs

OAG Library

Employment

OAG Grants

Proposed Rules

OAG History

Services A-Z

Statutes / Regulations / Rules

Agencies / Programs / Units

Other News Pages

Governor's Office

Otras Noticias en Español (OAG)

Civil Rights (Division on)

Consumer Affairs (Division of)

## For Immediate Release:

April 4, 2018

### Office of The Attorney General

- Gurbir S. Grewal, *Attorney General*

### Division of Consumer Affairs

- Sharon M. Joyce, *Acting Director*

### Division of Law

- Michelle Miller, *Director*

## For Further Information:

### Media Inquiries-

Lisa Coryell

609-292-4791

### Citizen Inquiries-

609-984-5828

# Virtua Medical Group Agrees to Pay Nearly \$418,000, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Medical Treatment Files of Patients

[view final consent judgement](#)





We need to *focus* on **people first** when it comes to **cyber security**.

- Michael Archuleta, CIO, Mt. San Rafael Hospital



TUNE IN NOW

## Telemedicine vendor breaches the data of 2.4 million patients in Mexico

A configuration error left a database filled with healthcare data exposed on the internet, and the data could be accessed and changed by anyone without a password.

By [Jessica Davis](#) | August 07, 2018 | 04:28 PM





# Singapore hack affects 1.5 million -- including Prime Minister



By **Joshua Berlinger**, CNN

🕒 Updated 0211 GMT (1011 HKT) July 23, 2018



## News & buzz



Trump's latest boast about the economy isn't even close to...



Cambodia opposition leader Kem Sokha released from prison



## Daily Dashboard



# Crypto-trading platform confirms data breach

 Aug 28, 2018

 Save This

Atlas Quantum, the Brazilian crypto-trading platform, announced it suffered a data breach that exposed the personal details of approximately 261,000 customers, Blockchain Focus reports. Information involved in the breach included the names, email addresses, account balances, and phone numbers of customers. The investment and trading



Our software makes it easy for you to stay GDPR compliant

Get a free demo



Economia

# MP pede que Banco Inter pague R\$ 10 mi por dados vazados de clientes

Ministério Público concluiu que informações de 19.000 correntistas foram comprometidas, entre elas cadastros de conta bancária

Por Da Redação

1 ago 2018, 13h31 - Publicado em 1 ago 2018, 12h41



## Pela web



5 benefícios da portabilidade 100% digital do seu salário

(Banco Original)



Milionários querem banir o passo a passo milionário da jovem

(Negócio em 21 Dias)



Relógio Inteligente com GPS Integrado para acompanhar suas

Tenha um E-mail Personalizado - @SuaEmpresa do Gmail. Teste Já

Garanta Maior Armazenamento e Suporte 24h. Adquira o Gmail Empresarial Agora!  
gsuite.google.com/Gmail\_Email

ABRIR

# Loja da C&A usou dados de candidatos a emprego para bater 'meta de cartão'

POR [FELIPE PAYÃO](#) | @felipepayao - EM [SEGURANÇA](#) - ⌚ 28 AGO 2018 — 11H48



COMPARTILHAR



9

2.731 compartilhamentos







COMISSÃO DE PROTEÇÃO DOS  
DADOS PESSOAIS

Sobre

Legislação

Atuações

Palestras

Comunicação de Incidente de  
Segurança

Vídeos

Contato



COMISSÃO DE  
PROTEÇÃO DOS  
DADOS PESSOAIS  
MPDFT



SOBRE A COMISSÃO

A Comissão de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal e Territórios (MPDFT) é a primeira iniciativa nacional dedicada exclusivamente à proteção dos dados pessoais e da privacidade dos brasileiros.

Foi instituída pela [Portaria Normativa PGJ nº 539, de 12 de abril de 2018.](#)





Possible costs of a data breach





# Examining the 2018 Cost of a Data Breach



Share

## Do you know how much a data breach could cost your organization?

The cost of a data breach differs for every organization. Use the calculator to explore data from the 2018 Cost of a Data Breach study by the Ponemon Institute to see what type of impact one can have on your organization.

Once registered to download the report, you'll be able to uncover the potential cost of a data breach with the same calculator.

Register to explore the data

The 2018 Cost of a Data Breach study explores the implications and effects of a data breach on today's businesses.

Register to download the report



[Return to Cost of a Data Breach overview](#)

Global



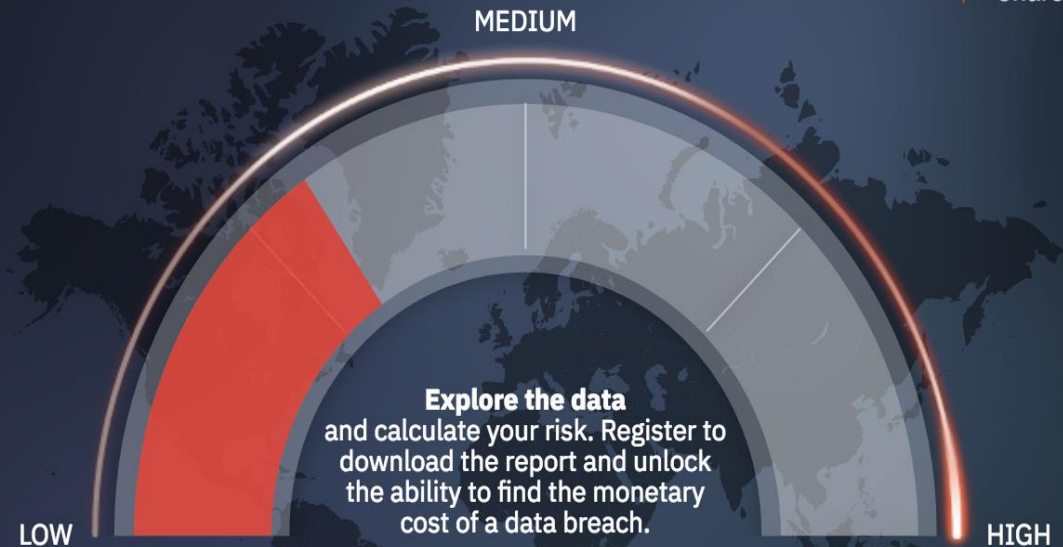
All



Select cost factors



Share



# Average Cost Of A Data Breach Highest In The U.S.

Average total cost of a data breach by country in 2018

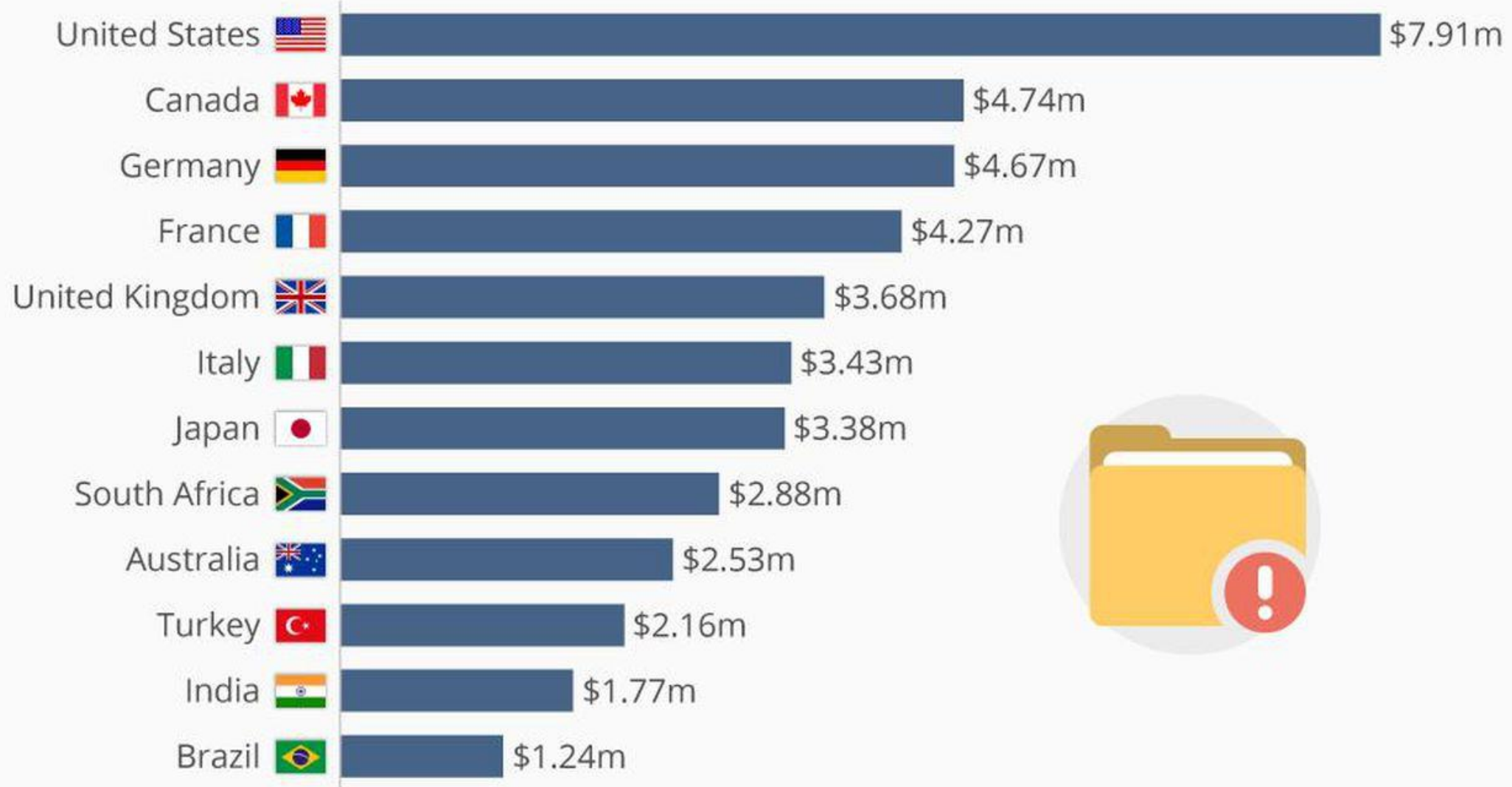






Table 2 provides the percentage cost changes for 11 general cost categories. The two highest costs are lost customer business and investigations & forensics. Since 2013, investigations and forensics has increased by 6 percent and lost customer business has increased by 8 percent.

<b>Table 2. Percentage data breach costs over 5 years</b>	2013	2014	2015	2016	2017
Investigations & forensics	24%	26%	29%	30%	30%
Audit and consulting services	15%	12%	13%	11%	9%
Outbound contact costs	3%	2%	1%	0%	1%
Inbound contact costs	3%	2%	1%	2%	2%
Public relations/communications	3%	3%	2%	1%	0%
Legal services – defense	6%	7%	5%	4%	4%
Legal services – compliance	5%	6%	5%	6%	7%
Free or discounted services	7%	5%	4%	5%	4%
Identity protection services	1%	1%	2%	0%	0%
Lost customer business	25%	27%	29%	31%	33%
Customer acquisition cost	8%	9%	9%	10%	10%
Total	100%	100%	100%	100%	100%

**WHAT DO WE WANT ?**



**PRIVACY PROS**



**HOW DO WE FIND THEM ?**



**???**



Booz | Allen | Hamilton

strategy and technology consultants



# 2017 Global Information Security Workforce Study

## *Benchmarking Workforce Capacity and Response to Cyber Risk*

A Frost & Sullivan Executive Briefing

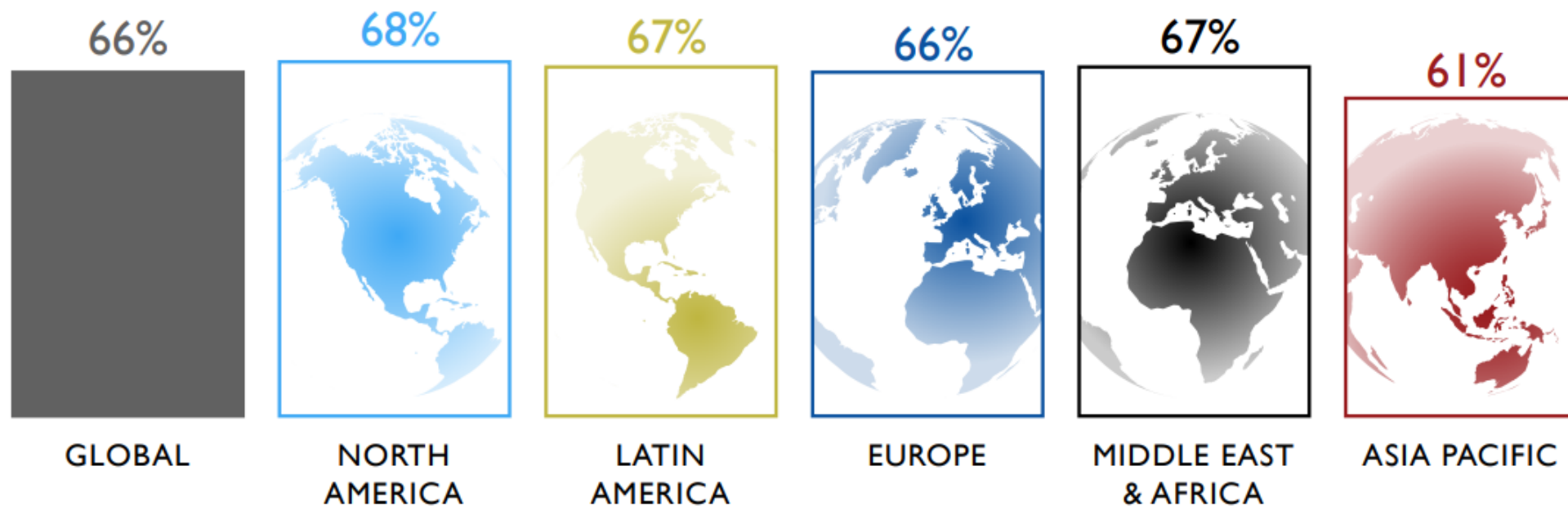




## UNDERSTANDING THE SKILLS GAP

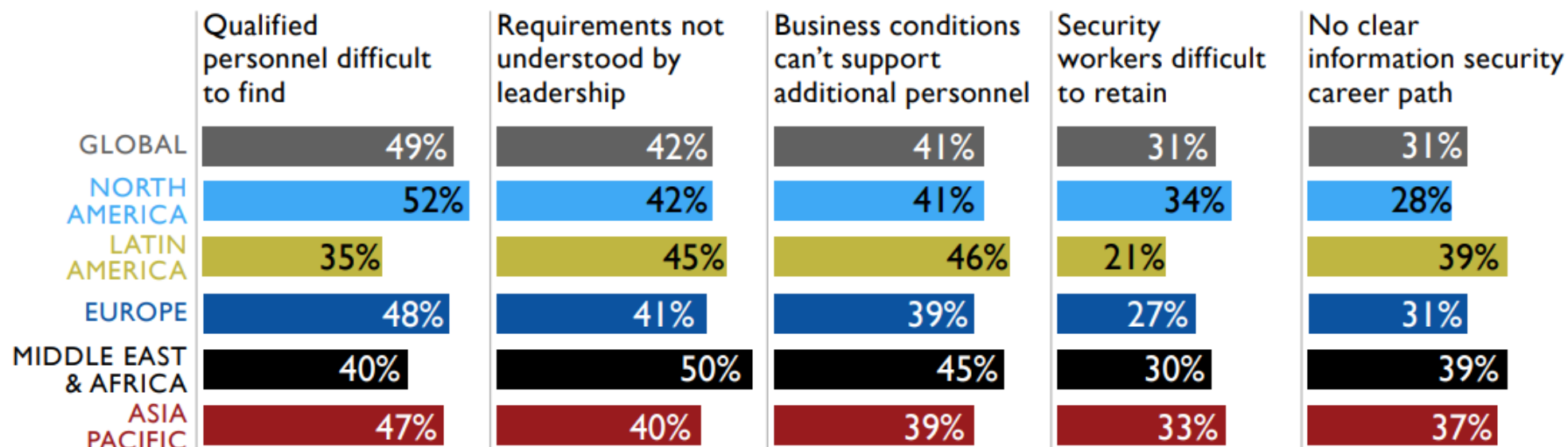
In 2015, Frost & Sullivan forecasted a 1.5 million worker shortage by 2020. In light of recent events and shifting industry dynamics, that forecast has been revised to a 1.8 million worker shortage by 2022. This is reflected by the extraordinarily high number of professionals across the globe who indicate that there are not enough workers in their departments.

Exhibit 3: Too Few Information Security Workers in My Department



Source: 2017 Global Information Security Workforce Study. (n = 19,175)

#### Exhibit 4: Reasons for Worker Shortage by Region

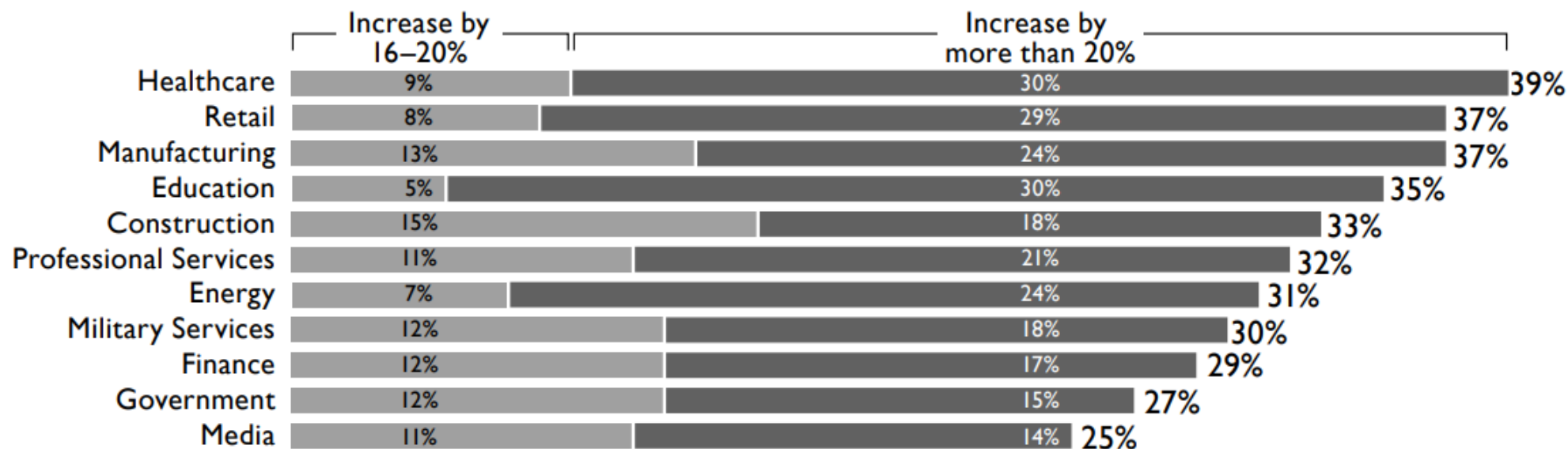


Source: 2017 Global Information Security Workforce Study, (n = 12,709)

#### Hiring is on the Rise

There is good news in an industry that urgently needs to address its worker shortage: globally a third of hiring managers are planning to increase the size of their departments by 15% or more. A great deal of hiring will be concentrated in Europe, where 27% of hiring managers intend to expand their department by 20% or more, and a total of 38% will grow their department by at least 15%. The Middle East, Africa, and APAC can expect lower rates of hiring, however one in four hiring managers in each region still expect to see their departments grow by 15% or more.

### Exhibit 6: Hiring Managers Expecting to Increase Workforce by 15% or More By Industry (Among Managers Expecting to Increase Workforce)



Source: 2017 Global Information Security Workforce Study, (n = 2,906)

Globally, the most sought after positions are Operations & Security Management, with 62% of the workforce indicating that there are too few who occupy this position, followed by Incident & Threat Management and Forensics, at 58% globally. In fact, the latter position is in greater demand in LATAM (63%) and the Middle East & Africa (65%) than any other position.

Despite efforts by managers to increase hiring, historically demand has outpaced supply, and Frost & Sullivan projects that the gap will grow if current trends continue. Nearly 90% of the global workforce is male, a number that remains unchanged, and the majority arrive in information security with a computer science or engineering



## And some of the desired skills include...

- Design, implement, manage and oversee a local privacy program;
- Report incidents and issues to “C-level”, Higher Management or Board;
- Review and revise programs – local, geography or global;
- Ensure employee, independent contractors and third parties are in sync with policy;
- Draft and Manage Privacy materials (notices, policies ).

# Privacy Notice v. Privacy Policy

- Notice – statement directed to data subject (end users, customers, clientes) describing how the organization collects, uses, retains and discloses personal information.

Can be simple and easy to read.

- Policy – Internal document (or set of documents) for users of personal information collected by the organization that define the handling practices of that personal information.

Should be detailed, but clear, and easy to read.

# Layered Privacy Notices

---

Option to lengthy documents;

---

Short top-level with detailed links;

---

The “need to know” is right at front ;

---

Easy to find and at or before the point of collecting any personal information.



# Privacy Notices “must-haves”

Effective Date	Scope	Collected Information	Information Uses and Disclosures
Sensitive information	Choices available	Global variation or other variations (children, exemptions)	Cookies, Adware or Behavioral Advertising
Dispute	Requests	Policy change communication	VALID ACCEPTANCE AND CONSENT

## COOKIE CONSENT

This website uses cookies to improve your browsing experience. To learn more, [click here](#).

agree



## COOKIE CONSENT

This website uses cookies to improve your browsing experience. If you want to benefit from this improved service, please opt-in.

☐ I opt-in to a better browsing experience.

continue

[I don't want an improved experience.](#)



## STATEMENT

### TERMS OF USE

### ARVATO SYSTEMS TERMS & PRIVACY POLICY

### COPYRIGHT COMPLAINT POLICY

### TRADEMARKS & OTHER NOTICES

### END USER LICENSE TERMS FOR AVID SOFTWARE

### PRODUCT WARRANTIES

### PRODUCT SALES TERMS (EMEA)

### PROFESSIONAL SERVICES TERMS AND CONDITIONS

### REPORT PIRACY

### SUBSCRIPTION TERMS AND CONDITIONS

### AVID ADVANTAGE TERMS AND CONDITIONS

### PATENT MARKING

### AVID DNXHD® LIST OF PATENT RIGHTS

### AVID LEARNING CENTRAL

### MANAGING COOKIES

## RIGHTS UNDER THE GDPR

Avid is compliant with the General Data Protection Regulation (GDPR). Under that regulation, you have the right to (a) be informed about Avid's use of your data, (b) to access the data Avid has collected from you, (c) to correct any mistakes in the data Avid has collected, (d) the right to have the data Avid has collected erased, (e) to restrict processing (f) to portability of the information Avid has collected, (g) to object to the collection and processing of information, and (h) to not be profiled. To exercise any of these rights, please contact Avid at [privacy@avid.com](mailto:privacy@avid.com) or via mail at the address below.

## CONTACTING THE WEBSITE

If you have any questions about this privacy statement, the practices of this site, or your dealings with this site, you can contact the Data Privacy Officer at the following address and email:

### **Data Privacy Officer**

Avid Technology, Inc.  
75 Network Drive  
Burlington, MA 01803  
U.S.A  
[privacy@avid.com](mailto:privacy@avid.com)

## NOTICE TO EUROPEAN USERS

Please note that the information you enter on the site or otherwise provide to Avid Technology, or its subsidiaries or divisions, may be transferred outside of the European Economic Area, for purposes of processing, by Avid Technology, Inc. a company located in Burlington, Massachusetts, U.S.A., or its subsidiaries or Avid's subsidiaries or divisions, or authorized partners, located worldwide, in order to provide this site and its services to you. You are advised that the United States uses a sectoral model of privacy protection that relies on a mix of legislation, governmental regulation, and self-regulation. You are further advised that the Council of the European Union has found that this model does not provide "adequate" privacy protections as contemplated by Article 25 of the European Union's Data Directive. (Directive 95/46/EC, 1995 O.J. (L 281) 31)



A Compliance  
perspective



# Privacy Compliance To-dos (possible)

- **Data mapping & discovery.** Start mapping all personal data processed for your store, as well as their life cycle. Knowing exactly where the information is, how it is stored, who has access, whether the data is shared with third parties, in Brazil and abroad, and what are the existing risks should IT need to make any changes.
- **Always work with informed consent.** Whenever data is collected, make sure that users are well aware of that, and provided consent.
- **Manage consent.** Work with IT to build/use a management consent tool that is efficient to your company.

# Privacy Compliance To-dos (possible)

- **Short storage.** Advise to keep the data stored only for the necessary time, and follow all statutory restrictions. If the data processing is no longer required to achieve the purpose for which it was collected, suggest IT to exclude it or tell your processor to do so.
- **Documentation is your best ally.** Document everything you do. From collecting, storing, using and sharing personal data, all must be documented. This documentation should also contain which risk mitigation measures you take, as the LGPD and other authorities establish that, whenever requested, company must present these documents to the regulatory authority.

# Privacy Compliance To-dos (possible)

- **Audit regularly.** DPIAs are great for risk management and help identify and reduce data protection risks.
- Keep an **open channel** with the regulatory authorities in charge;
- **Build (or Know)** your InfoSec / Privacy Program;
- Be **friends** with your DPO / Compliance teams;
- Keep an eye on **Third Party Processors / Service Providers**;
- **Prepare & Train** for Security Incidents.

# Education (why) vs. Training (what)

- Your 15 year old son comes home from school and says he is having sex *education* class tomorrow

OR

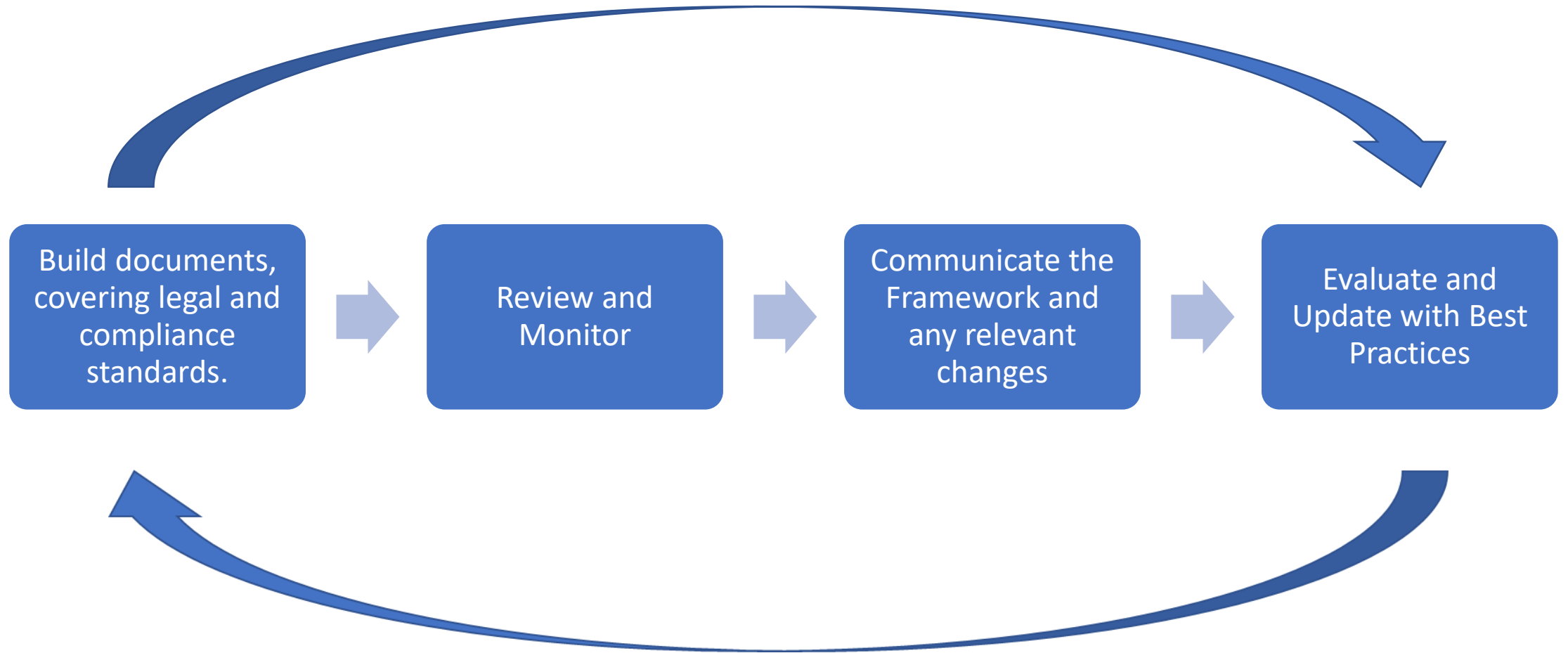
- Your 15 year old son comes home from school and says he is having sex *training* class tomorrow



# Avoiding Risks on Organizational Level

- Create a “Data Protection” mission statement for your company;
- Structure the Data Protection Team;
- Involve Compliance teams to monitor legal compliance factors on local and global Market;
- Develop a Data Protection strategy aligned with business;
- Not “one-size-fits-all”. Ongoing efforts.

# Developing a Data Protection Framework



# Who you need to “talk” to

- Compliance – Interacts for Internal Policy and Enforcement
- Legal – Handle specific issues and tasks.
- HR – Employee records, Talent acquisition, Compensation and Benefits.
- Marketing & Finance – Disaster plans,
- IT – All technical support.
- Third Party Vendors – Making sure policies are in place.
- Outside Authorities – Good relationship with regulators.

# Data breach compliance

- Who has legal liability for any harm associated with collected data ?
- When a breach occurs, who should make the necessary notifications to the public ?
- To notify or not to notify ? 5 factors : nature of the data breached, number of affected individuals, likelihood that the information is accessible and usable, likelihood that breach can be harmful and the organization's ability to mitigate the risk of harm.





Net Income

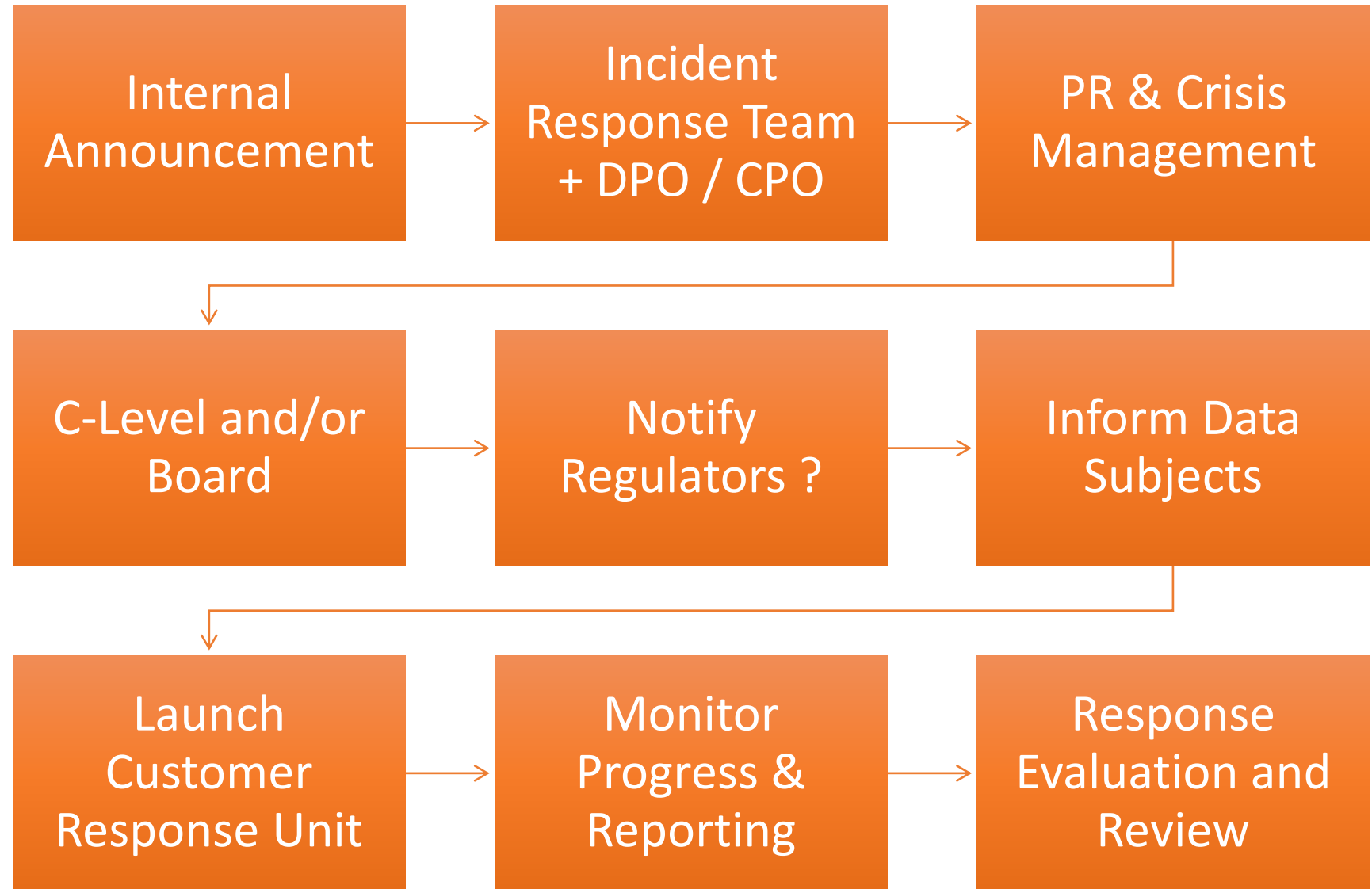
Cost of Recovery

Client Trust

Corporate Reputation

Cyber Breach

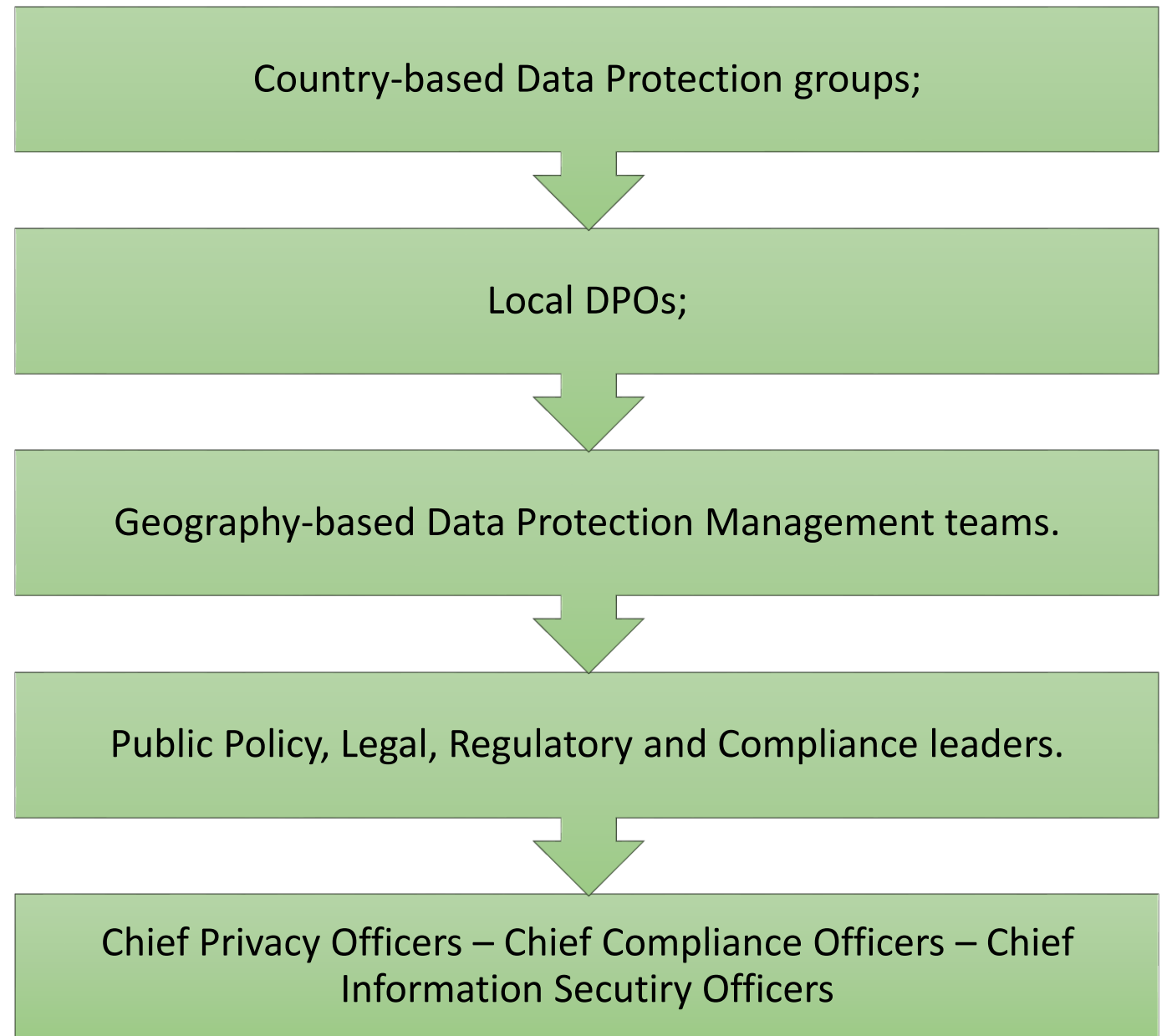
Security



Data Protection is Global. Regional. Local.



# A possible structure







# Minnesota ransomware attack shows the right way to handle breach response

TOPICS: Attack Breach Handle Minnesota Ransomware Right Shows



-15%

MOTO Z3 PLAY  
R\$ 2.199

MOTO Z2 PLAY - POWER  
PACK & DTV EDITION  
R\$ 1.899

FOLLOW ON FACEBOOK

**Jab News**  
28 likes

Connect with friends  
and family today

Like Page

Send Message

Be the first of your friends to like this

FEATURED VIDEO

Sky News - Live

\* Legal

**GO!**

Para: Rio de Janeiro - Ga...  
De: Vitória  
A partir de R\$ 337,47\*

Para: Rio de Janeiro - So...  
De: Vitória  
A partir de R\$ 337,47\*

*Frequently Asked Questions about Associates in Psychiatry & Psychology's  
Security Breach*

**Q: What exactly happened?**

A: Sometime between Friday evening, March 30th and Saturday morning, March 31, 2018, hackers from Eastern Europe, breached APP's servers and did the following:

- Encrypted all the data files on our main servers with an RSA2048 encryption protocol.
- Disabled the system restore function on all affected computers      Reformatted our network storage device where we maintained our local backups.
- Left a ransom note indicating the cost and payment method for restoring our systems.



# Corporate Compliance Insights

THE PREMIER SOURCE OF NEWS FOR TODAY'S GRC PROFESSIONAL

HOME

ARTICLES ▾

ABOUT ▾

NEWS ▾

JOB'S ▾

EVENTS ▾

DOWNLOADS ▾

SUBSCRIBE

PODCASTS

VIDEOS



Home > Featured > **Getting the Board on Board with Cybersecurity**



## Getting The Board On Board With Cybersecurity

Posted on September 6, 2018 by Thomas Kelly



428



0



SITE SEARCH

Search ...



SUBSCRIBE



Free  
eNewsletter:

articles, jobs,  
training & more

Sign Up



# COMPLIANCE





**LGPD**



**COMPLIANCE**



**GDPR**





**COMPLIANCE**

**LGPD**

**GDPR**

# Conclusions

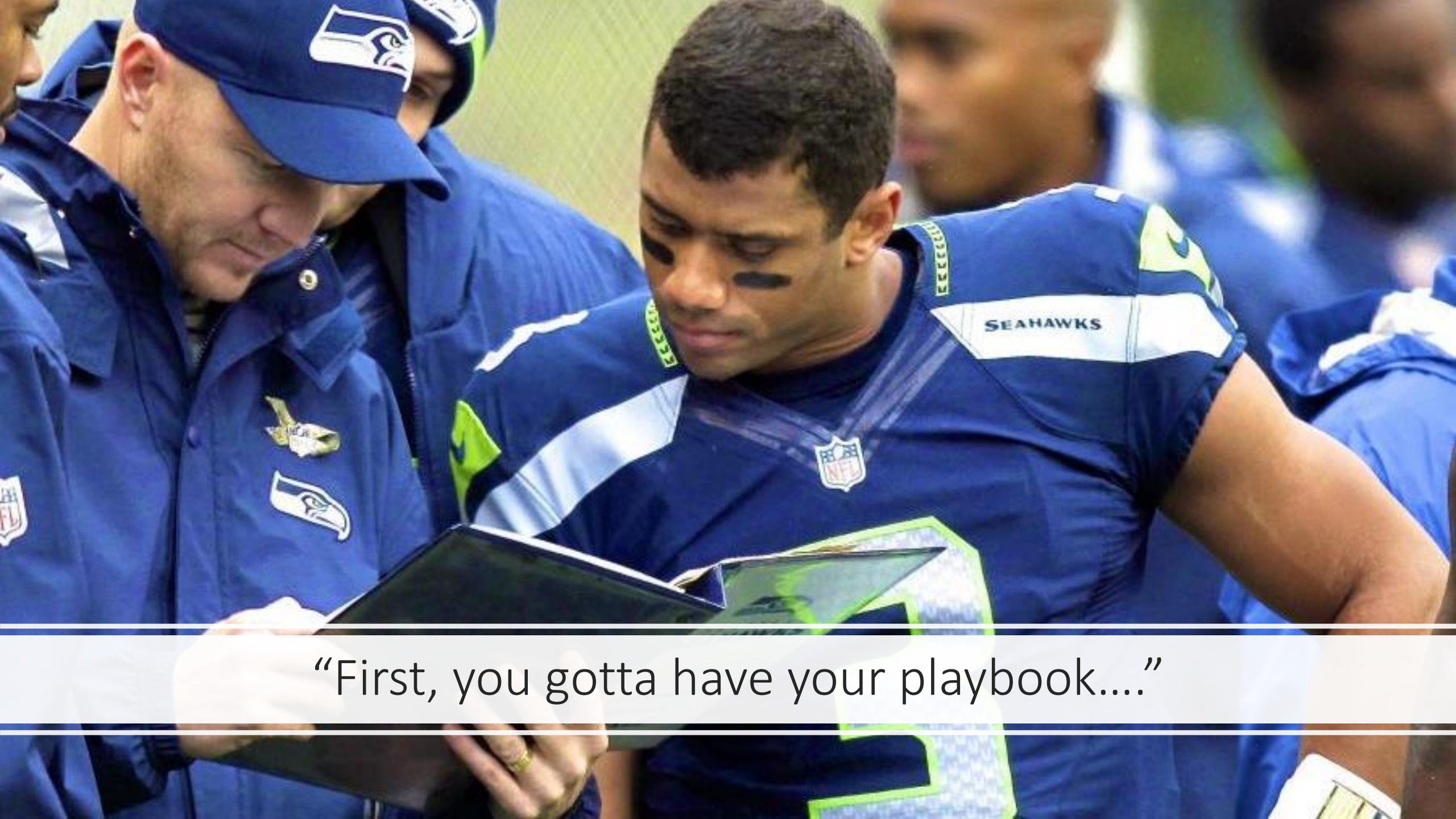




# GAME PLAN







“First, you gotta have your playbook....”





And communicate properly...





Teams must be ready and trained..





To work even in difficult circumstances..





But always working together, as a team..



For the same  
goals and  
milestones.









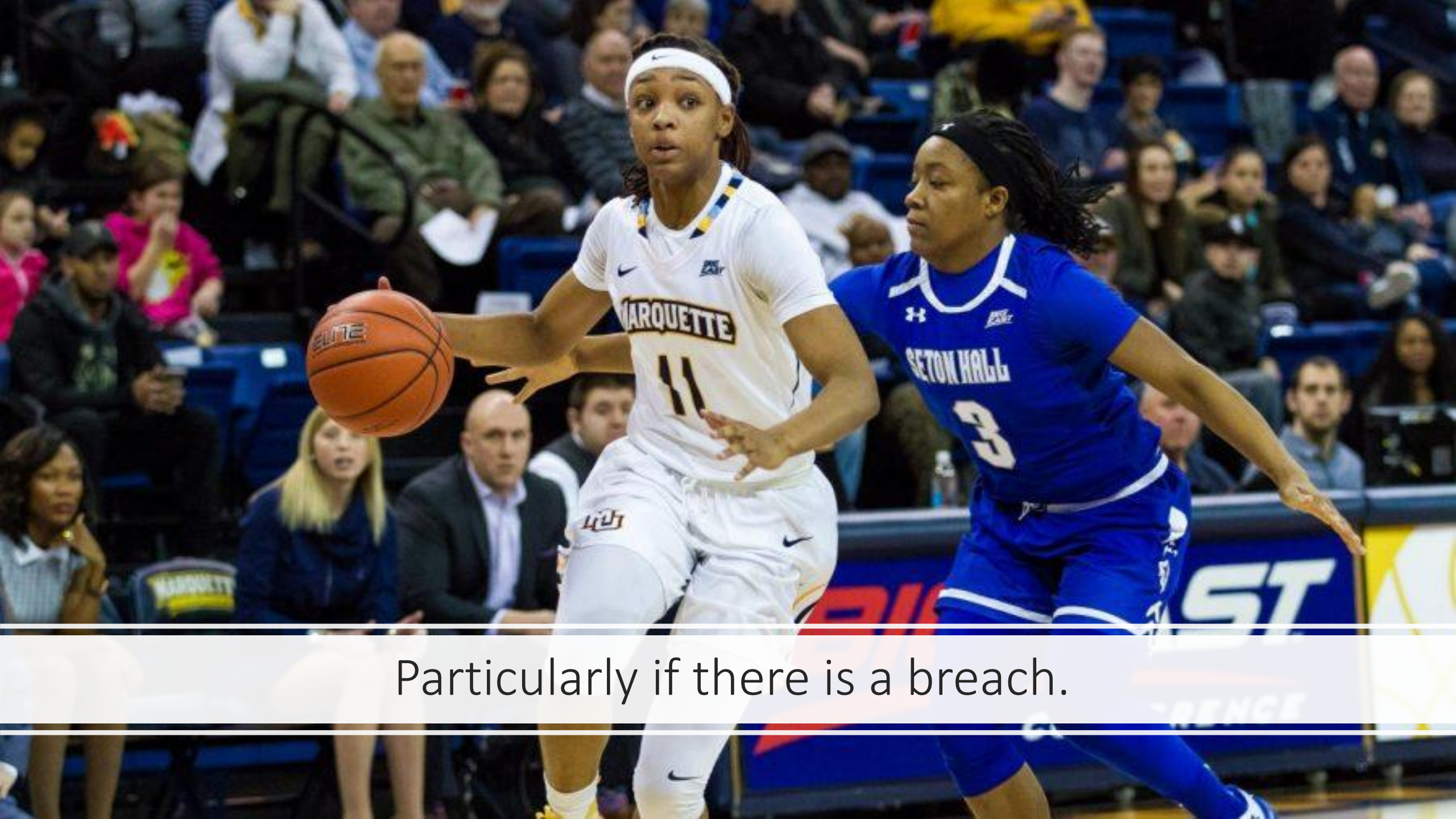
Reason why Internal support is key !!





And learn how to deal with regulators.






Particularly if there is a breach.




# And don't be afraid to use outside counsel SOON ENOUGH

MENU TODAY'S PAPER Newsday LOGIN SUBSCRIBE



**St. Francis Hospital,  
The Heart Center®**  
Catholic Health Services  
At the heart of health





**THE #1 HEART HOSPITAL  
ON LONG ISLAND  
12 YEARS IN A ROW.**

LEARN MORE

SPORTS / COLLEGE / ST JOHNS

## Seton Hall hires law firm to investigate basketball loan allegations, coach says

Seton Hall basketball coach Kevin Willard says the school is "going to be 100 percent open" and "going to be 100 percent honest" in the investigation.





Work hard, educate and prepare relentlessly





Get the tools you need..







And go for the win !





It is a daily effort..



But you can be your company's Data Protection "Champion" !!!





DON'T  
Believe  
THE  
HYPE!





**45 R.P.M.**

**45-2904**

Pub., Bellboy /  
Assorted;  
BMI  
Time: 3:10

VOCAL  
ST-A-24951 SP  
**STEREO**

**I'LL BE AROUND**  
(Thom Bell, Phil Hurtt)  
**THE SPINNERS**

Produced, Arranged and Conducted  
by Thom Bell  
© 1972 Atlantic

MFG. BY ATLANTIC RECORDING CORP., 1841 BROADWAY, N.Y., N.Y.





Montaury Pimenta  
Machado &  
Vieira de Mello  
ADVOGADOS • PROPRIEDADE INTELECTUAL

OBRIGADO!



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



+55 21 2524-0510



[dirceu.rosa@montaury.com.br](mailto:dirceu.rosa@montaury.com.br)



[/montaurypimenta](https://www.linkedin.com/company/montaury-pimenta)

BRASIL

