

Deloitte.



Cyber Scenario in Brazil and Risk of remote work
Eder de Abreu – Deloitte Brazil Cyber Partner

Speaker



- Eder de Abreu is a Cyber Partner at Deloitte Brazil.
- He has 20 years of experience with IT and Information Security, leading several projects throughout his career, including Cyber Maturity Assessments, Development of IT Strategic Plans, Definition of Identity and Access Management Strategy and Architecture, IT Governance Assessment and Implementation, IT Internal Audit, IT Risk Management and Compliance, etc.
- Currently leads the Cyber Intelligence Center in Sao Paulo, Brazil, providing cyber defense services to clients, aiming to rapidly detect and respond to cyber attacks.

Agenda

Cyber Scenario in Brazil

Cyber risks and the remote work

Cyber risks for individuals

Q&A

Cyber Scenario in Brazil

The frequency with which cyberattacks occur in Brazil is one of the largest in the world.



34%

data breaches in the world involve internal actors of companies¹



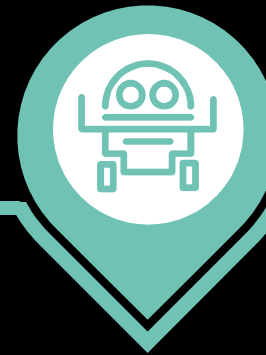
4

of every 10 organizations in Latin America have registered at least one cybersecurity incident²



85 bi

cyberattacks in Latin America occur in one year, with 24 billion in Brazil alone³



\$20bi

is the amount of losses arising from the cyber attacks in Brazil⁴



36%

is the portion of emails containing harmful URLs in Brazil, which leads the ranking in this area⁵

Sources: 1 Varonis Research worldwide "Must-know Cybersecurity Statistics for 2020"; 2 Nd Cyber Search Survey Latam" (Deloitte, 2019); 3 LA Fortinet Report 2019; 4 Senate Agency and Report of the International Telecommunications Union (ITU) "Global Cybersecurity Index", un body (2019); 5 Symantec Worldwide Search "ISTR Internet Security Threat Report | February 2019"

Brazil Overview - Key Facts Around Cybersecurity

Although there is a common sense that Cybersecurity is an important topic to be discussed and addressed globally, in Brazil companies need even more care, since we have a scenario in which the risks associated with cybersecurity are enhanced. Here are some facts:

1. There is only **some recent regulations** associated with Cybersecurity:
 - April 2018 – Central Bank of Brazil established a cybersecurity regulation for financial institutions (4,658) and payment industry (3,909);
 - February 2020 - Brazilian Government establishes the decree **National Cyber Security Strategy** to be implemented in the next 4 years;
 - September 2020 - The **General Data Protection Act (LGPD)**, Brazilian privacy regulations.
 - Other sectors do not have a specific regulation
2. **Brazil** is classified as **#2** in the ranking of **global cybercrime** (behind only China). To illustrate, in the first half of 2020, Brazil had approximately 1.6 billion cyber attacks (16% in Latin America). In addition, 14.2% of all malware in the world emanates from Brazil. (globaltechcouncil.org)
3. More than **a third of all emails** in Brazil contain *Links Harmful*. (Broadcom 2019 Internet Security Report)
4. **Low level of security awareness among users** – many Brazilians have accessed the internet for the first time using their smartphones and, given that, unfortunately, a high percentage of the population has a low level or no education, the chances of an attack being successful are very high.



Brazil Overview - Key Facts Around Cybersecurity

5. According to a survey conducted by FEBRABAN (Brazilian Federation of Banks) and Deloitte, more than **60% of bank transactions in Brazil** are performed using **digital channels**. However, Cybercriminals share newly discovered daily techniques on how to generate credit card data and/or how to commit fraud with slips.
6. Lately, there has been a **increase in the number of cyber attacks** focused on Life Sciences and Health companies, as they control a variety of personal and sensitive information – and with the LGPD, that number is expected to grow further. In addition, small and medium-sized enterprises are expected to suffer more from cyber attacks because they tend to invest less in cybersecurity.
7. **Lack of skilled cyberlabor** (not specific to Brazil) – almost 600,000 workers in Latin America. (ISC2 Cybersecurity workforce study 2019).
8. According to a Deloitte survey* in 2019, we found that:
 - 63% of the companies surveyed invest less than 5% of their IT budget in Cyber. Only 17% invest more than 11%;
 - A third of companies do not have an awareness program in place;
 - 70% of companies do not share threat intelligence information to anticipate cyber attacks;
 - 70% of companies feel they are not prepared to respond to a cyber incident

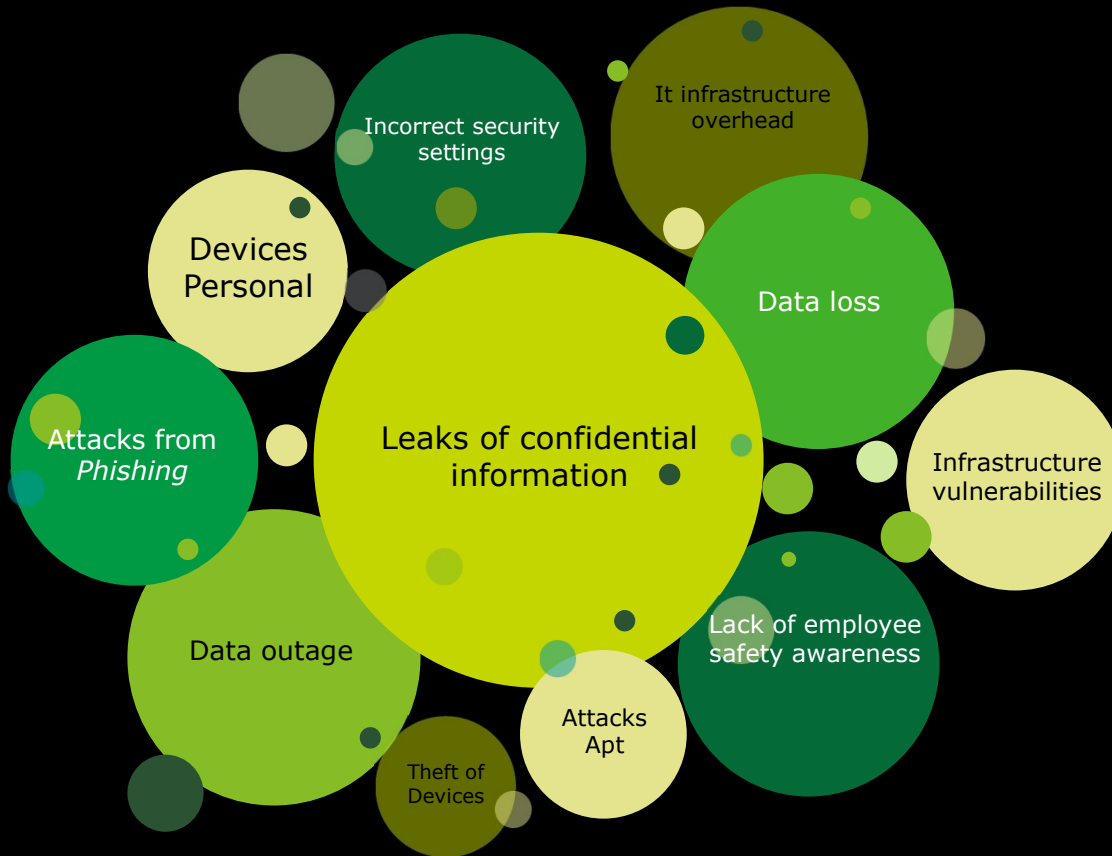


* countries in Latin America and the Caribbean





© 2021. Para mais informações, contate a Deloitte Touche Tohmatsu Limited.

Cyber risks and the remote work

Risks and threats associated with remote access

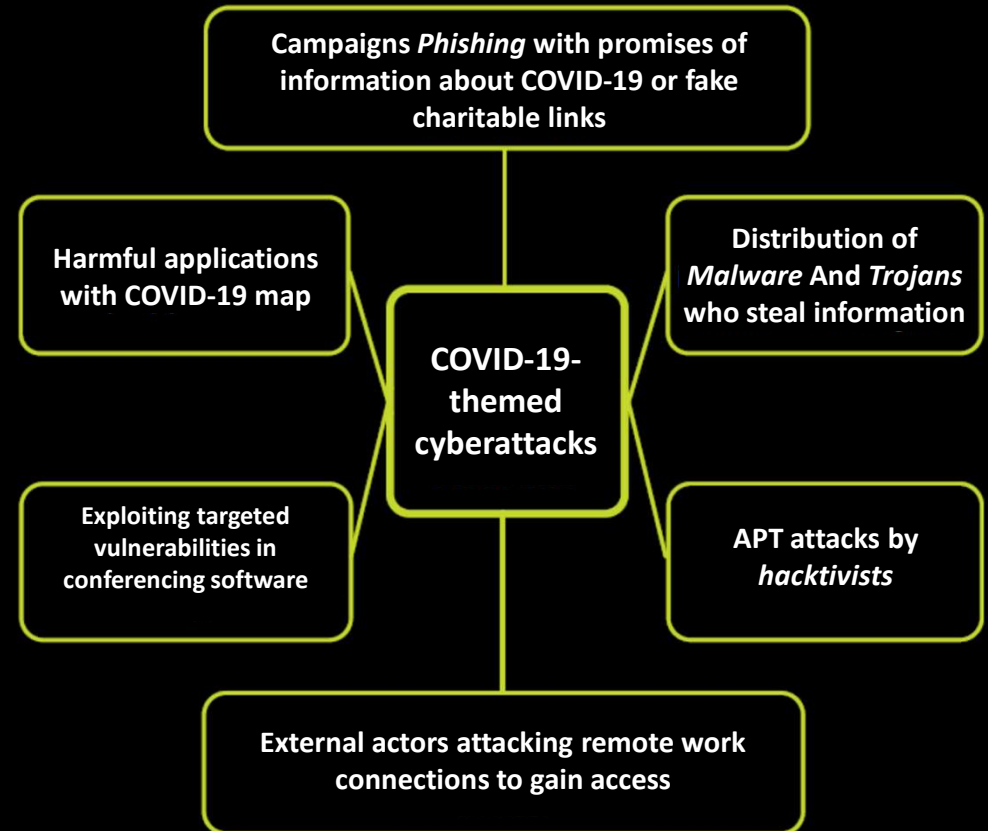


What should be protected?

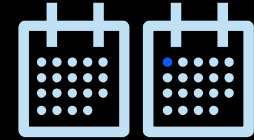
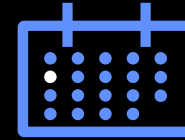
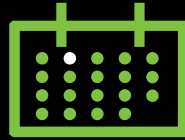
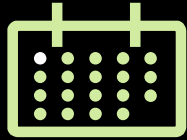
-  User and partner devices
-  IT Infrastructure
-  Channels used for information exchange and sharing
-  Users and their awareness

COVID-19-themed cyberattacks: Incident preparation and response

- Since the COVID-19 outbreak, a sharp increase in the number of attacks of *Phishing* And *Malware* using COVID-19 themes, indicating that threat actors are capitalizing on fear and uncertainty surrounding the global pandemic.
- COVID-19 is becoming a significant factor for social engineering, because the high level of interest in the subject increases the likelihood that receivers will be attracted to harmful bait.
- These attacks may result in loss of company data, trademark or reputation damage, loss of intellectual property and trade secrets, denial of service to external customers, direct financial loss, or fines related to non-compliance with privacy laws.



Priorities for the current moment



Timeline

- Confirm that systems/infrastructure are scalable and remotely accessible
- Ensure that threat/risk assessments are completed before new technologies are taken
- Assess SLAs and chain impacts caused by third-party outage
- Update business continuity plans, including succession plans and essential systems/functions that need to be maintained
- Adopt security best practices for remote work (for example: securely share files, use VPN, keep passwords secure, ensure the security of home and wireless network settings)
- Protect remote access - deploy multi-factor authentication and evaluate the scope of services that can be accessed remotely securely
- Strengthen cyber threat monitoring and response capabilities
 - Integration of cyber intelligence programs with threat monitoring
 - Running periodic scans to identify vulnerabilities and threats
 - Create a plan to ensure uninterrupted 24x7 coverage of monitoring
- Review security monitoring controls
 - Reset traffic/behavior patterns
 - Adjust/develop and deploy new sets of monitoring rules
 - Increase the search and identification of *it shadow*
- Assess the scalability/longevity of security solutions, update *Playbooks* responses to security incidents, and create a post-action report
 - Upgrade security architecture and ensure coverage for internal threats and cyber due diligence
- Improve the capacity of Crisis Management throughout the company to:
 - Perform sensing, monitoring, reporting, fine adjustments in operation
 - Develop strategies for executive response
 - Plan stakeholder engagement, crisis communications and operational response

Cyber risks for individuals

Are individuals subject to cyber attacks?

- As we become more connected than ever to technology, our growing "digital footprint" is bringing new conveniences, new joys and new emotions.
- With these new devices and technology, we are introducing opportunities, but also **increasing the risks in our lives**.
- Executives from large corporations are at greater risk compared to other people, as their information can be accessed more easily. For example:
 - Your personal identities and your own reputation
 - Your public and private agendas
 - Your business and personal travels
 - Your investment accounts and business relationships

Did you know that?

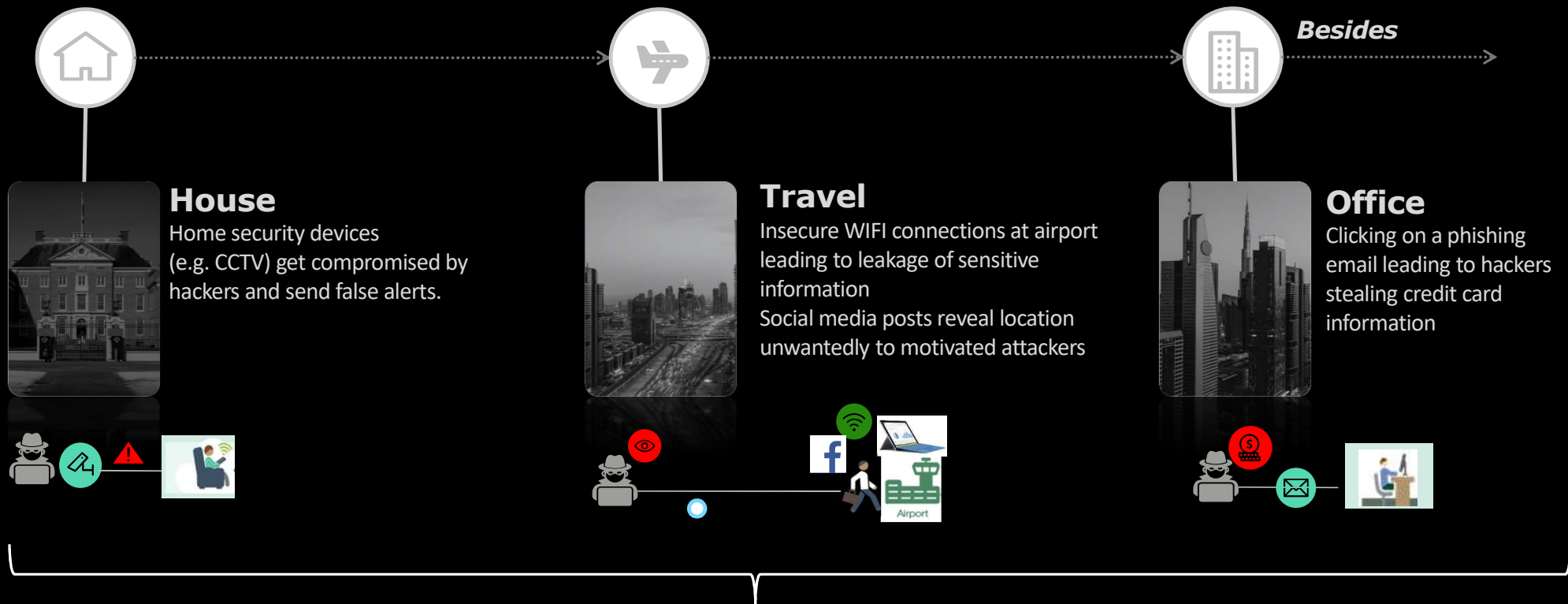


38% of ultra high net worth individuals **don't** have a **cyber security plan**



28% of high net worth international families, family offices and family businesses have experienced a **cyber attack** in the past.

Are individuals subject to cyber attacks?



As you pass through each day you are constantly presented with new points of vulnerability and potential opportunities for your cyber footprint to be used against you

Executive Cyber Security Protection Program

Case Study (Small Office)

For this case study, the Small Office had requested support to provide a view of the current state of their social media footprint and what exists in the public and dark web realm that is associated with their name and reputation:



Social media exposure

Postings of Family Office members' subscriptions and passwords via social media such as Facebook and twitter either inadvertently or for malignant purposes. Sources: Google, Facebook, twitter, Orkut and blog sites.



Sensitive data postings

Postings of sensitive data on the internet on blogs or forums either inadvertently or for malignant purposes.



Data leakage

Unauthorized release of client data and information by internal Family Office employees.



Email and contact harvesting

Corporate email accounts and other contact information available over the internet can be used for spear phishing attacks.



Harmful software and activity

BOT activity from the office's network. Phishing and publicly released vulnerabilities that provide unauthorized monitoring of activities



This case study proved the complex and very tangible components that make up each HNWI's brand and how vulnerable they are during day-to-day activities if left unattended.



Questions



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on [Facebook](#), [LinkedIn](#), or [Twitter](#).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021. For information, contact Deloitte Touche Tohmatsu Limited.

© 2021. Para mais informações, contate a Deloitte Touche Tohmatsu Limited.