

Cyber Security / Latin America

Key cybersecurity threats and opportunities in Latin America

A financial sector perspective

André Salgado (CISA, CISSP, CRISC)



Why attack a bank?

Because it
is where the
money is.

Willie Sutton (1901 – 1980)

In a cyber-world, it is also because

INFORMATION IS



POWER

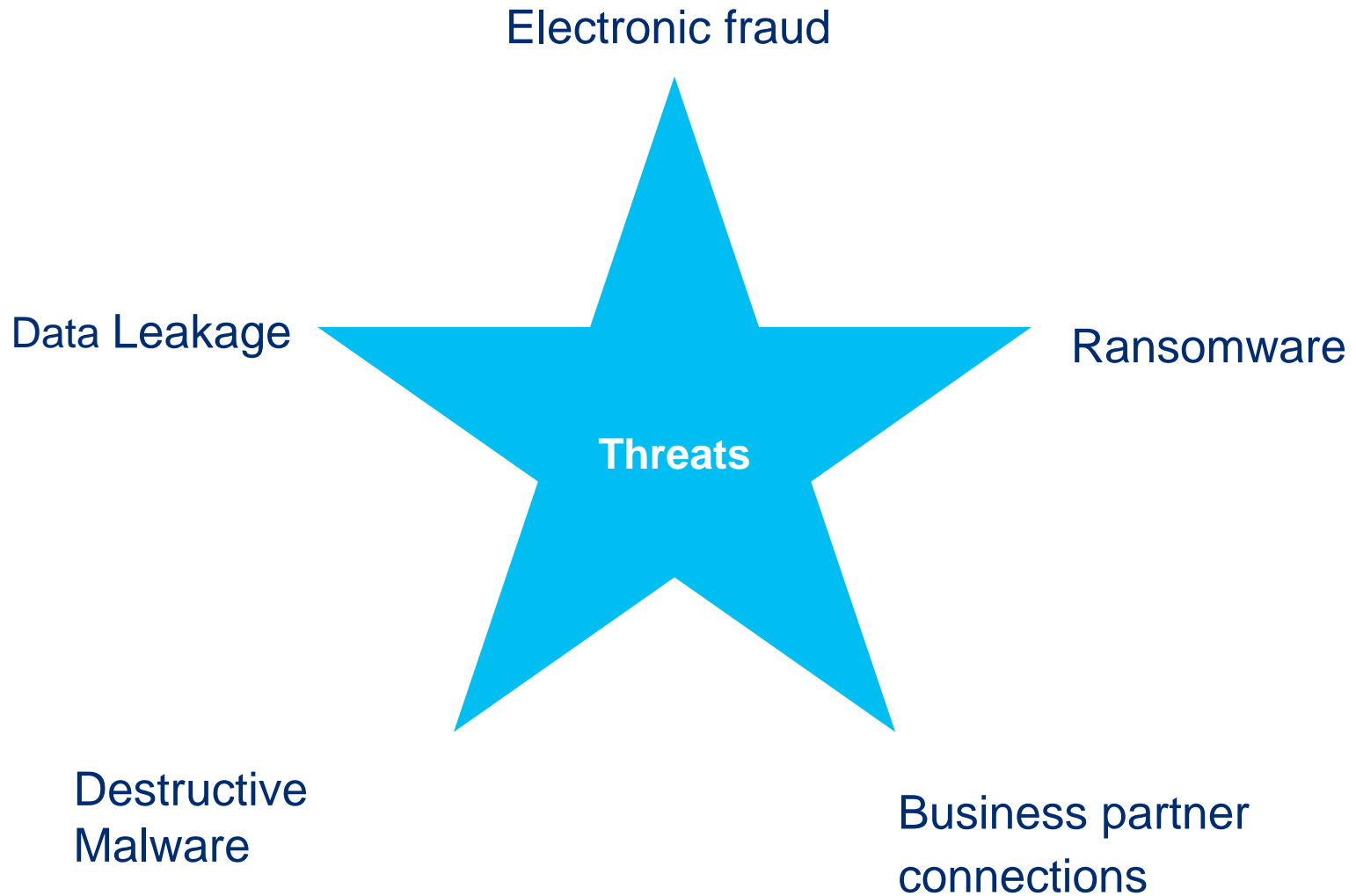
An attack will happen. It is only a matter of when.

- **Even if an attacker fails 99 times out of 100, it is a success.**
- **Likewise, an organization that fails to protect itself 1 time out of 100 is considered a failure in regards to cyber security.**
- **Prevention is key in order to make your company a less attractive target.**
- **Detection and response are key elements for any cybersecurity plan.**

The Risks.

- Lack of leadership and technical talent
- Significant share of Latin America population is not aware of cybersecurity risks
- Most countries are fighting digital crime with “analogic” laws
- Organizations have not been successful at detecting attacks
- Existence of Shadow IT in many organizations.
- Process outsourcing solely focused on cost reduction.

The Threats.



The Opportunities

- An intelligence-led approach is fundamental
- Collaboration is an effective way to gather intelligence
- Latin America governments must start discussing cyber security with the general population
 - Initial focus should be on privacy
 - Discussion should evolve towards cyber-crime laws and regulations
- Law enforcement agents must be trained to operate in this new context
- Cyber crime has no boundaries. Nations must cooperate to legislate and fight it accordingly

Thank you!

Contact information:



www.linkedin.com/in/andrealsalgado



andre.salgado@citi.com

The Citi logo is centered on a blue gradient background. It features the word "citi" in a white, lowercase, sans-serif font. A red, curved arch is positioned above the letters "i" and "t". To the right of the word "citi" is a registered trademark symbol (®).

citi®