Baker McKenzie.

Deciphering Data – Latin America Series

Phishing and Data Theft

Key Takeaways

- Increase in data thefts during the pandemic.
- Insecure home devices while working from home creates incentives for criminals including data phishing and hacking
- Distribute rules and trainings, so employees understand how easy it is for criminals to attack that information
- Cloud services and cloud providers offers different levels of security, it is important to contract the highest level possible and to make sure that the service provider complies with Mexican laws.
- There are new technologies and devices, including APIs that can allow criminals to develop new ways to attack. When developing a new product, it is important to establish a beta stage to monitor the progress and the way the product interact to test the security.
- In the financial sector ransomware attacks have become easier to monetize. The way to be paid varies from bank transfer, to cash, to cryptocurrencies, that were not available before, so there are new ways to capitalize an attack.
- Open banking is being implemented in LatAm. Mexico has rules to share information between Fintechs and traditional banks, which can gather information from banks and users and communicate the product best suited for consumers. This is something that could be a target.
- Monitor and audit regularly to ensure that all the security measures are in place and that employees are complying with security measures.

How data incidents are handled

- We can't see a standard practice on cyberattacks, since every attacker works in its own different way therefore we recommend to implement standard security mechanisms but with high level of protection.
- We do training plans and sessions all year, to be ready in the event of an attack.
- In the US there are in place teams of PR, crisis management, ransomware negotiators, insurance company with a clear plan to respond.
- In Mexico and LatAm: we don't see this type of preparation.
- There are two frameworks in Mexico, if you are a private company and one for public entities.
- Both require notice to the data subject, both contain regulations about the content of such notice, and the definition of data breach is quite similar and encompass any lost, unauthorized use.
- Differences: government entities have more requirements to give the DPA, more similar to the EU rules.
- If we don't have a solid practice to respond to incidents it's because these are rarely notified to the regulators or data subjects. Only cases of significant risks to the data subject, this is a grey area. This is why there is no information on the total incidents and there's not sharing of common practices.

Click here to video recording

Financial institutions, are commercial entities, they don't have any mechanisms required by law.

- The Fintech companies included in the Fintech law (e wallets, crowdsourcing) do have requirements.
- They need to have a chief information officer designated and notified to the regulator,
- You need the protocol and manual to be presented to the regulator.
- Not all financial institutions are subject to this obligations.
- Aggregators process credit card information but don't have obligations to notify or to have a CIO.
- There will be an increase of reporting obligations, this is the trend we are seeing.

Working from home and cybersecurity:

- Traffic monitor of the network,
- Checking emails and attachments in the network
- Monitoring keyboard and camera monitoring, to enforce cybersecurity internal policies.
- This creates tension with privacy laws.
- DPA has issued guidelines to consider. I.e. making employees aware of their responsibility, taking security measures, need to communicate security incidents(i.e. lost or stolen computer). We've seen employees don't know how to act in this situation. This affects not only the employer but also third parties (providers, clients, etc)
- Advise employees against the use of personal email account with business email and/or sending professional email to personal emails.
- Verify the address of the sender, most phishing attacks are from fake emails account.
- We see lack of policies on personal devices, lack of monitoring, lack of compliance with the purpose of the collected information notified to the users and employees.

Trends in Legal

- Some state have included updates in the criminal law to recognize identity theft as a crime, but not at a federal level.
- These laws create new definitions about crimes.
- New bills have included some definitions about testing, white hat hacking, testing infrastructure. They been in congress for long still being discussed.
- The Criminal code does not address in specific definitions for this type of fraud.
- There is a need to update the criminal codes, to make them easier to prosecute these type of crimes.
- Having Good corporate governance, with levels and the possibility to escalate, following clear protocols.

Cost of a data breach

- 3.8 Millions in the US
- The Mexican association $500.000 USD.
- Difficult to assess, costly because they may lead to class actions. We may probably see class actions in Mexico.
- In the financial sector the issuers of a card carries the costs of a fraud, unless it can prove the responsibility falls on someone else's.
- Good practices: beta testing, encryption, different levels of authentication (token, password, two-factor security).
- Patrol your network. Train your employees. The Internet Mexican Association survey shows that 50% of companies do one training once a year. This is too low. We recommend hiring a company to conduct a fake phishing attack to test your readiness and awareness. Transparency creates more trust.