Cybersecurity in Mexico

Selected information about Cybersecurity in Mexico

June 2015
Executive Summary

As technology is evolving more and more, cyber-attacks against institutions are becoming increasingly frequent and sophisticated. As a result, cybersecurity has become a top priority for companies. According to “Allianz Risk Barometer Top Business Risks 2015”\(^1\), Cybercrime has become one of the top 5 business risk. In Germany, the United Kingdom and the United States, for instance, cyber risks are now among the top three corporate risks. However, risks are still underestimated which is preventing companies to be better prepared against cyber-attacks. In fact, this was the top reason given for why companies are not well-prepared to combat cyber risks.

McAfee report\(^2\) estimates that the global cost of cybercrime is more than 400 billion USD and accounts for 0.8% of global GDP. In fact, the total cost of cybercrime in 2014 has been estimated at 445 billion USD, with 200 billion USD being sustained by the US, China and Germany. To be more specific, in 2014 around 2,803,036 data records were stolen or lost every day; 116,793 every hour; 1,947 every minute; and 32 every second.\(^3\) Many of the breaches in 2014 involved the theft or compromise of identifiable information, such as names, addresses and social security numbers.

As for Mexico, according to the 2013 Norton Report, illicit activities in the digital domain increased in Mexico during the year costing the economy 3 billion USD. The average cost per victim increased from 197 USD to 238 USD between 2012 and 2013. In fact, Mexico ranks as the second country with the largest number of cyber-attacks in Latin America. In 2014, cyber-attacks have grown 40% in Mexico and 10 million of Mexicans were affected by cybercrimes. In 2013, Mexico’s Federal Police registered 23,549 cybercrime cases. However, this number does not reflect accurate information of the cases of cybercrime, because many of them are not reported by most of the companies, either because of their fear of reputation damage, either because they are unaware of the attacks. However, according to Fortinet Security Survey 2014\(^4\), 91% of Mexican companies have prioritized the cybersecurity in their organizations, making Mexico the country with more investment in cybersecurity in Latin America and one of the first globally.

---

\(^{1}\) Allianz, Risk Barometer Top Business Risks 2015  
\(^{2}\) McAfee (2014), Net Losses: Estimating the Global Cost of Cybercrime  
\(^{3}\) Gemalto, 2014 Year of Mega Breaches & Identity Theft  
\(^{4}\) El Financiero, “México, preocupado por la ciberseguridad”, 2014
Index

1. Cybercrime .................................................................................................................. 4
   1.1. Cybercrime Overview ......................................................................................... 4
   1.2. Causes of cybercrime ....................................................................................... 4
   1.3. Cost of Cybercrime ......................................................................................... 5

2. Cybercrime and Business ............................................................................................. 9
   2.1. Overview ........................................................................................................... 9
   2.2. Cost of cybercrime for companies .................................................................. 11
   2.3. Cybersecurity strategies ................................................................................. 14

3. Cybersecurity in Latin America .................................................................................. 18
   3.1. Overview ........................................................................................................... 18
   3.2. 2015 Latin America Predictions ..................................................................... 20

4. Cybersecurity in Mexico ............................................................................................. 21

5. 2015 Predictions ......................................................................................................... 25
   5.1. Security Predictions ......................................................................................... 25
   5.2. Biometrics Predictions ..................................................................................... 26

6. Conclusion .................................................................................................................. 27

References ..................................................................................................................... 28

Knowledge Center Mexico ............................................................................................. 30

Reach us .......................................................................................................................... 31
1. Cybercrime

1.1. Cybercrime Overview

The Internet and related technologies have changed the way we work, play, and live. This boom in new technologies brings with it new opportunities for productivity, entertainment and innovation. In 2012, there were 7.8 billion mobile devices connected worldwide, and this number is expected to reach a value of 15 billion devices in 2015 and 50 billion in 2020. Unfortunately, there is also a negative side to these advances. A tool that has become so crucial and necessary nowadays has also become a target for criminals. Keeping personal information private is becoming more and more difficult. As expected, cyber criminals are taking advantage of the same advances in technology to perpetrate more complex and extensive crimes. In fact, the scenario once dominated by the worms and viruses unleashed by irresponsible hackers is now ruled by a new class of cybercriminals.

More and more criminals are taking advantage of the speed, convenience and anonymity of the Internet to perform a diverse range of criminal activities that escape borders, either physical or virtual. Cybercrime is a term that covers a broad scope of criminal activity using a computer; it concerns performing illegal activities towards an organization, using digital means.

1.2. Causes of cybercrime

There are two primary factors contributing to the growing number of cyber-attacks. First, cyber criminals have the benefit of jurisdiction. A cyber-attack can be originated from anywhere in the world, involving several perpetrators of different nationalities and countries, and can have numerous hosting servers located in different countries. Second, cyber criminals are becoming more sophisticated with support from a significant underground economy.

Speaking of factors that can motivate cybercrimes, they can be summarized in three main groups:

- Economically motivated cybercrime

As is the case with many crimes committed outside the Internet, money is an important trigger for many cybercriminals. In this case, there is a low perceived risk, due to anonymity and very high financial reward encourage many cybercriminals to participate in phishing, malware, fraudulent money request attacks and identity theft. In fact, individuals aren’t the only ones targeted for financial cybercrimes. Financial institutions are targeted as well, if not more frequently nowadays, mostly because financial institutions are significant money makers for criminals.

- Personally motivated cybercrime

Cybercrimes can also be the cause of personal emotions and revenge. Cyberspace is anonymous and therefore contributes to an increased tendency to commit crimes online that they may not typically commit in person.
Politically-ideologically motivated cybercrime
These kinds of attacks are carried out for moral and ethical purposes, ideological or political reasons, harming or disabling online services to protest against individuals, corporations or governments. Anonymous group is a popular example of ideologically motivated hackers. Hacktivism emerged in 2012 and became the main tool for public expression of controversial opinions, whether political or economic. In addition, it is today a way to protest about ideological conflicts.

1.3. Cost of Cybercrime

MacAfee report estimates that the average annual cost to the global economy from cybercrime is more than 400 billion USD or 0.8% of global GDP.

**Total global cost in 2014: 445 billion USD, with 200 billion USD being sustained by the US, China and Germany**

Besides economic loss, cybercrime also affects hundreds of millions of people by stealing their personal information stolen. Incidents in 2013 included more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China.

While identity theft may be one of the most profitable forms of cybercrime, generating around 1 billion USD per year in revenue on a global context, while direct losses to consumers may be the smallest element of the cost of harmful cyber activity. An estimate of 3.5 billion USD in 2012 for online fraud. However, as companies have implemented more and more anti-fraud measures, the rate of fraud has been dropping, going from 1.8% in 2004 to 0.9% in 2012. Although the total cost to a national economy is small, it might conduct the society to a general distrust of the internet and as a result the inability to make further use of it to gain business efficiencies, which remains a concern for governments.

According to the same report, the most significant loss resulting from cybercrime is in the theft of Intellectual Property (IP) and business confidential information, as this has the most significant economic consequences. To be more specific, the US Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs US companies 200 to 250 billion USD annually. Thus, IP is an important source of competitive advantage for companies and for countries. In this line, IP theft acts against innovation and slows the global rate of technological improvement. In fact, cybercrime harms innovation.

Financial crime, the theft of financial assets through cyber intrusions, is the second largest source of direct loss from cybercrime. Financial crimes usually come along with fraud, but this can take many forms to mistreat consumers, banks, and government agencies. The most damaging and harmful financial crimes seek to infiltrate bank networks, with cybercriminals gaining access to accounts and stealing money. Extortion has been emerging as a new type of stealing information, especially in India. In Mexico, banks lose up to 93 million USD annually just because of online fraud, as for Japan, the National Police Agency estimates the banks lose about 110 million USD annually.

The theft of confidential business information is the third largest cost from cybercrime. The loss of investment information, exploration data, and commercial negotiation data can cost millions of dollars to companies. By breaking into company’s networks, cybercriminals can acquire internal information on acquisition plans, revenue reports, or other data that could affect a

---

5 McAfee (2014), Net Losses: Estimating the Global Cost of Cybercrime
company’s stock prices. That stolen information can later be sold to other hackers or companies, in exchange of other relevant information, and this goes on like a cycle.

In 2014, the United States, Brazil and Russia were among the countries from which most cybercrime attacks were launched.

*Countries with most cybercrime attacks, 2014*

Source: Threat Forecast 2015
Regarding regional variations, North America, Europe, and Asia lost the most, while Africa lost the least. There is a significant correlation between income levels and losses from cybercrime, as richer countries (or firms) have more chances to be attacked. Brazil, Mexico, and Colombia are the most affected countries in Latin America.

According to the Ponemon Institute\(^6\), the cost of cybercrime impacts all industries but in different ways. The cost of cybercrime for companies in the energy & utilities, financial services and technology industries experienced the highest annualized cost. In contrast, companies in the media, life sciences and healthcare industries incurred much lower cost on average.

---

\(^6\) Ponemon Institute (2014), Global Report on the Cost of Cyber Crime
Global average annualized cost by industry sector, in Million USD, 2014

- Healthcare: 1.38
- Life Sciences: 1.47
- Media: 2.14
- Automotive: 2.25
- Retail: 3.33
- Hospitality: 3.34
- Education & research: 4.52
- Consumer Products: 4.6
- Defense: 5.02
- Public Sector: 5.22
- Communications: 5.53
- Transportation Services: 5.79
- Industrial: 6.52
- Technology: 6.85
- Financial services: 8.51
- Energy & Utilities: 12.97
- Public Sector: 13.18

Source: Ponemon Institute
2. Cybercrime and Business

2.1. Overview

According to the “Allianz Risk Barometer Top Business Risks 2015”, Cybercrime has made it to the top 5 business risk. Cybercrime and IT failures continue to climb in the Allianz Risk Barometer, stepping up to the top five business risks globally for the first time (in 2014, cyber risks ranked 8th and in 2013 just 15th). In Germany, the United Kingdom and the United States cyber risks are now among the top 3 corporate risks.

According to a PwC survey, Cybercrime (39%) is still the second most common type of economic crime reported by financial services respondents after asset misappropriation (67%).

In addition, 45% of financial sector respondents said they had been victims of cybercrime, compared to only 17% in other industries. These figures in the financial sector can be explained due to the fact that big and regulated financial institutions possess more and security measures, which allow companies and institutions to detect more cyber-attacks. In addition, financial institutions are major targets because they provide larger amounts of personal financial information online, which can be sold in a future. However, the real proportion of cybercrime could be higher. Many entities may not have clear awareness on whether their networks and the data contained have been hacked; cybercrime operates largely unseen. In addition, most cybercrime incidents are unknown.

Clearly, financial organizations believe that cybercrime is becoming a greater threat than ever before and still many do not believe it will actually happen to them.

---

7 Allianz, Risk Barometer Top Business Risks 2015
8 PwC, 2014 Global Economic Crime Survey
9 PwC. US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey
Significant detected incidents across industries, 2014

**Banking & finance**

- Financial Fraud: 36%
- Denial of service attacks: 29%
- Financial Losses: 23%
- Customer records compromised or stolen: 23%
- Identity theft: 20%
- No incidents: 20%

**Government**

- Unauthorized access/use of data, systems, networks: 24%
- Operating systems/files altered: 24%
- Denial of services attacks: 22%
- Identity theft: 19%
- Confidential records compromised or stolen: 19%
- No incidents: 16%

**Health**

- No incidents: 30%
- Private or sensitive data unintentionaly exposed: 22%
- E-mail or other applications unavailable: 22%
- Financial losses: 19%
- Customer records compromised or stolen: 19%
- Theft of electronic medical data: 15%

**Information & Telecom**

- E-mail or other applications unavailable: 33%
- Denial of services attacks: 28%
- No incidents: 28%
- Operating systems/files altered: 20%
- Unauthorized acces/use of data, systems, networks: 19%
- Software applications altered: 11%

**Insurance**

- No incidents: 38%
- Financial losses: 29%
- Unauthorized access/use of data, systems, networks: 19%
- Financial fraud: 19%
- Customer records compromised or stolen: 19%
- Confidential records compromised or stolen: 19%

Source: PwC
Concerning the sources of cybersecurity incidents, the highest percentage of respondents (72%) identified outsiders such as hackers. Nation states (7%) and organized crime (8%) are in fact less likely to commit the crimes, although larger companies are more probable to be concerned about these threat actors. On the other hand, the survey showed that 26% of respondents that had detected a cybersecurity incident were unable to identify the origin of the attack.

However, the incidents are usually undertaken inside the company. 28% of respondents identified insiders, which includes trusted actors such as current and ex-employees, service providers, and contractors. The larger the business, the more likely it is to take insiders as a threat and to recognize that insider incidents can be more costly and harmful.

In this line, according to the PwC survey[^10], larger companies detect more incidents, which is not surprising since large organizations offer more and more relevant information to cybercriminals.

In 2014, large organizations (those with gross annual revenues of 1 billion USD or more) detected 44% more incidents compared with the year before. As larger companies implement more and more effective security measures, cybercriminals are increasingly stepping up their assaults on medium companies. That, in part, could explain the jump of 64% in the number of incidents detected by medium-size organizations (those with revenues of 100 million to 1 billion USD). As for small companies, with revenues of less than 100 million USD, they detected 5% fewer incidents in 2014. One of the reasons of this drop may be that small companies are investing less in cybersecurity, which may leave them unable of detecting intrusions and more exposed to cybercriminals.

### 2.2. Cost of cybercrime for companies

Companies are getting increasingly concerned about cybercrime. According to the PwC CEO study[^11], nearly 45% of the US CEOs say they were “extremely concerned about cyber threats and a lack of data security”. As for CEOs in China, 33% expressed “extreme concern”, while in Australia and Canada, 31% and 30% respectively were “extremely concerned”.

One important reason for the increasing concern is the high financial costs of cybercrime. Another study of PwC[^12] found that 7% of US organizations lost 1 million USD or more due to cybercrime incidents in 2013. 14% of respondents reported losses have increased in the past year. It is worth noting that the costs of these incidents remain usually unknown. Monetary losses attributed to cybercrime are hard to estimate. In fact, 67% of those who detected a cybersecurity incident were unable to estimate the financial costs.


[^12]: PwC, 2014 Global Economic Crime Survey
[^13]: Ponemon Institute, 2014 Global Report on the Cost of Cyber Crime
While risk has become universal, the PwC “The Global State of Information Security” study\textsuperscript{14} found that economic losses due to security incidents vary by organizational size. Small companies report that the cost of incidents in fact decreased 37% compared with the previous year, while large companies report a 53% jump in financial costs. As for medium-size companies, the costs of incidents increased 25% over the year before. The US sample reports the highest total average cost at 12.7 million USD and the Russian sample reports the lowest total average cost at 3.3 million USD. All seven countries experienced an increase in the cost of cybercrime cost over the past year, ranging from 2.7% for Japan to 22.7% for the United Kingdom.

However, cyber-attacks are not limited to financial losses. With a rise in the cybercrime, businesses are increasingly meeting impacts not only on the financial front but also damage to their brands and market reputations. They suffer reduced valuation after being publicly hacked, usually by a drop in stock prices. At the same time, consumer confidence in the brand is affected. In fact, reputational damage is one of the major reasons why organizations resist reporting such incidents to law enforcement or external agencies.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{chart1.png}
\caption{Total cost of cybercrime in selected countries, in Million USD, 2013-2014}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{chart2.png}
\caption{Average financial losses due to security incidents, in million USD, 2013-2014}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{chart3.png}
\caption{Main causes of economic loss}
\end{figure}

\textsuperscript{14} PwC, The Global State of Information Security Survey 2015
On the other hand, as mentioned before, the most important area for loss is in the theft of intellectual property and business-confidential information, causing a negative effect on innovation. It can harm the global capacity to innovate, by lowering the returns for innovators (and thus discouraging them to keep innovating) and by reducing the resources and incentives for innovation.

Cybercrime and cyber espionage can push companies to stop investing on Research & Development and rely on cyber espionage to gain new IP. By stealing IP, the target company has still access to its IP, but has now to face new competitors. New products and features attract new customers until competitors catch up. It is worth mentioning that the theft of IP might not generate an immediate effect. In fact, there may be a large gap (five to ten years) between the theft of the IP and the public exposure of the results. Thus, it is quite difficult to quantify the consequences of IP loss. This means that companies might underestimate or minimize loss and therefore underestimate their risk.

Although all companies face the risk of loss of IP and confidential business information, some sectors, such as finance, chemicals, aerospace, energy, defense, and IT, are more likely to be potential victims.

IP theft from cybercrime not only works against innovation and slows the global rate of technological improvement, but has an impact on the national economy.

Finally, all these factors lead to an increased cost of security.

**Governments and companies spend around 7% of their information technology budgets on security**

In 2012, federal agencies spent more than 15 billion USD on cybersecurity projects and activities, accounting for 20% of all federal spending on information technology.15

In 2014, small companies reduced security investments by 20% over 2013, while medium and large companies reported a 5% increase in IT security spending. This drop in security spending from small companies might be explained by the fact that smaller organizations often consider themselves too insignificant to catch the attention of professional hackers and organized crime. Also, the most talented candidates are usually hired by bigger organizations.

**Average security budgets, in million USD, 2010-2014**

Source: MacAfee

15 McAfee, The economic impact of cybercrime and cyber espionage, 2013
In fact, security spending has been increasing across most industries. According to Forrester\textsuperscript{16}, budgets for all industries grew between 2012 and 2014 by 83%. Retail and Wholesale, Manufacturing and Utilities and Telecommunications are the sectors that have increased their security the most between 2012 and 2014, growing by 115%, 2016% and 101% respectively.

Security budget as a percentage of IT spend by sector, 2012-2014

According to Allianz Risk Barometer, underestimating the risk is what is preventing companies to be better prepared against cyber risks. Although awareness of cyber risks is increasing, the different impacts are still underestimated. This was the top reason given (73%) for why companies are not well prepared to combat cyber risks, followed by budgetary constraints (59%) and a lack of understanding about the complexity such risks can bring to the company (54%).

2.3. Cybersecurity strategies

Many companies have likely underestimated the risk they face. Cybercrime remains a growth industry and companies that fail to adequately protect their networks will be at an increasing competitive disadvantage.

\footnotesize{\textsuperscript{16} Forrester, (2015), “Understand Cybersecurity and Risk for 2015”}
Collaboration

Organizations, private and public, are now starting to work together to fight cybercrime and gain more resources and information about current security threats and effective responses. According to the Global State of Information Security Survey 2014, 82% of companies with high quality security services collaborate with others to reinforce their knowledge of security and threat trends.

In 2014, 55% of respondents say they collaborate with others to improve security, an increase of 12% over 2013. The larger the company, the more they collaborate with others: 66% of large organizations do so, compared with 49% of small firms. Collaboration is more common in regions where IT infrastructure has evolved rapidly over the past years. Respondents from South America and the Asia-Pacific region, for instance, are have more chances of working with others to advance security intelligence.

According to the PwC study[^17], many CEOs appreciate collaboration between business and government on cybersecurity strategies. To be more specific, 43% of CEOs globally said they are in favor of collaboration between business and governments.

Employee training

According to Forrester, “your efforts depend on people, not just technology”[^18]. Investing in people is just as important as investing in technology and tools for data security and privacy, and user security awareness and training is not implemented enough or effectively in companies. As it was already mentioned, many insider incidents come from employee vulnerabilities such as social engineering and loss of devices, risks that could very well be diminished by employee training. Although security awareness and training is not taken seriously in some organizations, more and more, companies are embracing a culture of security through employee awareness and training programs. A cybercrime survey[^19] showed that 42% of respondents thought security education and awareness for new employees was essential in preventing a potential crime. In fact, organizations that do not have security awareness programs, in particular, training for new employees, report significantly higher average financial losses from cybersecurity incidents. Companies with no security training for new employees reported average annual financial losses of 683,000 USD; while those that do have training said their average financial losses totaled 162,000 USD.

<table>
<thead>
<tr>
<th>Awareness and training</th>
<th>Respondents have adopted</th>
</tr>
</thead>
<tbody>
<tr>
<td>New employee security training</td>
<td>46%</td>
</tr>
<tr>
<td>Periodic security education &amp; awareness programs</td>
<td>44%</td>
</tr>
<tr>
<td>Employees required to review &amp; accept written inappropriate use policy on periodic basis</td>
<td>40%</td>
</tr>
</tbody>
</table>

Source: PWC

Large organizations are more likely to recognize and act upon the importance of employee training. The survey showed that 58% of big companies do so, compared with 47% of small firms. Security training is most dominant in the North America and Asia-Pacific regions, and is most likely to be incorporated by organizations in the healthcare, industrial products, and financial services sectors.

[^17]: PwC, The 2015 US CEO Survey essay
[^19]: PwC, US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey
In addition, organizations can also prevent insider incidents by controlling and analyzing employees for negative behaviours. For instance, respondents of the above mentioned survey said that insiders who had committed cybercrimes most often presented behaviours such as violation of IT policies, disruptive behaviour, and poor performance reviews. They also said most insider incidents are conducted for financial gain.

On the other hand, customers have also become a point of focus for companies, as they also share private information with a company and expect protection from it. Based on the Forrester data\(^\text{20}\), 47% of firms in North America and Europe have training programs to educate their customers about information security and how to protect themselves, and 25% are planning to.

Cyber insurance

One of the measures companies have been undertaking to fight cybercrime is the cyber insurance. Due to the rising number of threat, protecting against financial losses from cyber risks is now ranked as high as other insurable risks. More than half (51%) of respondents of the PwC survey on The Global State of Information Security\(^\text{21}\) said they have purchased cybersecurity insurance, up from 45% the year before. It is worth noting that companies are focusing on cyber insurance as a way to improve their security system. Companies from the aerospace and defense, automotive, entertainment and media, and financial services industries are most likely to purchase cyber insurance. South America is at the top of the list concerning the adoption of cyber insurance, with 58% of respondents saying they have purchased policies. The US, with 44%, is the region that least invested in cyber insurance.

According to the department of Homeland Security, “A robust cybersecurity insurance market could help reduce the number of successful cyber-attacks by: (1) promoting the adoption of preventative measures in return for more coverage; and (2) encouraging the implementation of best practices by basing premiums on an insured’s level of self-protection”.

\(\text{NIST Cybersecurity Framework}\)

Finally, some companies have adopted the NIST Cybersecurity Framework, which offers an effective model for risk-based security for organizations across industries and across the globe. The US organizations are already beginning to adopt it. According to the PwC survey\(^\text{22}\), 29% of the American respondents say they have adopted the Framework, and an additional 25% say adoption is a future priority.

The Framework, created through the collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure.

On the other hand, one of the biggest problems companies and countries have to face when dealing with cyber-attacks is the problem of attribution. Whenever security researchers discuss the likely provenance of an attack, they realize that any attacker could make themselves appear to be from anywhere in the world. For most network defenders, identifying the attacker is not necessary. For policymakers, however, such uncertainty poses a problem. The identity, or at least the nationality, of an attack’s source is necessary for effective prevention. If a government decides to impose trade sanctions against whoever attacks its systems or networks,

attribution becomes necessary to effectively implement such penalties.

An interesting fact is that some companies offer an economic reward for those who find vulnerabilities in their website. Twitter, for instance, has announced that it is offering a minimum reward of 140 USD for those who find security holes in Twitter.com, ads.twitter, mobile Twitter, TweetDeck, apps.twitter, as well as in the apps for iOS and Android. This amount is still way off what others are offering. Facebook or Google reward users that uncover vulnerabilities with amounts upwards of 500 USD and 1,000 USD, respectively.
3. Cybersecurity in Latin America

3.1. Overview

Latin America and the Caribbean have the fastest growing Internet population in the world, with 147 million users in 2013. Mobile devices are flourishing as a preferred method to access the Internet, and especially to use social media. Nearly 95% of Internet users in the region actively use social networking sites. In fact, Latin American and Caribbean nations occupy five of the top ten spots for the most time spent on social networks. As a result, cybercrime and cyber espionage continue to grow in Latin America and the Caribbean. Only in Brazil, the cost of cybercrime reached 8 billion USD, followed by Mexico with 3 billion USD and Colombia with 464 million USD.

As in the rest of the world, cybercriminals in Latin America have been developing more sophisticated attacks and have adopted the methods of other criminals from other countries. Brazil suffered the most from cyber-threats in 2014, with up to 32% of users being affected by online threats. Peru and Panama were second and third on the list of countries under threat, with 28.7% and 28.5%. In fact, more than 28 million cyber-attacks and infection attempts were deactivated by Kaspersky Lab’s products on the computers and mobile devices in Latin America during first six months of 2014.

Top 10 Latin-American countries affected by online threats, 2014

<table>
<thead>
<tr>
<th>Global Ranking</th>
<th>Country</th>
<th>% users being affected by online threats</th>
<th>Number of cyber-attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td>Brazil</td>
<td>32%</td>
<td>22,122,995</td>
</tr>
<tr>
<td>63</td>
<td>Peru</td>
<td>28.7%</td>
<td>4,537,175</td>
</tr>
<tr>
<td>64</td>
<td>Panama</td>
<td>28.5%</td>
<td>929,976</td>
</tr>
<tr>
<td>74</td>
<td>Mexico</td>
<td>27%</td>
<td>17,514,481</td>
</tr>
<tr>
<td>80</td>
<td>Honduras</td>
<td>26.5%</td>
<td>458,438</td>
</tr>
<tr>
<td>90</td>
<td>El Salvador</td>
<td>25.4%</td>
<td>439,970</td>
</tr>
<tr>
<td>92</td>
<td>Nicaragua</td>
<td>24.9%</td>
<td>310,517</td>
</tr>
<tr>
<td>95</td>
<td>Ecuador</td>
<td>24.6%</td>
<td>3,157,211</td>
</tr>
<tr>
<td>97</td>
<td>Colombia</td>
<td>24.4%</td>
<td>4,991,622</td>
</tr>
<tr>
<td>98</td>
<td>Chile</td>
<td>24.2%</td>
<td>1,813,276</td>
</tr>
</tbody>
</table>

Source: Karpersky Lab
The most widespread types of cyber-crime across Latin America are related to offences against the confidentiality, integrity and availability of computer data and systems, i.e. phishing. While targeted attacks continue to rise in Latin America and the Caribbean region, they are evolving. Whereas spear-phishing once was the most common method attackers used to install malware, watering-hole attacks are slowly supplanting the former in the region. That is to say, attacks in which the attacker infects websites often used by the victims with malware. Brazil, Panama and Mexico are the top three sources of phishing attacks in Latin America and the Caribbean, contributing to 0.23%, 0.07% and 0.03% respectively, of all phishing attacks worldwide.

Manufacturing was at the top of industries targeted in 2013, comprising 30% of all attacks in Latin America, followed by Construction with 23% and Service-Professional (including Engineering, Accounting, Legal, and Heath related services) with 20%.

### Industries Targeted in Spear-Phishing Attacks, Latin America and the Caribbean, percent of all attacks in Latin America, 2013

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail</td>
<td>0.50%</td>
</tr>
<tr>
<td>Mining</td>
<td>1%</td>
</tr>
<tr>
<td>Services-Non Traditional</td>
<td>3%</td>
</tr>
<tr>
<td>Wholesale</td>
<td>9%</td>
</tr>
<tr>
<td>Finance, insurance &amp; Real Estate</td>
<td>10%</td>
</tr>
<tr>
<td>Services-Professional</td>
<td>20%</td>
</tr>
<tr>
<td>Construction</td>
<td>23%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>30%</td>
</tr>
</tbody>
</table>

Source: Symantec

On the other hand, across Latin America and the Caribbean, the number of incidents involving banking Trojan has increased significantly. In fact, during 2014, Kaspersky Lab solutions blocked 1,910,520 attacks attempting to launch malware capable of stealing money from online banking accounts. Noticeably, the number of attacks grew considerably in May and June 2014. This might was caused by an increase in online banking activity at the beginning of the holiday season as well as by the inauguration of the 2014 World Cup in Brazil, where cybercriminals used financial malware to steal tourists’ payment data. Online banking is becoming the greatest threat area. Initially discovered in Mexico, malware targeting ATMs has spread to other countries throughout the Americas.

Cyberspace is also being exploited by drug cartels and youth gangs. In fact, over 80% of all global online crime is now connected to organized gangs operating across borders, according to Interpol. Criminals use more and more the digital world to intimidate, signal control over territory, and extract illicit rents. The digital domain allows them to project influence and multiply their distribution networks, in some cases publicly challenging municipal and district level authorities. This has included the massive illegal collection of money (e.g. cyber pyramids), the use of virtual currency as a mechanism for money laundering, and the perpetration of illicit deals involving trafficking in arms, drugs, child pornography, etc.

In addition, hacktivism has also emerged in Latin America. LulzSecPeru is widely considered the region’s most accomplished hacktivist team. They have infiltrated the networks of the armed forces and police, and other government agencies in Argentina, Colombia, Chile and Venezuela. Until now, their signature exploit was hijacking the Twitter accounts of Venezuela’s president and ruling socialist party during elections last year. One of the latest hacktivist group to capture attention is TeamHackArgentino.
With the rise of cybercrime, governments and the private sector in Latin America seek new ways to protect against hacking and techniques. In fact, in 2013 many countries made important advances in developing their policy and legal frameworks and improving their technical capacities. For instance, Guyana, Jamaica, Trinidad and Tobago, and Barbados made significant progress in establishing operationalizing a national cyber incident response team. Other governments have started to do the same. Trinidad and Tobago is the only country in Latin America that has formally adopted a National Cyber Security Strategy. Speaking of the industry measures, the banking sector is the most preoccupied with the threat of cyber-crime. Many have introduced safety measures, including new password-protection and code schemes.

3.2. 2015 Latin America Predictions

<table>
<thead>
<tr>
<th>Case study – Machete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recently, a new cyber-espionage campaign named Machete was discovered. This “movement” has been targeting high profile victims (government, military, law enforcement agencies and embassies) for the last four years. Latin America is the main field of operation: most of the victims are located in Venezuela, Ecuador and Colombia; other countries touched by Machete include Russia, Peru, Cuba, and Spain. The main objective of the attackers is to hijack sensitive and relevant information. This cyber-espionage tool is capable of performing several operations, such as copying files to a remote server or a special USB device if inserted, hijacking clipboard content, key logging, computer microphone audio capturing, taking screenshots, getting geolocation data, and taking photos with the web camera on the infected computer.</td>
</tr>
</tbody>
</table>

Source: Kaspersky Lab

With the rise of cybercrime, governments and the private sector in Latin America seek new ways to protect against hacking and techniques. In fact, in 2013 many countries made important advances in developing their policy and legal frameworks and improving their technical capacities. For instance, Guyana, Jamaica, Trinidad and Tobago, and Barbados made significant progress in establishing operationalizing a national cyber incident response team. Other governments have started to do the same. Trinidad and Tobago is the only country in Latin America that has formally adopted a National Cyber Security Strategy. Speaking of the industry measures, the banking sector is the most preoccupied with the threat of cyber-crime. Many have introduced safety measures, including new password-protection and code schemes.

3.2. 2015 Latin America Predictions

<table>
<thead>
<tr>
<th>Banking Trojans</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking trojans will keep evolving. Its creators will integrate advanced persistence techniques in operating systems. In addition, criminals will no longer steal from users or customers of banks; they will steal from the banks directly. Also, criminals will not only steal money but confidential information, mainly managed by financial institutions in their private networks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cooperation with criminals in Eastern Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technologies will not only be used locally, instead platforms and existing infrastructure will be used fully which will make it more difficult to fight cybercrime.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Regional monetization through mobile applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Now the criminals will focus on integrating the “click” techniques on applications for Android. This will also include the development of Botnet networks on mobile devices in Latin America.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fraud interconnected devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices such as routers and others with ability to connect to the Internet will continue operating to store malicious code and launch attacks against third parties.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social engineering for everything</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events such as Copa America and the Olympics will keep being exploited by local criminals for all types of fraud, e.g. installation of malware, phishing attacks and selling nonexistent items.</td>
</tr>
</tbody>
</table>

23 Kaspersky Lab
The adoption and use of information technology and communication has increased in many contemporary societies. The growth of Internet use in Mexico had a significant increase from 5%, slightly more than 5 million users out of a total population of about 103 million in 2000, to 41%, with approximately 50 million Internet users in 2014. Although the wireless connectivity generated economic transformations in Mexico, illegal cyber activities emerged as a new method of generating profit. Mexico ranks as the second country with the largest number of cyber-attacks in Latin America, after Brazil. The constant increase in connectivity is one of the main factors that make cybercriminals direct their attacks against Mexico. In 2014, cyber-attacks have grown 40% in Mexico. In fact, according to the Norton Report, 10 million of Mexicans were affected by cybercrimes.

Cybercrime is growing rapidly, according to Ciro Humberto Ortiz Estrada, head of Mexico's Scientific Police Division, likely because of its high Internet connectivity and abundance of criminal groups. In addition, the Organization of American States (OAS) warns that growth can also due to the fact that Mexican authorities have better capabilities to identify such incidents nationwide.

In 2013, Mexico's Federal Police registered 23,549 cybercrime cases. However, this number does not reflect accurate information of the cases of cybercrime, because many of them are not reported by most of the companies, either because of their fear of reputation damage, either because they are unaware of the attacks.

### Type of cybercrimes in Mexico, 2013

- **Malware**: 52%
- **Defacement**: 13%
- **Phishing**: 13%
- **Spam e-mails**: 14%
- **Others**: 8%

Source: Comision Nacional de Seguridad

#### Entities Affected by cybercrimes in Mexico, percentage of total cyber-attacks, 2013

- **Academia**: 26%
- **Government**: 39%
- **Private Sector**: 31%
- **Other**: 14%

Source: Symantec

---

In 2013, the main segments affected by cybercrime were academic institutions, government and the private sector, according to the data released by Symantec\textsuperscript{26}. On the other hand, Malware, Defacement and Phishing were among the most common forms of cybercrime in the country. In Mexico, banks lose up to 93 million USD annually just because of online fraud, according to MacAfee\textsuperscript{27}. Small- and medium-size businesses were the most vulnerable to these attacks, since they do not have the sophisticated protection systems that larger companies can afford.

\textbf{Origin of cyber-attacks in Mexico, 2013}

\textsuperscript{26} Symantec (2014), Latin american + caribbean cyber security trends
\textsuperscript{27} McAfee (2014), Net Losses: Estimating the Global Cost of Cybercrime
According to the Fortinet survey\textsuperscript{28}, 6 million virus and more than 8 million cyber-attacks were detected in Mexico during 2014; fraud being the most denounced cybercrime. In 2014, the number of fraud doubled, mainly by the theft of credit cards information through online shopping. The survey concluded that consumers showed little trust in institutions to protect personal information. In fact, only 22\% truly trust financial institutions and in 2014, 82\% of consumers in Mexico are more worried about possible theft of their personal information derived from a data breach, than they were a year ago. However, users are not taking the necessary precautions to protect their personal information. 86\% of the respondents have only implemented stronger passwords as a means to improve security, ignoring more effective measures, such as two-step authentication and password management services options. The study found that 16\% of the companies were recently affected by data leakage.

\textbf{Measures taken by respondents to improve cybersecurity, 2014}

\begin{itemize}
  \item No measures: 8\%
  \item Password management (External): 10\%
  \item Password management (internal): 24\%
  \item Two-step authentication: 28\%
  \item More solid passwords: 86\%
\end{itemize}

Source: Fortinet

According to the Fortinet Security Survey 2014\textsuperscript{29}, 91\% of Mexican companies have prioritized the cybersecurity in their organizations, making Mexico the country with more investment in cybersecurity in Latin America and one of the first globally.

Among the companies that spend more in cybersecurity are those in the financial sector, followed by telecommunication.

On the other hand, Mexican authorities have confirmed the main obstacles to fight cybercrimes in Mexico are the constant lack of legislation to act immediately, the poor resources the police has to act, which affects the research and cause the lack of awareness among the society about cybersecurity.

However, as cyber threats increase each year in Mexico, people and companies are more concerned. Different units to fight cyber threats have been created by the Mexican government since 2000, but as the levels of Internet penetration continue to grow, the incidents have as well increased without counting with a real tool to defeat or prevent these attacks.

The Federal Police of Mexico serves as the first authority for cybercrimes, although numerous other government institutions also intervene.

In 2000, President Vicente Fox created the Cyber Police, in charge of identifying and dismantling organizations involved in identity trafficking, theft and corruption of under aged. Also, in 2002, the Coordination Center for the Prevention of Electronic Crimes was created in response to the growth of cyber incidents. The center is responsible for managing cyber incident responses, investigating electronic crimes, analyzing digital evidence, protecting critical infrastructures, and responding to digital threats. In addition, the Federal Police counts with the National Center for Cyber Incident Response, to monitor the integrity of technology-strategic infrastructure of the country and to identify potential attacks.

In 2012 as well, the Scientific Division of the federal police was created to fight cybercrimes with more innovated resources.

Although the government has been implementing different strategies to combat...
these crimes, including new units created to address the problem, cybercrime is still relevant in the country.

The National Security Program (2014 - 2018) was launched by Enrique Peña Nieto Government to become one of the main strategies to develop a real policy on cybersecurity for protecting and promoting national interest and objectives. Its main actions are:

- Promote actions to prevent and combat cyber-attacks.
- Strengthen mechanisms for preventing incidents in the federal executive sites.
- Promote compliance and development of procedures to evaluate and strengthen the performance of the response teams to incidents of cyber security in the federal executive branch.
- Improve human capital skills and technological infrastructure to address cyber security incidents.
- Establish international cooperation on cyber security and cyber defense to prevent and address attacks on the computer systems of the country.

In addition, Mexican experts maintain a close and constant collaboration with more than 300 teams from 69 countries to prevent and combat these crimes.

On the other hand, in May 2014, Microsoft and the Federal Police signed a business cooperation agreement to take actions against cybercrime in Mexico. The coordination with Microsoft Mexico was aiming to promote Internet security in Mexico.

In this line, in April 2014, the government announced its adhesion to the Budapest Convention which also seeks to combat crimes on the Internet.

In terms of fighting cybercrime, both the adhesion to Budapest Convention, and the agreement with Microsoft represent significant advances for Mexico. On one hand, Budapest Convention will help improving national capabilities for investigating such crimes, and increase cooperation between countries. On the other hand, Microsoft will help the Federal Police to understand and use diverse tools to prevent illicit activities in the cyberspace. In fact, from 2012 to 2015, the Federal Police has stopped more than 59 thousand cyber-attacks attempts.

However, the Mexican government and other governments around the world, now face the challenge of fighting crime in cyberspace, considering issues of great importance such as territoriality, privacy of citizens, national security, the right to information, freedom of expression, the development of new security mechanisms, the constant training of the guards bodies, the law, and the collaboration of the private sector and society. Fighting crime in cyberspace without jeopardizing significant individual rights of citizens is a major challenge for the government.

As cybercrimes have increased in the last years, it is important to raise knowledge and awareness about these incidents through a culture on prevention in order to avoid more Internet users being victimized.
5. 2015 Predictions

5.1. Security Threats Predictions

**Cryptolocker.** It encrypts all types of documents in a computer that could be important to the user and then blackmails the victim into paying a ransom to obtain the files. Payment is always requested in bitcoins, so it cannot be traced by the police.

**Advanced Persistent threat (APT).** APTs are a type of targeted attack directed at companies or institutions. These attacked are usually undertaken by countries that invest huge sums of money in ensuring that the target attack goes undetected for a long time. This type of attack won’t be seeing in 2015, but will be performed that year and results will start coming out in the future.

**Targeted Attacks.** Although the majority of malware attacks are within the millions of malware samples that appear every month, a small percentage of these are made to attack previously defined targets. These attacks are becoming more common and will be very significant during 2015. The risk with this type of attack is that companies do not expected being a target of targeted attacks, therefore do not have the right measures for detecting them and stopping them.

**Smartphones.** More and more, consumers store a growing amount of data on their smartphones, and more and more criminals are willing to steal all that information. It seems that in 2015 the number of victims will increase, and therefore it will be necessary to use antivirus products for these devices. In addition, voiceprint biometrics authentication will give more security to the phone channel authentication process.

**Internet of Things (IoT).** The number of Internet-enabled devices is increasing significantly. As a result, as soon as a security error is found in the software on anyone of these, compromising the device will be easy for any cyber-criminal. In addition, these devices are connected to internal networks, home or corporate, making them perfect entry points for undertaking any types of attacks.

---

30 Panda Lab “Pandalabs annual report 2014”
5.2. Biometrics Predictions

In addition, the introduction of biometric security systems has become an important factor in the fight against cyber-crime. Biometrics refers to “authentication techniques that rely on measurable physical characteristics that can be automatically checked”. There are several biometrics types, e.g. the analysis of facial characteristics, the analysis of an individual’s unique fingerprints, the analysis of the shape of the hand and the length of the fingers, the analysis of the capillary vessels located at the back of the eye, among others.

Consumers and companies have to move beyond passwords. Companies are now in a transitory stage where in the next few years companies will evolve and replace passwords by biometrics. For instance, by 2017, embedded fingerprint sensors will become normal in tablets and smartphones. Biometric technology, for the most part, is one of the hardest forms of security to breach. This is because the body has several unique features, which are difficult to reproduce.

Keeping safe one’s identity will soon have much to do with iris scan, voice technology and facial recognition. Mobile devices are already replacing ID and passwords systems with fingerprint sensors. Companies will have the opportunity to increase and improve their level of security by investing in biometric methods as well as other types of technology within their information infrastructures.

The Future Password Index was determined from an online survey of 2,000 UK consumers, which was commissioned by Intelligent Environments. This survey showed that 79% of British consumers are ready to replace their passwords for biometric security measures.

According to the new Future Password Index, more than half (51%) of UK banking customers demand more innovative security measures in their banks. In fact, what the survey revealed is that consumers demand more and more for these new technologies31.

31 Information Age “8 in 10 Brits would ditch passwords for biometric security”
6. Conclusion

The emergence of new media and technological advances has produced the rise of new attacks and new crimes that have transformed Internet and computer technologies in extremely hostile and dangerous aspects for any organization or person. Nowadays, internet has become a tool to commit crimes and get economic benefit from it. As cybercriminals developed theirs skills and become more sophisticated with their activities, people and organizations face new challenges. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, Internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets and various email scams such as phishing. Companies not only suffer financial losses, which are very significant, but also their reputation and brand are affected, causing a drop in consumers’ confidence.

While some companies still underestimate the danger of cybercrime, most of them have already started demanding new measures to fight cyber-attacks. Cybersecurity has taken a step forward and is now becoming one of the main objectives for business.

In fact, as cyber-attacks get more complex and more harmful to companies, more innovated measures are emerging to fight against them. Not only companies are increasing the security budget but biometric methods are starting to rise. As mentioned previously, the introduction of biometric security systems has become an important factor in the fight against cybercrime. However, biometrics measures can also be hacked but with a higher level of difficulty. As time goes on, biometric technology will become more advanced and will offer more competences such as recognizing a user’s pulse or skin texture.

The year 2015 is predicted to be as bad or worse due to the constant movement of sensitive and confidential information and transactions in the digital space, and thus they will become more vulnerable to attack. Will companies be prepared enough to protect themselves from cyber threats? Are they taking steps to strengthen their cyber security system?

“Companies are divided into two: those that have been hacked and those that don’t know they have been hacked.”

- Cisco CEO
References

Academia.edu “Cybercrimes: law and practice”. [Accessed on the 18/03/2015]
http://www.academia.edu/6256988/CYBER_CRIMES


Briseño, I. (2014) “Memorandum for the president of the united Mexican states addressing Mexico’s cybercrime policy proposal for carrying out an information campaign for increasing awareness about cybercrime in Mexico”. [Accessed on the 27/03/2015]
https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/37282/BRISENOANGELES-CAPSTONE-2014.pdf

Cambridgeshire (2014) [Accessed on the 18/03/2015]
https://www.cambs.police.uk/GetCloser/Cybercrime/


CNN, (2014) "5 biometric alternatives to the password". [Accessed on the 24/03/2015]

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/31March/Impacto-y-gravedad-de-los-delitos.pdf


Cyber Threat Map https://www.fireeye.com/cyber-map/threat-map.html


https://www.forrester.com/Understand+Cybersecurity+And+Risk+For+2015/fulltext/-/E-RES117866

https://www.forrester.com/Understand+The+State+Of+Data+Security+And+Privacy+2014+To+2015/fulltext/-/E-RES119082

Fortinet, 2015, “Global Survey 2015-Mexico” [Accessed on the 22/05/2015]

Malware definition: http://cybercrime.org.za/malware/


Knowledge Center Mexico

Knowledge Center Mexico acts as a knowledge, innovation and best practices provider to PwC practitioners. This enables the practitioners to successfully identify new service offerings, approach the market and complete projects.

The expert staff of Knowledge Center designs innovative solutions for PwC partners and managers. The Knowledge Center delivers knowledge and experience through:

- Provide consulting and training in the use of various knowledge management tools.
- Research and information searches, based on the information needs of PwC staff & partners.
- Participating in the strategy design, related to global Knowledge Management & Innovation Management.
Reach us

José Antonio Quesada
Partner Clients & Markets
jose.antonio.quesada@mx.pwc.com

Manuel Flores De Orta
Sr. Specialist Manager Knowledge Management and Knowledge Center Clients & Markets
manuel.flores.de.orta@mx.pwc.com
+52 (55) 5263-8543

Alexandra Mendes
Consultant
alexandra.mendes@mx.pwc.com
+52 55 5263 6000 ext. 7536

Ekaterina Ponkratova
Consultant
ekaterina.ponkratova@mx.pwc.com
+52 55 5263 6000 ext. 7586

Itzel Andrade
Consultant
itzel.andrade@mx.pwc.com
+52 55 5263 6000 ext. 5574

© 2015 PwC Mexico. All rights reserved. PwC (www.pwc.com) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

“PwC” refers to PwC Mexico which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity and does not act as agent of PwCIL or any other member firm. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgement or bind another member firm or PwCIL in any way.