The state of cybersecurity in the Philippines

In the 3rd quarter of 2015, Kaspersky Lab reports the Philippines took the 33rd spot out of 233 countries prone to cybersecurity threats — a huge jump from the previous quarter's 43rd rank.

Jodesz Gavilan  @jodeszgavilan
Published 1:22 PM, April 27, 2016
Updated 11:37 PM, April 27, 2016

ARE WE ‘CYBERSECURE’? The recent incidents concerning Comelec highlight the state of cybersecurity in the Philippines.

MANILA, Philippines – The Philippine government seems to be a favorite target of hacking, given the number of defaced websites in recent years.

Following in the footsteps of so-called hacktivists, some have resorted to breaching systems to voice their concerns to government.

The Cybercrime Prevention Act in 2012 controversy alone attracted numerous cyberattacks from subgroups allegedly attached to Anonymous Philippines. Hackers defaced at least 20 government websites when the new law took effect in October that year.
The group went on to hack more than 100 government websites to protest several issues – including the slow Internet and the Mamasapano encounter which both erupted in 2015. On March 27 this year, Anonymous Philippines breached the Commission on Elections’ website to push them to use the security features of the vote-counting machines in the coming May elections.

The problematic state of cybersecurity in the Philippines, however, was put under the spotlight only when the Comelec attack became more than just defacement. (READ: White, black, gray hat hackers: What's the diff?)

Only a day after the poll body's website was defaced, LulzSec Filipinas got hold of Comelec data and made it publicly available. Security experts warned that the leakage of important information – including voter registration data – could result in “massive identity theft by preying criminals”. (READ: Experts fear identity theft, scams due to Comelec leak)

It became more disastrous when a website made the entire illegally-obtained and highly personal data searchable. The data breach, according to security firm Trend Micro, made Filipino voters "susceptible to fraud and other risks."

With the worrisome increasing trend of cyberattacks, how does the Philippines rate in cybersecurity?

**Poor performance**

The Philippines, based on various cybersecurity reports, may not be as prepared compared to other countries.

In 2014, the country ranked 9th among Asia Pacific countries when it comes to cybersecurity readiness, according to the Global Cybersecurity Index (GCI).

In the 3rd quarter of 2015, meanwhile, Kaspersky Lab reported that the Philippines took the 33rd spot out of 233 countries prone to cybersecurity threats – a huge jump from the previous quarter’s 43rd rank.

The security firm warned that the rise indicates that "cyberattacks against the Philippines are accelerating at full speed."

It may not show now, but "there is no doubt that cybercriminals are now noticing the country", with 17% of Filipino users’ systems infected with malicious programs or malware used by cybercriminals.

Symantec's latest Internet Security Threat Report (ISTR) said the Philippines placed 20th globally and 3rd in the Asia Pacific region for social media scams.

It added that in 2015, the country was hit by an average of 17 ransomware attacks a day – a type of virus that prevents a user from accessing his system.

**Lack of IT security professionals**
One of the weaknesses of the Philippines, according to Rene Jaspe of information security consulting company Sinag Solutions, is the low number of practicing cybersecurity professionals.

For instance, there are only 84 Certified Information Systems Security Professionals (CISSP) who are Filipinos. Out of this number, 40 are working overseas.

The roster of practicing CISSPs – just one of the most recognized information security certifications – in the Philippines is so short compared to other countries. Other Asian nations have a relatively high number of CISSPs: Indonesia has 107, Thailand has 189, Malaysia has 275, and Singapore has a whopping 1,000 experts.

The small circle of cybersecurity experts in the Philippines is problematic, considering the rising number of cyberattacks several institutions have faced in recent years.

According to the 2014-2015 Cybercrime Report of the Department of Justice's Office of Cybercrime, cyberespionage attacks or intellectual property theft is on the rise as a major threat.

In fact, 31% of the tallied attacks in recent years were directed against small businesses, while 33% of the 614 recorded cybercrime incidents involved internet/ATM fraud and identity theft.

Network security firm FireEye, meanwhile, reported in 2016 that organizations based in the country are “twice as likely to face an advanced cyberattack compared to the worldwide average.” It added that 30% of their customers were targeted by advanced persistent threat groups (APTs).

Aside from businesses, one of the main targets of cybercriminals is government, the firm added.

NOT CHEAP. Building a solid cybersecurity line of defense is expensive but worth it.

http://www.rappler.com/newsbreak/in-depth/130883-state-cybersecurity-philippines
Higher budget vs cyberattacks

The Philippines has a number of laws addressing cyberattacks such as the Cybercrime Prevention Act. However, these laws only deal with the aftermath of an attack and not so much with prevention.

For private individuals, there are a number of ways to defend computer systems and personal information from ill-minded hackers. (READ: How to protect your computer vs cyberattacks)

For government and organizations, Jaspe said they should remember that “security is not a one-time thing but a business process.”

In order to be considered as having firm security measures, Jaspe estimated that 10%-15% of the information technology (IT) budget should be allocated for cybersecurity infrastructure. This allocation, however, should be higher, especially if an organization falls under the “interesting targets” category.

It may be expensive but the long-term effects and security are worth it. In the United States, for example, President Barack Obama proposed to allocate $19 billion (P889.5 billion)* in their 2017 budget for cybersecurity, following reports that cyberattacks are the most imminent security threat his country faces.

In the Philippines, unfortunately, government budget constraints have often led to cybersecurity being put in the backburner.

This may change in the coming year as a memorandum released on April 4, 2016 by the Department of Budget and Management (DBM) now lists the formulation and implementation of the government’s cybersecurity plan and enhancement of cybercrime-solving capabilities of Philippine authorities as part of the 2017 Budget Priorities Framework.

Correcting mistakes

In the event that an organization falls victim to cybercriminals, Jaspe said the best thing to do afterwards is to “harden the platform” of systems.

Given the biggest data leak that’s worrisome to 55 million Filipino voters, it’s about time the country strengthens its cybersecurity measures.

In its ICT Manifesto for the Philippines for 2016 and Beyond, Microsoft pointed out the need for teamwork between the industry and government agencies to enhance cybersecurity.

The Philippine government should tap the technology sector in the country to assess vulnerabilities, and design strong IT systems. Microsoft also said there is a need for a framework that gives incentives to organizations that help embed cybersecurity measures.

Microsoft added that an army of cybersecurity professionals should be developed so that they can be tapped by government. This can be done by training individuals through the Technical Education and Skills Development
Authority (TESDA) and other cheap higher educational institutions.

In the end, government cannot afford to wait for another 23-year-old fresh graduate to get “bored” and test his hacking skills. – Rappler.com

Read more about the Comelec breach and how you can protect yourself:

- White, black, gray hat hackers: What's the diff?
- Experts fear identity theft, scams due to Comelec leak
- Comelec data leak puts Filipino voters 'at risk' – Trend Micro
- Is Comelec liable for website data leak?
- After Comelec data leak, what to do to protect yourself?
- Advice from banks: How to prevent identity theft

All photos from Shutterstock.

Show 3 Comments

Philippines and the world: Cybersecurity in numbers

Did you know that there have been 1,211 reported cybercrime incidents in the Philippines from 2013 to 2015?

Jodesz Gavilan  @jodeszgavilan
Published 8:30 AM, April 30, 2016
Updated 9:31 AM, May 02, 2016
IMMINENT THREAT. Cyberattacks are one of the rising threats around the world.

MANILA, Philippines – The importance of, and threats against, cybersecurity became an important issue overnight in the country due to the recent Commission on Elections data breach that resulted in personal information of about 55 million voters being leaked.

To Filipinos, defacement of websites to push a message of protest has perhaps been the most common cybersecurity threat. But other types of cyberattacks have been attempted not just in the country, but globally for years now. (READ: The state of cybersecurity in the Philippines)

For example, did you know that there were 781 recorded data breach incidents in 2015 alone? In the Philippines, meanwhile, most of the complaints received by authorities are related to online scams.

What other important facts about cybersecurity around the world and in the Philippines should you know? Rappler breaks them down in numbers.
1.5 million  Average global number of cyberattacks annually
4,000    Average global number of cyberattacks per day
70%    Percentage of cyberattacks that were undetected
$400-500 billion  Estimated global cost of cyberattacks annually
$2.1 trillion  Projected global cost of cyberattacks in 2019
$3.8 million  Estimated cost of global data breach annually
$1-$3  Cost per stolen record on the black market
781  Data breach incidents in 2015
312  Data breach incidents in the business sector
277  Data breach incidents in the healthcare sector
2.5 billion  Exposed data due to data breach in the past 5 years
84 million  New malware samples created in 2015
1,211 Reported cybercrime incidents from 2013-2015
366 Online scam complaints
240 Online libel complaints
129 Online threat complaints
127 Anti-photo and voyeurism complaints
33rd out of 233 Rank in Kaspersky’s list of countries most prone to cyberattacks
30% Percentage of Filipino clients of security firm FireEye that are targeted by advanced persistent threat groups
17% Filipino users’ systems infected with malicious program or software used by cybercriminals
17 Average number of ransomware attacks per day
84 Filipino Certified Information Systems Security Professionals (CISSPs)
44 Filipino CISSPs working in the Philippines

Better budget?

The latest cyberattack against the poll body highlighted the state of cybersecurity in the country. Despite laws that seem to keep the threats posed by cybercriminals under check, these efforts focus mainly on the aftermath of attacks.
Budget constraints prevent the full implementation of these laws and also make it difficult for government agencies to secure their systems firmly enough against hackers.

This may change, however, in the next few years as the formulation and implementation of the government's cybersecurity plan and enhancement of the cybercrime-solving capabilities of Philippine authorities have been identified as priorities in a recent memorandum released by the Department of Budget and Management. — Rappler.com


Read more about the Comelec breach and how you can protect yourself:

- White, black, gray hat hackers: What's the diff?
- Experts fear identity theft, scams due to Comelec leak
- Comelec data leak puts Filipino voters 'at risk' — Trend Micro
- Is Comelec liable for website data leak?
- After Comelec data leak, what to do to protect yourself?
- Advice from banks: How to prevent identity theft
- The state of cybersecurity in the Philippines