NATIONAL EMERGENCY RISKS AND IMPACT OF CYBERSECURITY THREATS

NULLFORGE
WHITEPAPER
WP0001-2024

www.nullforge.net

ABSTRACT

The Philippines being a country of choice for investments, correlates to the growth of technology being utilized as a backbone to sustain daily operations to meet goals set by institutions, whether it be government services, military, or private businesses. The entire country enjoys technology being each individual's ally when it comes to their daily living, subscribing to the great amount of convenience brought about by the technological advancements integrated into the different services they enjoy or are obliged to perform.

Information is the primary capital for these institutions that needs to be protected at all times. Compromised information can be negatively disruptive if it falls into the wrong hands.

Understanding the impact of cyber threats on different institutions helps prevent encountering adverse problems with services offered by different institutions that each individual enjoys having. On top of this, it will help us keep true to abiding to keep each citizen’s data privacy as an end product. In addition, the cost of repairing or continuously creating an information system over and over for each institution to serve a specific purpose to keepsake information will be lessened; as it is known that prevention is better than a cure.

INTRODUCTION

In an era where the digital realm interweaves with every aspect of modern society, safeguarding national security transcends traditional borders and takes on a multifunctional form. Today, the emergence of cyber threats presents a profound challenge to the stability and resilience of nations worldwide. As our reliance on interconnected digital systems grows, so too does the potential for catastrophic disruption from malicious actors seeking to exploit vulnerabilities for their gain.

This white paper aims to delve into the intricate nexus between national security emergency risks and the evolving landscape of cyber security threats. By examining the interplay between these two critical domains, we seek to shed light on the vulnerabilities inherent in our digital infrastructure and the imperative to fortify our defenses against emergent risks.

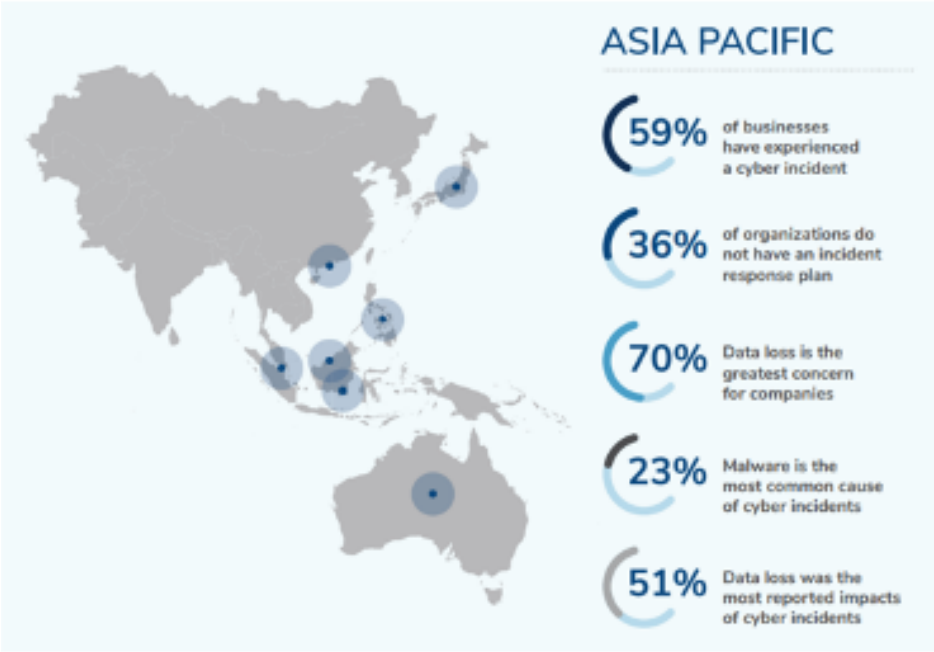
STATE OF PHILIPPINE GOVERNMENT INFORMATION SECURITY SURVEY (2021)

CYBERSECURITY INDUSTRY STATISTICS FOR THE PHILIPPINES (2022 -2023)

Global Ranking Most Number of Web Threats*1 Philippines:

Ranked 4th in 2021 (>51M threats, 100/min)

Ranked 2nd in 2022 (next only to Mongolia) *2



Compare to countries in APAC:

75% of Ph organizations experienced cyberattacks vs. 59% APAC average

70% of Ph organizations concerned on data loss

60% cited business interruption as the most significant consequence of a cyberattack

Reference: State of Incident Response: APAC (kroll.com)

CYBER THREAT LANDSCAPE (2023)

Cyberthreat Landscape of the Philippines according to *Palo Alto*

Primary threat vectors:

66% malware
63% phishing and spear-phishing attacks
56% password-related breaches

Surge of over 50% disruptive cyber incidents over the past year

5 year comparison (2018 - 2023)

10,042 unique exploit detections +68% over last 5 years
54 exploit detections per organization -75% over last 5 years
69% of organizations saw severe attacks -10% over last 5 years

Unique Exploits on the rise

Critical Prevalence Doubles:
- 100% increase malware infiltration global entities.
- Rise in cybercriminal and nation-state groups

Evolving Threat Landscape:
- selective, precise, and destructive.
- Rapid adoption, more capable, versatile, and covert.

Malware Families and Variants

Increased Botnet Activity
- 27% growth, 126% rise infections.

Prolonged Activity Periods
- Average 83/183 days active, over 1000 fold increase

•Adaptability and Exploits

Botnets Lingering in the Networks

DATA BACKGROUND (NULLFORGE RESEARCH)

The following data analyses are results of researching which institution type in the Philippines commonly encounters cyberattacks based on the number of domains that have been breached.

Collective data from the year 2018 up to 2023 shows a clear division in terms of the percentage of institution types in the Philippines that are at the receiving end of cyberattacks, in which government domains take on the share of forty-eight percent (48%), military domains at two percent (2%), and private domains at fifty percent (50%) of their domains being compromised to said cyberattacks. *(As shown in figure 1.)*

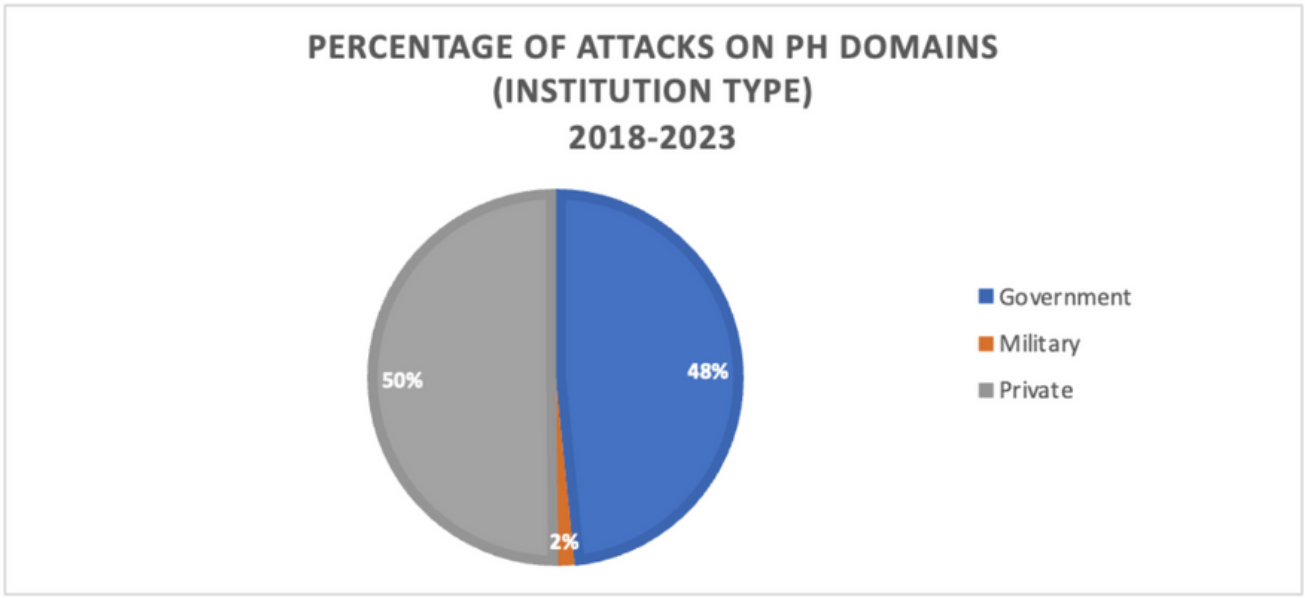


figure 1

The number of cyberattacks on each institution has kept growing each year, causing an alarm to the institutions that are impacted by such. *(As shown in figure 2.)*

The number of cyberattacks on each institution has kept growing each year, causing an alarm to the institutions that are impacted by such. Looking closely at the number of attacks on all three institution types clearly translate to which of these institutions are being reluctant in taking notice of the issue, and which institution type started addressing it.

It is found that both the government and military have a huge percentage increase from the year 2022 to 2023 compared to private institutions where it can be seen that the number of breached domains decreases yearly and starts to create a dent when it comes to improving their security structures. *(As shown in figure 2.)*

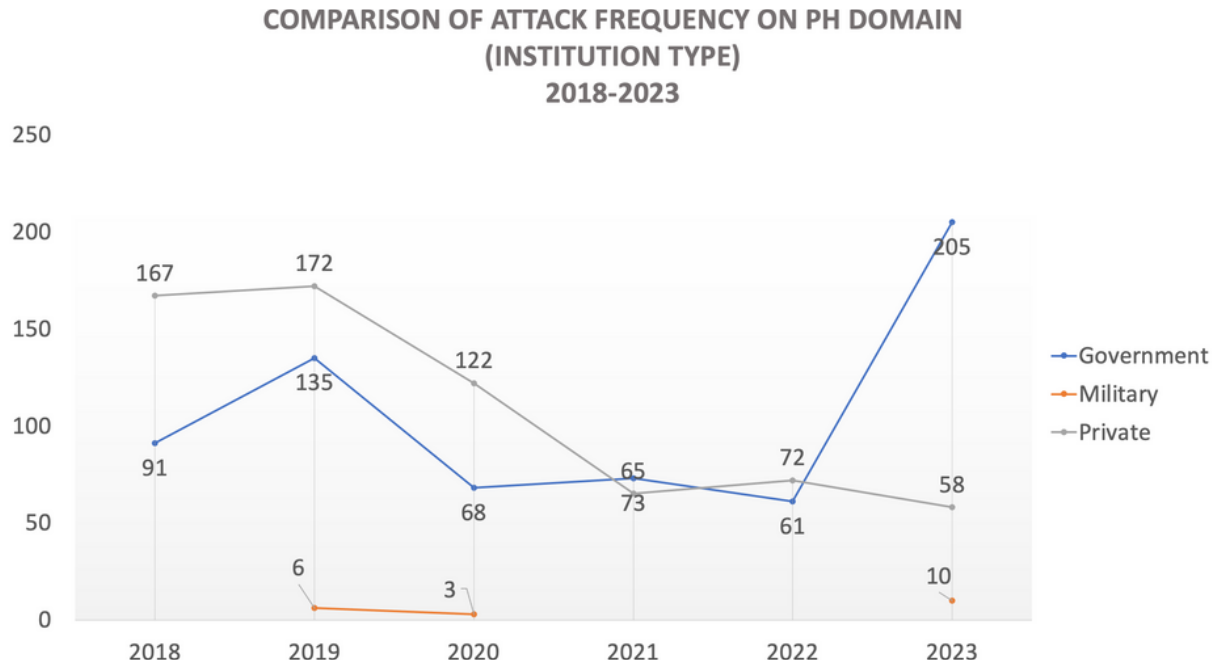


figure 2

Conducting a granular comparison of the number of domains that fall victim to cyberattacks among the three institution types shows the difference in the institutions' awareness and response to these threats.

Government domains have been breached from the year 2022 to 2023 have increased 236% in count, which calls for the immediate attention of administrators of impacted government institutions to revisit their security structure, and as such security by design should have been the utmost priority the creation of the domains impacted. *(As shown in figure 3.)*

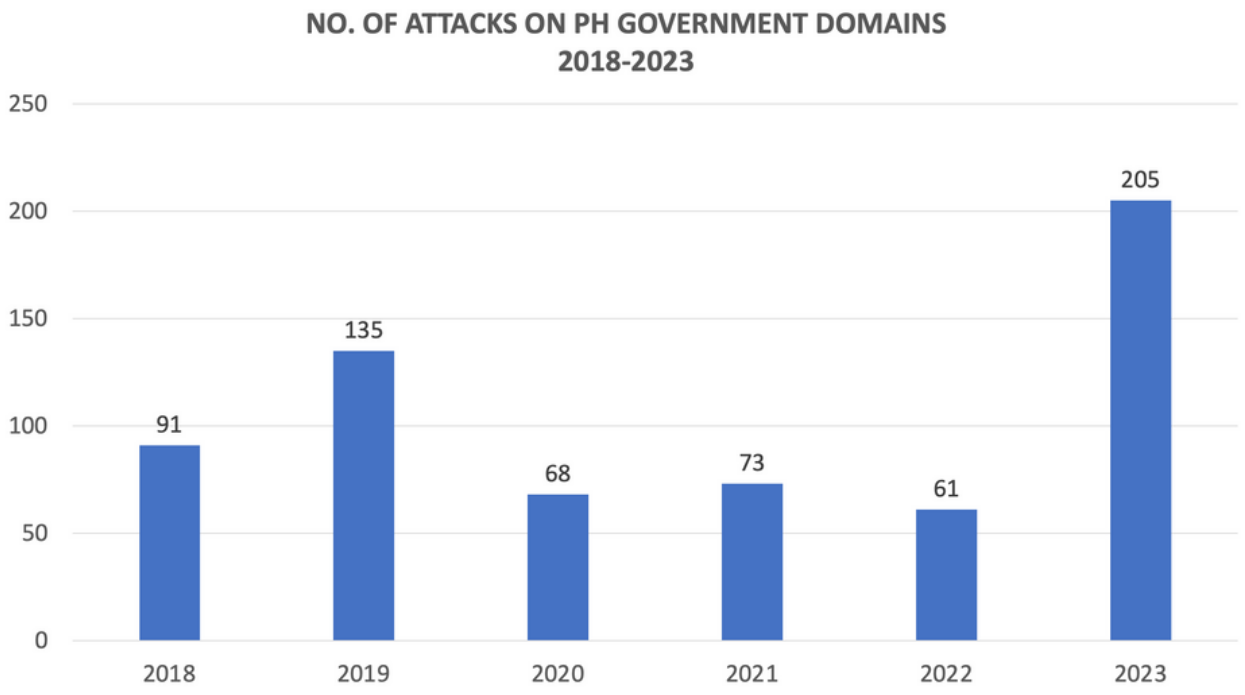


figure 3

PH Military has been working on their security structure for the past years, as it is understood that they are a primary target when it comes to cybersecurity threats. Looking closely at the number of domains breached that is owned by the PH military, there is a clear influx year on year from 2018 to 2023 which tells that the consistency in updating skills and knowledge base when it comes to new cybersecurity threats is an immediate need. (*As shown in figure 4.*)

Threat actors do advance their cybersecurity threat arsenal, which should be the main motivation for its largest target; which is military domains, creating the need for the PH military to do the same. Thus, the data presented in this collection of data analysis shows that there are gaps that are needed to be addressed accordingly for each institution type, in order to level the playing field between threat actors and the institution administrators in keeping their data secured.

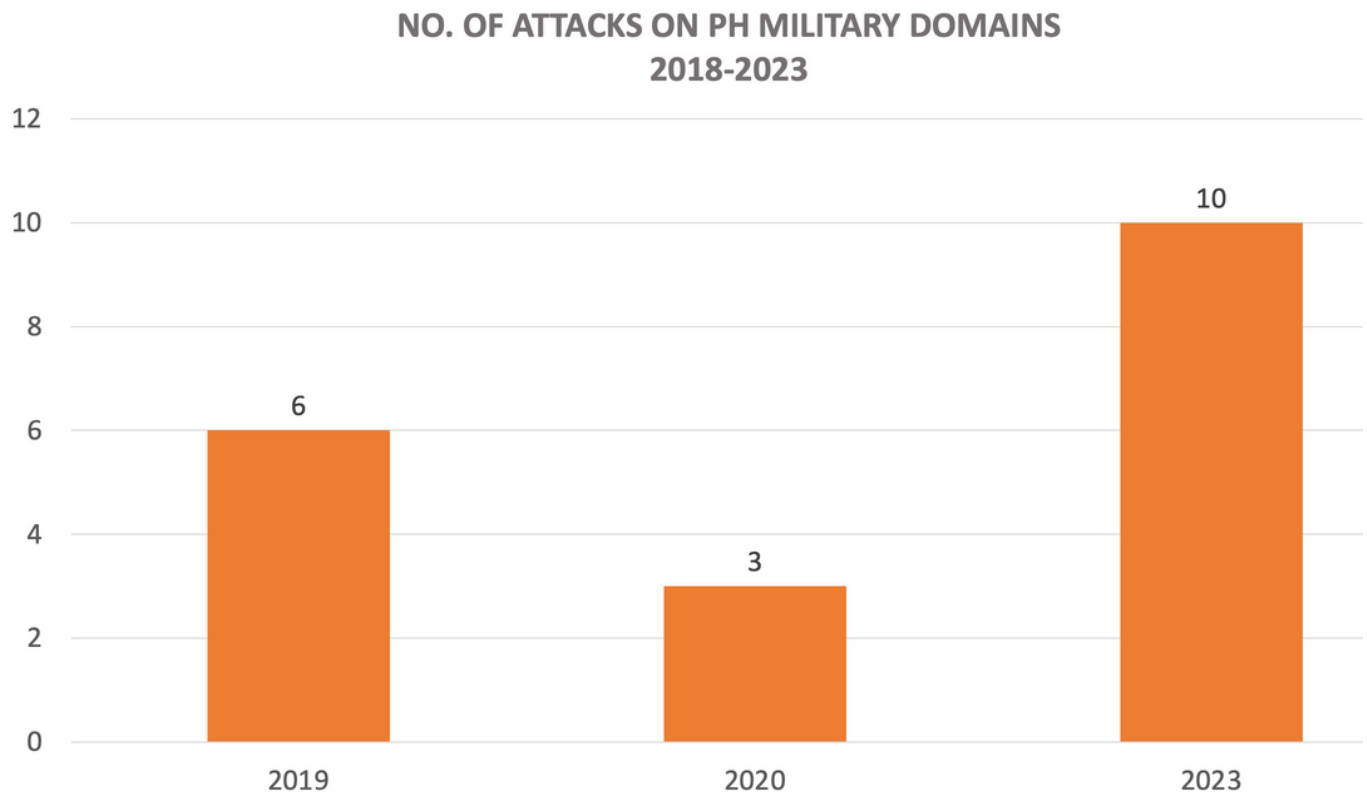


figure 4

CONCLUSION

Despite efforts of different institutions to protect their data, there are gaps that need to be addressed. Numerous reasons on why implementation of security measures are placed in the back burner such as awareness, knowledge base, consistency, budget restraints, lack of skill or capabilities and more plays a huge factor into this.

Addressing such challenges will create a huge benefit for these institutions when it comes to cost savings in information system security preservation. Having the ability to protect data is a strong suit that needs not to be taken for granted, as information is the most vital capital of any type of service or business, no individual would subscribe to any aim or goal to fully transition progressive activities if known to be unreliable in keeping their data, which impedes progress in developing better services.

Millions in cost to be paid due to leaked data is one of the top priorities to be addressed. Unknowingly for any institution that compensating impacted customers/subscribers, investing over and over to new security measures without being cognizant to the actual purpose of why having it in place is of importance, setting up of incident response efforts, investigation costs, fees for incompliance to the regulations or laws pertaining to data security and legal fees addressing the aforementioned possible costs can become debilitating and even damaging for any institution's reputation.

RECOMMENDATION

To address cybersecurity threats effectively, a multifaceted approach is necessary. Here's a comprehensive set of recommendations:

1. **Investment in Cybersecurity Infrastructure**: Allocate resources to enhance national cybersecurity infrastructure, including robust firewalls, intrusion detection systems, and secure communication protocols.

2. **Collaboration with Private Sector**: Foster collaboration between government agencies and private sector entities to share threat intelligence, best practices, and resources. Public-private partnerships can enhance cybersecurity resilience.

3. **Cybersecurity Education and Training**: Promote cybersecurity education at all levels, from elementary schools to professional training programs. Educated citizens and skilled professionals are essential for combating cyber threats.

4. **Regular Vulnerability Assessments**: Conduct regular vulnerability assessments and penetration testing to identify weaknesses in critical infrastructure and systems. Proactive measures can prevent potential cyber attacks.

5. **Promotion of Cyber Hygiene Practices**: Encourage individuals and organizations to practice good cyber hygiene, including regular software updates, strong password management, and awareness of phishing tactics.

RECOMMENDATION

6. **Legislation and Regulation**: Enact legislation and regulations to establish cybersecurity standards for critical infrastructure sectors, such as energy, finance, and healthcare. Compliance requirements can help mitigate risks.

7. **Investment in Research and Development**: Invest in research and development to innovate new cybersecurity technologies and strategies. Advancements in areas such as artificial intelligence and quantum cryptography can bolster defenses.

8. **Incident Response Planning**: Develop comprehensive incident response plans at the national, regional, and organizational levels. Prompt and coordinated responses are critical to minimizing the impact of cyber attacks.

9. **Promotion of Cybersecurity Culture**: Foster a culture of cybersecurity awareness and responsibility among citizens, businesses, and government agencies. Emphasize the importance of cybersecurity as a collective responsibility.

10. **Encourage Responsible Vulnerability Disclosur**e: Establish mechanisms for responsible disclosure of cybersecurity vulnerabilities to facilitate timely patching and mitigation. Encouraging ethical hacking and bug bounty programs can incentivize researchers to report vulnerabilities rather than exploit them maliciously.

REFERENCES

Archives Zone-H https://www.zone-h.org/archive

Incidents CSIDB https://www.csidb.net/csidb/search/?q=Philippines

Breaking News - Hacking Securityaffairs
https://securityaffairs.com/?s=philippines

Kaspersky

Fortinet

Palo Alto