POLICY BRIEF

Strengthening Data Privacy and Cybersecurity Awareness for CSU Employees

Author:

Dorothy M. Ayuyang & Richard R. Ayuyang
Cagayan State University-Gonzaga Campus, Gonzaga Cagayan Philippines
dorothyayuyang@csu.edu.ph, richard.ayuyang@csu.edu.ph
Contact Number: +63 9177925717

🔍 Key Findings and Policy Implications

- The study identified a strong positive link between the extent of implementation and employee awareness to data privacy and cybersecurity measures of the university.
- These findings imply that as the organization implements a strong data privacy and cybersecurity measures, the more aware employees become. This highlights the importance of a clear and positive approach to security within the University.

- Policy implications from the findings include:
  a. Investing in cybersecurity awareness programs by conducting training with a focus on the latest threats and best practices;
  b. Establishing communication and reporting channels for cybersecurity concerns;
  c. Enforcing compliance to security policies by conducting a periodic review and update data privacy and cybersecurity policies.

Background

This policy on cybersecurity outlines the requirements for safeguarding the university's information and technology assets from unauthorized access, use, disclosure, modification, destruction, or other malicious activities.

The policies that would be attributed to the result of the study having a positive link between the extent of implementation and the awareness of data privacy and cybersecurity among employees includes: Access Control, Security Awareness Training, Data Classification and Incident Response.

This policy would strengthen the knowledge and habits of employees when it comes to data privacy and cybersecurity. By improving awareness, the university can better protect its information, reduce risks and create a safer digital environment for everyone.

This policy applies to all faculty, personnel and employees which role is to manage and process data of the University.

Research Objective

- Generally, the objective of the study is to investigate the state of data privacy and cybersecurity knowledge and practices of the employees of Cagayan State University with a focus on evaluating the status of implementation and employee awareness.
- Specifically it aimed to:
  - examine the demographic profile and online activities of the employees;
  - assess the status of implementation of data privacy and cybersecurity acts;
  - assess the level of awareness of employees to data privacy and cybersecurity;
  - determine the potential differences in awareness based on demographic variables;
  - investigate the relationship between the status of implementation and level of awareness; and
  - identify key areas for recommendations based on the evaluation of results that could contribute to the development of a university cybersecurity system.

Methodology

The study used a quantitative research design utilizing descriptive correlational approach to find out how employees' awareness of data privacy and cybersecurity is related to how well these are being implemented in the university. It also looked at the employees' demographic profile and their online activities.

A total 279 employees were randomly chosen from the university's 1009 regular employees. This sample size was selected to ensure reliable results, using standard guidelines for accuracy.

To check the relationships between different factors, the study used statistical tools like Pearson, Spearman, and Point-Biserial correlation – depending on what fit best for each type of data. The results were considered significant if they met the standard 0.05 level of significance.
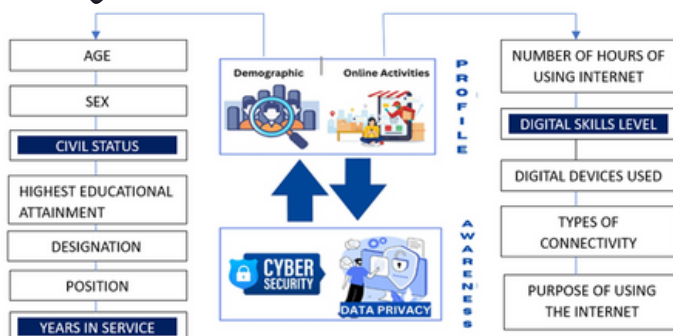
Key Findings

Figure 1. Result of Awareness and Demographic Profile.

Awareness and Demographic Profile
Single employees showed higher cybersecurity awareness than married ones.
Awareness and Online Activities
Greater internet skills were linked to higher cybersecurity awareness

Figure 2. Result of Implementation vs Awareness.

Implementation and Awareness to Data Privacy and Cybersecurity
There is a strong positive link between implementation level and employee awareness to data privacy and cybersecurity.

Cagayan State University
Knowledge & Technology Management and Publication Office
RDE Bldg., CSU- Andrews Campus Caritan Sur, Tuguegarao City, Cagayan

SCAN ME

Recommendations

- Strengthen cybersecurity training programs to enhance employee awareness, especially targeting groups with lower awareness levels.
- Regularly update and review data privacy and cybersecurity policies to keep up with evolving threats and best practices.
- Promote digital skills development to increase familiarity with cybersecurity risks and practices
- Adjust awareness programs based on employee backgrounds, since some groups may need more support than others

Figure 3. Dr. Dorothy M. Ayuyang delivering a lecture on Data Privacy Awareness.

Conclusions

Strengthening data privacy and cybersecurity awareness among employees is essential to protecting the university's information and digital systems. As organizations enhance their security measures, employee awareness also improves.

Key factors contributing to this include improved digital skills through training, evident management support, periodic review and regular policy updates, and proper resource allocation to support implementation of security policies. By educating employees and promoting responsible online practices, this policy supports culture of security and helps reduce risk of data breaches.

Overall, the findings highlight that investing in both awareness and implementation helps build a more secure and informed workforce.

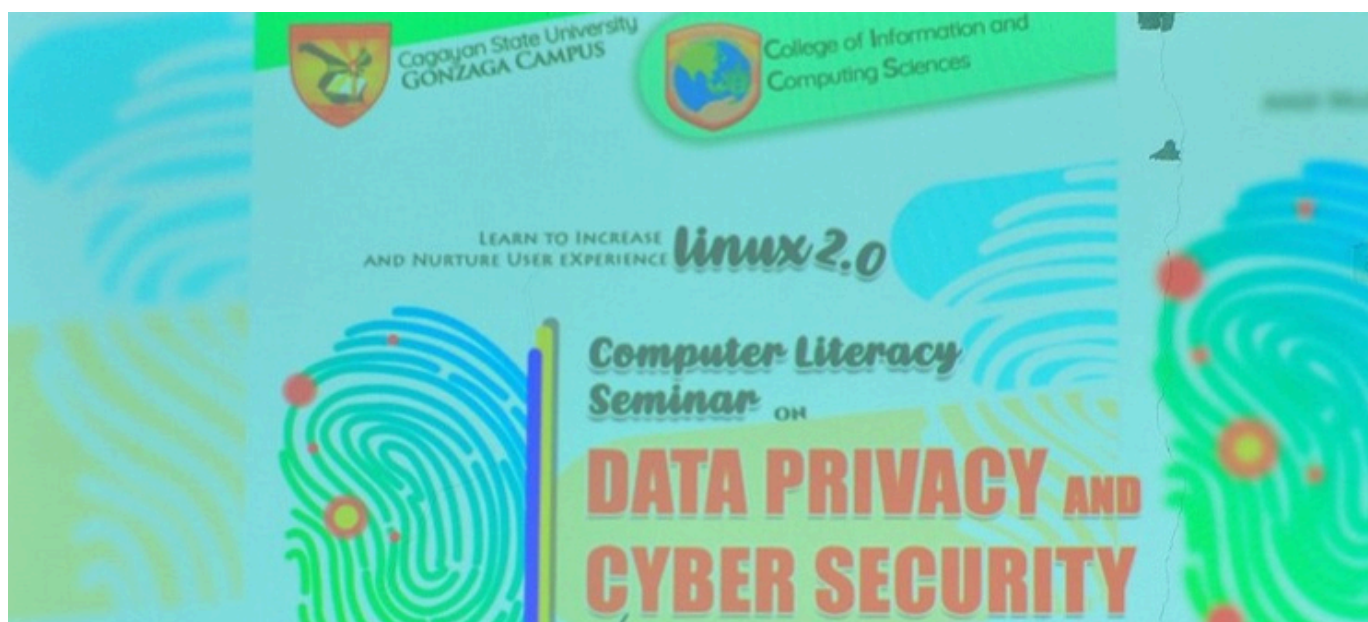## Regulatory and Legislative Agencies/ Organizations Benefiting from the Results

Figure 4. The Faculty of CICS conducts Computer Literacy Seminar on Data Privacy and Cyber Security.

SCAN ME

References

National Privacy Commission. (2012). Republic Act No. 10173 – Data Privacy Act of 2012. Public Law, 1–26. https://www.privacy.gov.ph/data-privacy-act/
Interpol. (2020, August).

Cybercrime: COVID-19 impact. Interpol. https://www.interpol.int/en/News-and-Events/News/2020/COVID-19-cybercrime

Department of Justice. (2015). Rules and regulations implementing Republic Act No. 10175. Official Gazette. http://www.officialgazette.gov.ph/downloads/2015/08aug/20150812-IRR-RA-10175.pdf

Dorothy M. Ayuyang ,Richard R. Ayuyang (2024). Extent of Implementation and Level of Awareness of Employees on the Data Privacy and Cybersecurity Acts of Cagayan State University. Frontiers in Health Informatics, 13 (7) 1074-1086

Scribd. (n.d.). Cybersecurity and cybercrime: Philippine perspective [PDF file]. https://www.scribd.com/document/327711600/Cybersecurity-and-Cybercrime-Philippine-Perspective

Figure 5. Dr. Richard R. Ayuyang discusses Cybersecurity Awareness to employees.

Figure 6. Coaching and Mentoring Co-employees on cyber threats.

Figure 7. Dr. Suetos delivering a lecture on Computer Ethics.

Figure 8. Mr. Cacao discusses about hacking during the seminar on Data Privacy.

EDITOR'S NOTE

This policy brief is based on results of the CSU-funded project "Extent of Implementation and Level of Awareness of Employees on the Data Privacy and Cybersecurity Acts of Cagayan State University" This project was implemented by the Cagayan State University - Gonzaga Campus. The CSU - Gonzaga Campus project team is composed of Dorothy M. Ayuyang & Richard R. Ayuyang (OP-5005-SO-2022-03-206).

EDITORIAL BOARD

SCAN ME