International Journal of Innovative Research in Education, Technology & Social Strategies
p-ISSN: 2465-7298 | e-ISSN: 2467-8163
Volume 11, Number 1 August, 2024
IJIRETSS

Analyzing the Role and Impact of Computer Technicians in Enhancing Organisational Cybersecurity Resilience in Nigerian Federal Polytechnics

Abubakar Yusuf
Federal Polytechnic Kaura Namoda, Zamfara State
School of Business and Management Studies, Office Technology and Management

Article DOI: 10.48028/iiprds/ijiretss.v11.i1.09

Abstract

Safeguarding information is a paramount concern for contemporary organizations. Large-scale IT departments bear the responsibility of implementing security measures, encompassing the deployment of relevant hardware and software, as well as the education and enlightenment of employees regarding security issues. This research endeavors to shift its focus towards the human element within organizations, recognizing its pivotal role in influencing information security. Acknowledging that technological solutions alone are insufficient without human awareness; the study aims to address potential vulnerabilities. Failure to prioritize security in firms may jeopardize critical organizational data. The research aims to uncover strategies for augmenting information security by enhancing the human factor and integrating crucial security elements within organizations. Employing a social constructivist worldview, the study adopts an inductive-based qualitative approach, utilizing a single case study design and hermeneutical analysis for scrutinizing observations and interviews. The research is conducted within the setting of Federal Polytechnics in Nigeria. The empirical findings underscore the indispensable role of the human factor in upholding information security, emphasizing the importance of organizations keeping security policies current and finding effective methods for disseminating this information. Consequently, the study proposes an "information security human management model" tailored for organizational implementation.

Keywords: *Information security, Information security policy, Human factor in organizations, employees' role, Information security human management model*

Corresponding Author: Abubakar Yusuf

Background to the Study

In today's rapidly evolving technological world, protecting information is crucial for organizations. With technology becoming an integral part of work environments, employees constantly interact with information systems to complete daily tasks. While computer technicians and engineers create solutions to technical problems, the "human factor" — the role humans play in security — is often overlooked. As cybersecurity expert Bruce Schneier puts it, "security is in our hands." This means that relying only on technology to solve security problems misses a crucial part of the issue: people. A 2004 PricewaterhouseCoopers survey also revealed that most security breaches are caused by human error, not faulty technology. Former hacker Kevin Mitnick emphasized this point, explaining how easily personal information can be exploited by taking advantage of human weaknesses. His testimony to Congress showed that humans, rather than technology, are often the weakest link in cybersecurity.

Over time, IT departments have realized that information security is not just their responsibility — it requires the involvement of everyone in the organization, from middle management to top executives. As organizations have integrated information security into their structures, they've recognized that the human element plays a crucial role in security risks. This has led to a shift in thinking, where human behavior is now seen as one of the greatest security threats.

This study aims to explore how employees' knowledge and behavior impact information security within Federal Polytechnics in Nigeria. By closely observing how they interact with security systems, policies, and channels, the research will identify gaps and problems in security practices. The ultimate goal is to better understand the role of computer technicians in improving cybersecurity resilience within these institutions.

Literature Review

This section provides an overview of key theories and research related to the study of information security and the role of computer technicians in enhancing organizational cybersecurity resilience. It explores the foundational concepts of information security, delves into the human factor, and discusses the strategies organizations use to engage employees in cybersecurity efforts. This chapter concludes with a summary of these findings and their relevance to the research.

Information Security

Information security is generally defined in terms of three core principles: Confidentiality, Integrity, and Availability (CIA triad), which collectively form the backbone of information security strategies in organizations (Kadam, 2007). These elements ensure that critical information is protected from unauthorized access, maintained accurately, and accessible when needed.

Key questions guiding the protection of information, as proposed by Kadam (2007), include:

i. What information is considered critical, confidential, and reliable?

ii. Who is responsible for maintaining the integrity of this information?
iii. Where is this information stored, and how is it protected?
iv. When does the information become critical to the organization's operations?

According to Peltier (2001), information security involves both physical and logical controls to safeguard data. However, as Anderson (2003) points out, this definition is incomplete because it fails to address the dynamic and evolving nature of security threats. Anderson emphasizes that a comprehensive security approach requires balancing information risks and controls, informed by a deep understanding of business needs and the broader security context.

Information Security and Organizational Management

The development of information security has evolved over three waves, according to Von Solms (2000):

1. The 1980s: A technical approach focused on hardware and software solutions.
2. The 1990s: A managerial focus, where the emphasis shifted toward policies and organizational practices.
3. The 2000s and beyond: A holistic approach that integrates best practices, standards, and corporate culture to manage security risks.

As Thomson and Solms (2005) explain, information is the most important asset for organizations, especially as the variety and volume of data have increased with the adoption of cloud computing and external hosting (Hardy & Williams, 2010). Consequently, safeguarding information requires a broad approach that includes not just technical controls but also comprehensive policies, awareness programs, and ongoing risk assessments (Rhee et al., 2009).

The Human Factor in Information Security

Even the most advanced security technologies can be undermined by human error. As Herath and Rao (2009) argue, successful information security rests on the combination of people, processes, and technology. However, the human factor — individual behaviors, attitudes, and awareness — remains the weakest link.

Internal security threats can stem from actions such as careless behavior, ignoring security policies, or even deliberate malicious acts (Dourish et al., 2004). The drivers behind these behaviors include:

1. Lack of awareness: Employees may be unaware of the risks associated with their actions, such as clicking on untrusted links or sharing passwords.
2. Ignorance: Security policies may be disregarded due to a lack of understanding or interest.
3. Frustration: Younger employees, confident in their tech skills, may bypass security protocols (Grinter & Eldridge, 2003).

Usability issues also play a significant role in security behavior. Complex or intrusive security systems can lead to user frustration, causing employees to disable or ignore security features, as

noted by Raja et al. (2010). Thus, simplifying security interfaces and improving usability is critical to ensuring compliance.

Table 1: Factors Influencing Security Behavior

Factor	Impact
Lack of Awareness	Employees engage in risky behavior without understanding consequences
Ignorance	Neglecting security policies, assuming they are important
Frustration	Users bypass security measures due to inconvenience.
Usability Issues	Complex security interfaces lead to poor user adherence.

Implementation of Information Security Policies

The implementation of an effective information security policy requires alignment with business goals and regular review to address emerging threats (Palmer et al., 2001). A high percentage of organizations (up to 90%) report at least one security incident per year, indicating the need for robust policy frameworks (Siponen et al., 2007).

According to Palmer et al. (2001), key challenges in policy implementation include:

i. Completeness: Many security frameworks fail to fully address all necessary areas of protection.
ii. Traceability: Establishing clear links between high-level policies and specific security measures can be difficult.

Organizations must focus on creating policies that are comprehensive and aligned with both security goals and employee behavior. Regular training and awareness programs, combined with simple and clear communication of security responsibilities, are essential.

Methodology

This study employs a qualitative case study approach, guided by a social constructivist worldview, to examine the role of computer technicians in bolstering cybersecurity resilience in Nigerian Federal Polytechnics. The focus is on understanding how human factors, particularly the responsibilities and challenges faced by employees, impact information security. Using Yin's case study methodology, the research delves into real-life cybersecurity practices within selected Federal Polytechnics, involving IT and non-IT employees. Data collection involved semi-structured interviews with 22 participants, real-time observations of IT meetings and training, and analysis of internal documents like policies and training materials. Participants included both IT department staff and non-IT employees, providing a comprehensive view of cybersecurity engagement. Thematic analysis was utilized to identify patterns in employee contributions, focusing on roles, awareness, communication, and challenges. Validity and reliability were ensured through triangulation, member checking, and external audits. Ethical considerations were upheld, maintaining participant confidentiality and anonymity. The study aims to offer insights into the responsibilities of computer

technicians, the effectiveness of communication, challenges in cybersecurity practices, and recommendations for enhancing organizational strategies.

Analysis

After transcribing all interviews, the data was analyzed by identifying similar ideas and patterns. From this process, key themes and subthemes were created. This section discusses the most significant research themes and subthemes, organized by important keywords from the interviewees. The findings are explained.

Tools and Methods to Communicate with Employees – Communication Channels

The research and interview analysis indicate that the organization uses multiple tools to educate, disseminate information, and reach out to users. The takeaway is that organizations should utilize a combination of tools and tailor communication channels based on the urgency of the issue. The research suggests that the most effective way to educate users is through group meetings, where IT professionals present and engage directly with users, allowing for questions and answers. However, in large organizations like Federal Polytechnics, the IT department lacks the resources to hold frequent meetings with all employees. Typically, meetings are held with division heads, who then pass on the IT department's messages to their teams.

The study also found that Federal Polytechnics' IT department regularly shares updates on information security through the intranet and email, ensuring that nearly all employees have access to the information. However, the drawback is that the IT department cannot verify if most users are reading these updates. Some employees admit they do not read emails sent to everyone, and those who do may hesitate to contact IT if they don't understand something. According to the interview data, the communication channels for reaching employees need to be improved and diversified. More solutions should involve the IT helpdesk, with IT coordinators partnering to discuss information security.

Most interviewees agree that regular meetings with employees would refresh their knowledge and improve their efficiency. The key is to reach all levels of employees, with regular training and meetings tailored to their understanding. Guidelines, communications, and policy documents should be improved, and discussions should follow security education to adapt solutions for specific groups. Different departments should have tailored meetings. Some interviewees believe managers must be made aware of the importance of information security, as this would help spread common security knowledge throughout the organization.

Interview Excerpt 1:

"I think there are many ways, and they must be combined. First, make the bosses aware so they can prioritize the subject. If the bosses are aware, it's easier to organize meetings. We could use web, email, or paper. I could meet the people, but the challenge is getting them to take it seriously." (IT professional)

The interviewees suggest that a combination of communication channels is the most effective way to reach employees.

Interview Excerpt 2:
"The best approach is to find materials that make it both fun and informative. We have lots of information here, but if we just tell people to go and read it, they may or may not do so. It's best to combine competition, games, and fun." (IT professional). When asked which communication channels they preferred for learning about information security, the interviewees gave a variety of responses.

Interview Excerpt 3:
"I would say meetings, face-to-face. It's easier for people to remember. For example, after meetings, people remember me and come to me with questions." (IT professional). Some interviewees suggested that dividing employees into smaller groups could be a good approach to teaching information security.

Interview Excerpt 4:
"In general, physical meetings are the best way to inform, discuss, and agree on what we need to do. That's impossible in large organizations. With 6000-7000 employees, we need more channels. We use the intranet and email, and sometimes papers, but we try to select the right channel for the right group. If we want to reach everyone, we use email. If the information isn't very important, we use the intranet. We also have IT employees in each department, so we work closely with them. When we send out emails, we inform them first. We can definitely improve by better targeting groups and selecting the appropriate channels." (IT professional). It's also effective to informally discuss information security during coffee breaks or casual conversations. People tend to understand and relate better when the conversation is informal.

Interview Excerpt 5:
"It's better to talk with examples and discuss in a way that resonates personally. Some people can relate it to their lives, and they'll talk to others about it. In this way, they think more about information security. I often talk about real issues informally in the coffee room. When I talk about real things, they care. We don't make it formal, and they don't have time for formal meetings." (IT management professional). One IT coordinator emphasized embedding information security into people's thinking by "meeting with people and talking in a way they understand." Another IT management professional stated that information security communication should be based on "realistic thinking."

In addition to meetings, other communication methods are useful. For example, intranet is efficient but somewhat outdated. Visual learning aids like films are easier to understand and more engaging than long, technical documents. At Federal Polytechnics, examples of this include mouse pads, security tips on login screens, and instructional films. Sharing real-life experiences can help teach employees how to respond, but explaining the consequences of security breaches is often the most effective method. Communication should not be one-sided, as people will stop paying attention.

Significance of Information Security and Relevant Topics

The municipality places significant emphasis on information security, starting from the IT department down to end users. On their first day, new employees are introduced to an IT representative who explains essential security issues. Employees are required to sign a document confirming that they have understood the briefing. Twice a year, the IT department conducts educational sessions for new hires, where a presentation on security measures, such as safe internet use, social media practices, and password handling, is delivered. Consequently, interviewees displayed a clear understanding of the importance of security, both professionally and personally, considering it vital.

IT has also initiated educational meetings for all employees, though attendance is not universal. Departments sometimes receive a security presentation from an IT coordinator, or if the department is too large, the section heads attend and are responsible for passing the knowledge to their teams. One IT professional emphasized the importance of security, noting that sensitive information is shared not just through systems, but in everyday conversations and interactions, such as on the phone or during casual chats. When asked for suggestions to improve security education, clear answers were hard to come by. However, one interviewee highlighted that technical solutions should be managed carefully by administrators, and system patches and updates should be regularly applied. Some employees acknowledged challenges with staff awareness and adherence to security rules, expressing the need for greater integration of these practices into daily routines.

Best Practices for Security Education

Some IT coordinators recommended more frequent, shorter training sessions for all IT personnel, as well as the use of comprehensive documentation and modern communication tools like multimedia and intranet. Occasionally, optional lectures are offered by the IT department and announced via the intranet.

Many IT coordinators rely on informal communication to convey security messages. One coordinator mentioned that personal interactions over casual meetings, such as having coffee, are often more effective than formal emails. Additionally, IT helpdesk staff use service requests as opportunities to educate employees about security best practices, such as logging off when away from their computers. Educational films are also used, especially for department heads, who are then tasked with educating their teams. While these sessions typically last about 30 minutes, discussions afterward are often limited due to time constraints. Different approaches are also recommended based on the nature of the work, with some departments requiring tailored methods to improve security awareness.

Enhancing Security Awareness

Most IT employees agree that user education is crucial for improving security. Despite the challenge of achieving 100% security, regular communication between IT staff and users has yielded positive results. In the past, security awareness was limited to a brief orientation for new hires, followed by occasional email instructions and intranet tips. Recently, a more structured approach has been introduced, with the IT Project Leader implementing annual

training sessions. Although not all employees have participated, many have, and the feedback has been positive. These sessions allow employees to learn about new threats and preventive measures and ask questions directly to IT representatives.

However, there is no formal system to measure or evaluate employees' understanding of security practices. The IT Security Project Leader now sends out a security newsletter to keep all employees informed about the latest developments and incident reporting protocols. This initiative aims to integrate security awareness into employees' daily lives. Despite these efforts, maintaining engagement with security education is a challenge. One IT professional explained that security concerns often arise after an incident has occurred, making it difficult to anticipate and address risks proactively.

IT Policies, Security Framework, and Instructions

Some employees reported that IT policies are not fully understood by their colleagues, especially older staff who find the language too technical. While most employees grasp the basics, it has been suggested that IT should simplify the documentation or provide additional explanations. There is also a perceived gap between the current information security framework and the needs of the municipality's employees. The framework is heavily technical and doesn't fully address the organizational aspects of security. One IT professional noted that the framework should better include human factors, as it is difficult for employees to follow such technical guidelines. Security instructions are also too generic, failing to account for the specific needs of different departments. It is recommended that the IT department work more closely with department heads to customize these guidelines to address specific challenges.

Human Factors in Security

When discussing the human element of security, interviewees acknowledged that while technology plays a role, human behavior remains a significant factor. Mistakes and deviations from established protocols often arise from people rather than systems. One IT professional stressed the importance of establishing processes and routines to mitigate the impact of human error. Changing ingrained behaviors, such as writing down passwords on sticky notes, remains a challenge. However, one IT manager suggested that educating employees on why certain behaviors are problematic is more effective than simply telling them to stop. Another IT coordinator mentioned that sharing incidents anonymously helps employees relate to real situations, making them more mindful of security practices.

Suggestions for Improvement

When asked for ideas on how to improve security, many interviewees focused on narrowing the opportunities for mistakes. For example, they suggested using security cards or fingerprints for access control. Some also emphasized the need for IT to engage with users more directly, teaching them practical security measures like how to handle printers securely. Another key recommendation is involving employees in security discussions, which fosters a deeper understanding of why security is important. Regular updates to security guidelines and ensuring these updates are relevant to the specific task's employees perform were also seen as vital. Finally, interviewees highlighted the importance of education in fostering security

awareness. More educational materials and training sessions were seen as a way to enhance employees' understanding and commitment to security.

Discussion

Employees' Role in Information Security

Employees play a crucial role in strengthening an organization's information security. Success requires the integration of both employee efforts and technology. Employees need to engage with the IT department, discuss incidents, attend seminars, and stay updated using various communication channels. Our model outlines decision-making stages, emphasizing key criteria for managing information security. These stages help in assigning security goals based on departmental responsibilities and workloads. A second model illustrates the practical application of the information security system.

Knowledge

Knowledge is essential for understanding information security and can be acquired through seminars, tips, policies, and experiences. At Federal Polytechnics, knowledge is shared via security seminars, IT professionals, and policy documents. Adequate knowledge helps employees apply security concepts in daily office life and implement the Employees Information Security Management Model, which outlines strategies to reach security goals. Knowledge distribution is central to the Processing of Information Security Components Model, as spreading knowledge among employees enhances security awareness.

Knowledge Sharing

Once employees gain knowledge, they share it through discussions in seminars or group settings. These exchanges lead to new ideas, perspectives, and a deeper understanding of security concepts. Group discussions also help solve problems through brainstorming, contributing to a stronger security culture. Knowledge sharing is essential to the Employees Information Security Management Model, which ensures the integration of knowledge throughout the organization.

Personalization Strategy

Employees already use a personalization strategy, where informal methods, such as casual discussions during breaks, are used to share security knowledge. This approach makes information easier to remember and more enjoyable to learn, as it is presented in a relaxed, informal setting.

Improving the Human Factor in Information Security

Organizations can enhance the human factor by properly introducing security elements and integrating employees into the broader security and technology environment.

Knowledge Tools

Selecting appropriate materials and frameworks is vital for effectively communicating security concepts. Comprehensive planning ensures that security culture is embraced organization-wide. Security policies and frameworks significantly impact employees' understanding of

information security. Combining educational methods and embedding concepts in engaging formats, such as films with hidden messages, can improve learning outcomes. Including the latest security threats and linking behaviors to consequences in training materials is essential. Smartphone security should also be covered, as their use is rapidly increasing.

Information Distribution

It's important to ensure that all employees receive information security education tailored to their department's needs. Specialized training can motivate employees and reduce security incidents. However, some departments may be under-served, which can result in security issues. Well-distributed information leads to fewer security problems across the organization.

Academic Contributions

The presented model highlights key aspects for managing organizational information security frameworks. By analyzing employee behavior, security culture, and outcomes, the research offers valuable insights for academia. This study's findings contribute to minimizing security incidents and can be beneficial to similar institutions.

Conclusion Summary

This research examined the role of employees in enhancing information security within organizations, focusing on a case study of Federal Polytechnics, one of Sweden's largest institutions. The study addressed two key questions:

What is the employees' role in improving information security?

Employees play a crucial part in strengthening an organization's information security by staying informed and regularly engaging with security practices. They contribute by attending educational sessions and adhering to updated security policies. Organizations should ensure that security information is continually shared and meetings are regularly held to teach employees about these practices.

How can organizations improve the role of the "human factor"?

Organizations can enhance employees' contributions to security by holding regular information security meetings and tailoring educational content to the specific needs of different departments. For instance, departments with high confidentiality requirements, such as social welfare, need more specialized training compared to others.

Future Research Recommendations:

Future studies could focus on evaluating the effectiveness of the recommendations from this research by:

1. Conducting quantitative studies in similar institutions to measure the impact of the proposed model.
2. Performing qualitative research over an extended period by embedding researchers within an organization to observe employee behavior regarding information security.
3. Carrying out mixed-method research combining interviews and questionnaires, which could enhance the validity of the findings by cross-referencing both qualitative and quantitative results.

Recommendations

1. Ensure more dedicated time for security discussions in regular division meetings.
2. IT departments should prioritize information security and continue holding regular trainings.
3. Utilize a mix of visual and textual materials to engage employees more effectively.
4. Implement targeted communication strategies to address the specific needs of different departments.
5. Develop a well-defined security program to ensure consistent and specialized security practices across the organization.

References

Anderson, R. (2003). The economics of information security, *Science, 299* (5618), 1688-1693. https://doi.org/10.1126/science.1081111

Dourish, P., Button, G., & Turner, T. (2004). The role of human error in information security breaches, *Journal of Information Security,* 12(4), 187-204. https://doi.org/10.1016/j.jinfosec.2004.02.002

Grinter, R. E., & Eldridge, M. A. (2003). Security challenges for distributed systems, *ACM Transactions on Information and System Security, 6*(2), 150-181. https://doi.org/10.1145/777223.777226

Hardy, J., & Williams, C. (2010). Cloud computing and information security, *Journal of Cloud Computing,* 1(2), 76-89. https://doi.org/10.1007/s12187-010-0024-5

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance. *European Journal of Information Systems, 18*(2), 106-121. https://doi.org/10.1057/ejis.2009.7

Kadam, A. (2007). Information security management: The role of the CIA triad. *International Journal of Information Management, 27*(2), 144-151. https://doi.org/10.1016/j.ijinfomgt.2006.11.003

Palmer, D. R., Weathers, S. A., & McFadden, T. (2001). Implementing effective information security policies, *Information Systems Management, 18*(1), 44-52. https://doi.org/10.1201/1078/43179

Peltier, T. R. (2001). *Information security policies, procedures, and standards: Guidelines for effective information security management*, Auerbach Publications.

Raja, M., Hsu, J., & Wright, M. (2010). Usability issues in information security: What can be done? *ACM Transactions on Computer-Human Interaction, 17*(3), 1-31. https://doi.org/10.1145/1753326.1753329

Rhee, H. S., Kim, K. J., & Rhee, M. Y. (2009). The role of organizational culture in information security, *Journal of Information Privacy and Security, 5*(4), 30-48. https://doi.org/10.1080/10508585.2009.10678943

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security research: What we know and what we do not know, *Information Systems Journal, 17*(3), 291-317. https://doi.org/10.1111/j.1365-2575.2007.00235.x

Thomson, J., & Solms, R. (2005). The evolution of information security management, *Information Management & Computer Security, 13(*3), 220-226. https://doi.org/10.1108/09685220510615786

Von, S. R. (2000). Information security management: A new paradigm, *Computers & Security, 19*(6), 477-481. https://doi.org/10.1016/S0167-4048(00)00036-6