Research on the Influence of the Network Security Behavior of the Employees in the Enterprise on the Overall Security of the Enterprise and Countermeasures

Tian Tian

Peken Global，Hong Kong China 999077

Abstract: With the advancement of digital transformation, enterprises are faced with the double risks of external network attacks and internal employee behaviors.Employees 'illegal behaviors, such as password sharing and email misoperation, have become an important hidden danger to enterprise network security.This paper studies the role of network security in precision marketing and its impact on enterprise performance, focuses on the analysis of the impact of employee network behavior on the overall security of enterprises, and puts forward the corresponding management countermeasures.Through the questionnaire survey, this paper discusses the effectiveness of the behavior-oriented information security management mechanism, including the normalization of security training, behavior audit system and security score system.The research shows that the network security behavior of employees directly affects the enterprise security, and strengthening the management mechanism and safety culture can effectively reduce the risk.Finally, it is suggested that enterprises should shift from "technical response after the event" to "behavioral mechanism intervention," incorporate employee behaviors into the information security protection system, and improve overall security and enterprise performance.

Keywords: Network security; Precision marketing; Employee behavior; Information security management; Enterprise performance

Introduction

With the rapid development of information technology and the acceleration of digital transformation, the security risks faced by enterprises have become increasingly complex.In the past, threats such as external hacker attacks, virus intrusions, and malware have been a major source of enterprise network security.However, in recent years, the network behavior of employees in enterprises has gradually become an important reason for information leakage and system vulnerabilities.Whether it is unintentional or malicious, employee non-compliance behavior can bring huge security risks to enterprise information systems.Employees 'weak password use, account sharing, failure to update software in time, disclosure of sensitive information and other behaviors often provide hackers with an opportunity to invade.Internal personnel behavior mistakes and management loopholes, can also be a trigger for large-scale security

incidents.

1 Literature review

1.1 Research progress of network security behavior

With the continuous development of information technology and the enterprise's attention to network security, the research on the network security behavior of employees has gradually attracted the attention of the academic community [1].Network security behavior can be generally divided into two categories: compliance behavior and violation behavior.Compliance behavior refers to employees 'compliance with the enterprise's network security policies and regulations in their daily work, and taking proactive measures to ensure the security of information systems, such as using complex passwords, regularly updating software and following data protection procedures.And irregularities is refers to the staff not in accordance with the provisions of the operation, may lead to corporate network security vulnerabilities, such as the use of weak passwords, free to share account information, click on the unknown link, etc.Employees 'violations are often one of the causes of network security incidents, and may even lead to major security incidents such as enterprise data leakage, system paralysis and other serious security incidents[2].

In the formation mechanism of compliance behavior, TPB model (theory of planned behavior) and HBM model (health belief model) are widely used.The TPB model holds that the behavior of employees is affected by their behavior attitudes, subjective norms and perceived behavior control.Employees 'attitudes towards cybersecurity behaviors and the social pressures they feel in the organization (e.g., peer behavior, leadership requirements, etc.) will directly affect the implementation of their security behaviors.HBM model emphasizes the impact of employees 'perception of cybersecurity risks and their self-efficacy on compliance behavior.Employees are more likely to demonstrate compliance if they believe that non-compliance with safety regulations will have serious consequences and they believe they are capable of complying with safety regulations.Relevant literature also shows that the employee's personal habits, work pressure and awareness of the enterprise security policy, will affect the occurrence of compliance and violations to a certain extent [3].

1.2 Research on insider threat and organization security

As an important part of enterprise information security, insider threat has been paid more and more attention in recent years.Insider threats typically refer to security risks from people inside the organization, such as employees, outsourcers, partners, and so on.According to research, insider threats can be divided into three categories: unintentional disclosure, malicious compromise, and privilege abuse.Inadvertent disclosure is usually the disclosure of information by an employee through negligence or lack of security awareness without malicious intent.For example, an employee sends sensitive information to the wrong email address or loses a device that contains sensitive data.Malicious destruction is the deliberate destruction or tampering of company data, or even data theft, by employees or other insiders for their own personal purposes.Privilege abuse is refers to the

employees use their authority to access and abuse should not be exposed to sensitive information, usually involving data theft, information manipulation and other behavior, this behavior not only directly endanger the enterprise information security, may also lead to serious legal and financial consequences [4].

The role identity of employees plays an important role in the security boundary within an organization.The research shows that the role identity, the position authority and the contact degree with the enterprise information system of the employee are closely related to the security risk that may cause.Because high-level employees have access to more sensitive information and critical systems, their misbehavior or malicious behavior can cause greater harm to the enterprise.At the same time, although the low-privilege employees have less access to information, their work habits and security awareness are weak, and they may also provide hackers with the opportunity to invade through technical loopholes or management mistakes.The lack of trust between employees and cross-departmental communication, can also be a potential factor in internal threats.Therefore, in the organization's security management, we must consider the role of employees, the design of a reasonable authority management mechanism to ensure the effective protection of information security boundaries [5].

2 Theoretical basis and research model construction

2.1 Theory of planned behavior (tpb) and employee network behavior

Theory of Planned Behavior (Theory of Planned Behavior, TPB) is put forward by Ajzen, aims to explain the relationship between the intention of individual behavior and actual behavior.TPB consists of three core dimensions: behavioral attitude, subjective norms and perceived behavioral control, which are widely used in the research of employee network security behavior.

Behavioral attitudes refer to the employee's positive or negative attitude towards compliance with the cybersecurity policy.Employees are more likely to behave in compliance if they believe that compliance will have a positive effect (e.g., data security, productivity gains), whereas employees who believe that these actions are unnecessary or burdensome may ignore the rules and result in non-compliance.

Subjective norms are employees 'perceptions of expectations and pressures in their surroundings.Employees are more likely to comply if they feel the support and expectations of management and colleagues, and may have a tendency to ignore safety regulations if the company has vague requirements for safe behavior and poor supervision.

Perceived behavior control is the employee's confidence in whether they can effectively perform safe behaviors.Employees are more likely to demonstrate compliance if they believe they have the skills and resources to implement security measures, and may ignore security measures if they lack confidence or believe the rules are difficult to implement.

2.2 Model design of employee behavior influence mechanism

Based on the TPB model, this paper designs a mechanism model to analyze the influencing factors of employees 'network security behavior.The model assumes that the network security behavior of employees is not only

affected by the external environment (such as security policy, management mechanism), but also by the role of employees 'own security awareness and self-efficacy.

The main variables of the model include perceived organizational support, safety awareness, self-efficacy and institutional constraints.Perceived organizational support refers to the employee's perception of the security support provided by the enterprise, such as training and technical support. Studies have shown that employees with strong sense of organizational support are more likely to show positive security behaviors.Security awareness is the awareness of employees on the importance and potential threats to network security. Employees with high security awareness are more inclined to comply with security regulations.Self-efficacy is the confidence of employees in their ability to effectively perform safety behaviors, and employees who think they have the ability are more likely to comply with safety regulations.Institutional constraints refer to the rules and regulations formulated by enterprises to ensure network security and their enforcement. Clear and strict security policies can encourage employees to comply with regulations.

The path model proposed in this study assumes that perceived organizational support, security awareness, self-efficacy and institutional constraints affect employees 'behavior attitudes, subjective norms and perceived behavior control, and ultimately affect employees' network security behaviors. Specifically, the sense of organizational support and safety awareness enhance the behavior attitude and subjective norms of employees, thus improving compliance behavior; self-efficacy and institutional constraints help employees overcome obstacles to implementing safe behavior by enhancing their perceived behavior control.

3 Empirical study design and data analysis

3.1 Questionnaire design and variable measurement

In order to explore the impact of employee's network security behavior on the overall security of the enterprise, this study adopts the questionnaire survey method to collect data.The survey respondents were mainly employees from IT, operations and administration positions.These positions represent different functional areas of the enterprise's employee groups, can fully reflect the network security behavior and security awareness of employees.Employees with different industry backgrounds and enterprise sizes were selected to ensure the representativeness and universality of the sample.

The sample size of this study was 500 valid questionnaires with a final recovery rate of 85%.During the sample collection process, random sampling was adopted to ensure that employees in all positions and departments had the opportunity to participate.The questionnaire is issued through the online questionnaire platform to ensure the anonymity and confidentiality of the data.

The questionnaire design is based on the existing literature and theoretical framework, and the Likert five-point scale is used to measure.The scale covers many variables, such as employees 'network security awareness,

security behavior, organizational support, institutional constraints, self-efficacy and so on.Specifically, the employee's network security behavior includes two dimensions: compliance behavior and violation behavior, which measures the compliance degree of employees to the enterprise network security policy and common violation behaviors (such as using weak password, abusing authority, etc.).Security awareness is measured by employees 'perception of cybersecurity risks and personal responsibility.Self-efficacy measures whether employees think they can effectively implement safety measures, and perceived organizational support is evaluated by employees 'perception of company safety resources and support.

Table 1 Measurement Indicators and Scales

variable	measurement index	Gauge Type
cyber security practices	Comply with security regulations, use strong passwords, update software regularly, and so on	Likert 5-point scale
safety awareness	Awareness of the importance and potential risks of cybersecurity	Likert 5-point scale
self-efficacy	Do you think you can effectively comply with safety regulations and take appropriate safety measures	Likert 5-point scale
perceived organizational support	Perception of security training, technical support, and policy support provided by the enterprise	Likert 5-point scale
institutional constraints	Clarity, strictness and enforcement of corporate security policies	Likert 5-point scale

Table 1 summarizes the measures of each variable used in this study and the Likert five-point scale used.Each measure is related to a different dimension of employee cybersecurity behavior, ensuring the comprehensiveness and effectiveness of the questionnaire.

3.2 Analysis of empirical results

In the data analysis stage, the reliability and validity of the collected data were tested first.The reliability test used Cronbach's alpha coefficient to ensure good internal consistency of the scale.

Table 2 Reliability test results of each variable

variable	Cronbach's α
cyber security practices	0.83
safety awareness	0.80

self-efficacy	0.77
perceived organizational support	0.81
institutional constraints	0.79

Table 2 shows the reliability test results for each variable.As can be seen from the table, the Cronbach's alpha coefficients of all variables were greater than 0.7, indicating that the scale has high reliability and can reliably measure the relevant variables.

The KMO values were used to verify that the data were suitable for factor analysis.A KMO value greater than 0.6 indicates that the data is suitable for factor analysis.The KMO value for this study was 0.82, indicating that the data are suitable for further regression analysis.

Regression analysis is to explore the path relationship between the variables, and analyze the influencing factors of employees 'network security behavior.Through the regression model and path coefficient calculation, the study finds that perceived organizational support, security awareness, self-efficacy and institutional constraints have a significant impact on employees 'network security behavior.Specific path coefficient is as follows:

Table 3 Regression Analysis Results

path	path coefficient	p-value
Perceived Organizational Support → Cybersecurity Behavior	0.35	<0.001
Security Awareness → Cybersecurity Behavior	0.28	<0.001
Self-efficacy → Cybersecurity Behavior	0.22	<0.01
Institutional constraints → network security behavior	0.30	<0.001

Table 3 shows the results of the regression analysis.As can be seen from the table, all path coefficients are significant, indicating that organizational support, security awareness, self-efficacy and institutional constraints have a positive impact on employees 'network security behavior.The path coefficients were 0.35 and 0.28 respectively, which indicated that the perceived support of the enterprise and the awareness of the importance of safety were the important factors to promote the employees to comply with the safety regulations.

In order to further analyze the differences between different departments and positions, this paper also conducted an interactive item analysis.The results showed that IT and operations employees showed high compliance with cybersecurity behaviors, while administrative employees showed relatively low compliance.This indicates that the differences in cybersecurity behaviors among employees in different functional positions are closely related to their job responsibilities and work contents.

Through these empirical results, this paper further verifies the impact of each variable on employees 'network security behavior, and provides data support for enterprises to optimize

security management strategies.

4 Analysis of the impact of employees "Network behavior on enterprise's overall security

4.1 The direct impact of employee behavior on system security

In the enterprise information security management, the network behavior of employees is a crucial factor.Improper behaviors of employees, such as failure to comply with network security regulations, password sharing, use of weak passwords or incorrect email operations, may provide opportunities for network security vulnerabilities and directly threaten the confidentiality of enterprise information systems and data.especially that use of password share and weak passwords, are often the breach for attacker.Using social engineering, hackers can gain access to employee login credentials, take control of critical systems, or steal sensitive data.Data breaches can also occur when employees mistakenly click on phishing links or send sensitive information to the wrong recipient while processing email.

Typical cases can help us understand the impact of employee behavior on safety.For example, a company employee clicked on a malicious email link, causing the company's intranet to be hacked and sensitive data to be leaked, resulting in financial losses and reputation damage.Another example is when employees use simple passwords (e.g., 123456) and share account information, leading to hacking and data loss.The above cases show that the daily operation and behavior habits of employees directly affect the safety of the enterprise.

4.2 The moderating role of management mechanism and organizational culture

Employees 'network behavior is not only influenced by individual safety awareness, but also regulated by organizational management mechanism and corporate culture.The security climate in corporate culture directly affects the network security behavior of employees.If the enterprise attaches great importance to the construction of safety culture, the safety behavior of employees will be more compliant by formulating clear safety regulations and strengthening training.Enterprises with a strong security culture usually establish strict security management mechanisms to ensure that employees comply with network security policies and reduce security risks.

Organizational support plays an active role in the standardization of employee behavior.Enterprises to provide the necessary security tools, technical support and training, help to improve the safety awareness and self-protection ability of employees. Management involvement is also crucial, regular training and strengthen the supervision mechanism can improve the compliance of employees, especially in the cross-departmental collaboration, managers need to pay attention to coordinate the safety cooperation of various departments, to ensure the overall safety protection of the enterprise.

5 Countermeasure suggestions and management path optimization

5.1 Establishing behavior-oriented information security management mechanism

With the complexity of enterprise

information systems and the increase of network security threats, it is particularly important to establish an information security management mechanism oriented by employee behavior.The clarity of the system is the basis of the implementation of this mechanism.Enterprises should refine the list of network behavior responsibilities, clarify the safety behavior requirements of employees in daily work, especially the specific provisions on sensitive data access and processing, password management, mail processing, etc..These specifications should be tailored to the responsibilities of different positions to ensure that each employee has a clear understanding of his or her responsibilities.Normalization of security training is an important means of improving staff's network security behavior.The enterprise shall regularly carry out safety training, especially accurate customized training for employees of different posts.For example, IT staff should focus on training to fix security vulnerabilities, while the average employee should focus on the discipline of day-to-day behavior, such as setting strong passwords and avoiding mail scams.By strengthening the safety awareness and compliance behavior of employees, enterprises can effectively reduce the security risks caused by employee behavior.

5.2 Construction of employee behavior monitoring and incentive mechanism

In order to effectively control the network security behavior of employees, enterprises should build a perfect employee behavior monitoring and incentive mechanism.The introduction of behavior audit system and real-time early warning mechanism is the key to improve the monitoring effect.Behavior audit system can record the behavior of employees in the network environment in real time, find abnormal operation and analyze in time, so as to take measures to prevent potential security incidents quickly.For example, when an employee accesses unauthorized sensitive data or performs a high-risk operation, an audit system can immediately trigger an alert to notify security personnel for action.Real-time early warning mechanism through data analysis and pattern recognition, to predict and identify the safety risk behavior of employees may exist, to take preventive measures in advance.Enterprises should also establish a security score system to incorporate employees 'network security behaviors into performance appraisal.Employees who comply with safety regulations will receive safety credits, which will be linked to annual performance.In this way, organizations can motivate employees to actively comply with safety regulations, provide positive feedback, and create a positive safety culture.

5.3 Building an organization-level safety culture system

Building an organization-level security culture system is a long-term measure to ensure enterprise network security.Enterprises should build a safety culture through leadership demonstration and employee participation. Senior management should play an exemplary role in daily work, participate in network security training, care about the safety awareness of employees, and demonstrate the importance of network security through practical actions.Employees should actively participate in the construction of enterprise safety culture, safety management Suggestions are put forward, and jointly promote the improvement and

implementation of enterprise safety standards.In order to strengthen the implementation of safety culture, enterprises should also enhance the safety awareness of all employees through the visualization of internal risks.For example, regularly publish internal security incident reports, notify recent security incidents and consequences, and help employees learn lessons through case review.Regular security incident review and risk notification can improve the safety sensitivity of employees, encourage employees to pay more attention to details in their daily work, and prevent potential security threats.By building this positive security culture, enterprises can form a common security awareness among all employees, so as to improve the overall level of information security.

Conclusion

Employee behavior is the risk source that can not be ignored in enterprise information security management.Under the background of digital transformation, enterprises not only face the threat of external network attack, but also the network behavior of internal employees may have a serious impact on information security.Whether it's unintentional operational error or intentional malicious behavior, employee behavior can become a source of network security vulnerabilities, which in turn affect the enterprise's information systems, data security and overall operations.Therefore, strengthening the management of employees 'network security behavior has become one of the core elements of enterprise information security protection.

Enterprise network security management means should be gradually from the "post technical response" to the "behavior mechanism intervention" transformation.The traditional security management mode lays particular stress on the technical defense of external attacks, ignoring the control of internal staff behavior.With the increase of internal threats, enterprises should adopt a comprehensive security management strategy, through the specification of employee behavior, enhance safety awareness, establish effective behavior audit and monitoring mechanism, from the source to reduce the occurrence of security incidents.Behavioral mechanism intervention can not only effectively prevent violations, but also improve the safety compliance of employees, and further protect the overall information security of the enterprise.In a word, enterprises should incorporate the management of employees 'network security behaviors into the overall security framework to realize the dual protection of technology and behavior, so as to improve the network security resilience and operational efficiency of enterprises.

References

[1]Fredrik K ,Shang G .Guest editorial: New frontiers in information security management[J].Information & Computer Security,2025,33(1):1-4.

[2]Liu Z .Intelligent classification of computer vulnerabilities and network security management system: Combining memristor neural network and improved TCNN model.[J].PloS one,2025,20(1)77-78.

[3]Okonkwo C ,Awolusi I ,Nnaji C , et al.Privacy and security of wearable internet of things: A scoping review and conceptual framework development for safety and health management in construction[J].Computers & Security,2025,150-175.
[4]Saini H ,Singh G ,Dalal S , et al.Enhancing cloud network security with a trust-based service mechanism using k-anonymity and statistical machine learning approach[J].Peer-to-Peer Networking and Applications,2024,(prepublish):1-26.
[5]Kumar S U ,Kapali C S B ,Nageswaran A , et al.Fusion of MobileNet and GRU: Enhancing Remote Sensing Applications for Sustainable Agriculture and Food Security[J].Remote Sensing in Earth Systems Sciences,2024,8(1):1-14.

Author Biography：Tian Tian，Male，Mongolian，from Hebei Province，China，research focuses on Business Administration.