

I. INTRODUCTION

Our world is entering a strange divide: people are excited about the revolutionary advances in the age of big data, while they are also worried about data security and privacy issues. Policy, laws, standards, products, and academic research show unprecedented enthusiasm for the innovation and security of big data. But the dazzling voices have plunged people into confusion and data panic. If we fail to find a clear idea and find a balance between development and security around big data, we may lose the biggest development opportunity in human history, or fall into the biggest security crisis.

For any organization, data is a very valuable asset. Therefore, protecting the data from unauthorized access is critical. Data breaches, audit failures, and failure to comply with regulatory requirements can all lead to a damaged reputation, loss of brand equity, damaged intellectual property, and fines for violations. Under the EU's Common Data Protection Regulation (GDPR), data leaks could result in organizations facing fines of up to 4% of their global annual revenues, causing significant economic losses. Sensitive data includes personally identifiable information, financial information, health information, and intellectual property rights. Organizations need to adopt data protection measures to avoid data leakage and help achieve compliance.

II. CORRELATION THEORY

The International Organization for Standardization (ISO) defines the security protection of computer systems as "the security protection for the technology and management established and adopted by the data processing systems, protecting the computer hardware, software, and data from being damaged, changed, or leaked for accidental or malicious reasons."

At the Gartner 2017 Security and Risk Management Summit, analyst Marc delivered a speech titled "Data Security Situation 2017" and mentioned, "Data Security Governance" (Data Security Governance). Marc compares it to "the eye of the storm" to describe the important position and role of data security governance (DSG) in the field of data security.

The basic definition of data security governance is: "Data security governance is not only a set of product-level solutions combined with tools but from the decision-making level to the technical level, from the management system to the tool support, from top to bottom, through the complete chain of the entire organizational structure. All levels within the organization need to reach a consensus on the objectives and purposes of data security governance to ensure that reasonable and appropriate measures are taken to protect information resources most effectively."

This can be understood as: ensuring the data availability, integrity, and confidentiality of various strategies, technologies, and activities, including enterprise strategy, corporate culture, organization construction, business processes, rules and regulations, technical tools, and so on, on various aspects that improve the data security risk response process, control the data security risk or minimize the impact of the risk.

Data security strategies and technologies can identify the requirements of information sensitivity, importance, and compliance, and then apply appropriate protection measures to protect these data

resources. Data security governance involves multiple technologies, processes, and practices to ensure data security and prevent unauthorized and illegal access. At the same time, data security governance should also focus on protecting personal sensitive data, such as personal identity, contact information, or critical business intellectual property.

Data security governance is specifically designed to protect enterprise data through the development of data security strategies and processes involving data, business, security, technology, management, and other aspects. Data security governance is a subset of data governance that can be carried out either within or independently under the data governance framework. Data security governance supports the development of data governance from the strategic and tactical level, through the implementation of secure access, classification, and compliance use of data security strategies, to achieve business goals, such as meeting the requirements of laws and regulations, protecting consumer privacy, etc.

Data security governance is mainly centered around the vulnerability of data security, developing targeted strategies for various risks to reduce the risks to an acceptable degree. In the whole process of data security governance, the most important thing is to develop an appropriate data security strategy.

The enterprise data security governance system is a whole based on risk and strategy, with operation and maintenance systems as the link, and technical systems as the means, organically combining the three with data asset infrastructure, which runs through the whole life cycle of data.

The enterprise data security governance system mainly includes the following five parts to ensure the availability, integrity, confidentiality, and compliance use of the whole life cycle of the data.

- A. Data security governance objectives: emphasize the consistency of security objectives and business objectives. The goal of data security governance is to ensure the security of data, ensure the compliance use of data, and escort the realization of business goals.
- B. Data security management system: mainly including the organization and personnel, data security responsibility recognition strategy, data security management system, etc.
- C. Data security technology system: it mainly includes the sensitive data identification of the whole data life cycle, data classification, classification, data access control, data security audit, etc.
- D. Data security operation and maintenance system: mainly including regular audit strategy, dynamic protection strategy, data backup strategy, data security training, etc.
- E. Data security infrastructure: Focus on the physical security and network security of the host where the data is located.

In the architecture of the data security governance system, the data security strategy is the core, the data security management system is the foundation, the data security technology system is the support, and the data security operation and maintenance system is the application. Data security strategy is formulated through a management system, created by the technical system, and executed through a security operation and maintenance system.

Data security governance is a special branch of data governance. Its governance system can be structured under the overall framework of data governance, or it can be built separately to implement

special governance of data security. Data security governance is a strategic strategy level, emphasizing the framework of strategy, organization, and policy, defining the strategy of data governance, form a cooperative order, so that data security management from "disorder" to "orderly", from "rule of man" to "legal system".

The network security system is the highest level of the abstract concept of a network security guarantee system, which is composed of various network security units, security strategies, security technology, security management, and so on according to certain rules to jointly achieve the goal of network security.

Its characteristics include wholeness, which is, the overall, long-term perspective to achieve security, each unit has an interaction, constraints, dependence, Form man and machine integration; comprehensiveness, which is, based on multi-dimensional and multi-layer security threats, constructing network security functions such as protection, detection, response, and recovery; cooperativity, which is, the various security mechanisms interact, build a systematic network security scheme; process nature, which is, for the protected objects, provide a process-type network security mechanism, covering the whole life cycle of the protected object; adaptability, which is, the dynamic evolution, adapt to the changes and demands of cyber security threats. The network security system is conducive to systematically resolving the network security risks, ensuring continuous operation and minimizing the loss; strengthening the network security awareness of organizations and individuals; protecting the network assets of the organization and maintaining the competitive advantages of the organization; facilitating the certification of the network security management system, proving that the organization can guarantee important information and enhance the visibility and trust of the organization.

Look at what the security standards and frameworks are.

Well-known safety standards and frameworks include ISO27000 Series, NIST, COBIT, and ITIL.

NIST is a security framework proposed by the US government to monitor and control a company's security capabilities. NIST documents have two significant advantages: they are free and available for a while; so they have been extensively reviewed and updated by government and industry professionals. However, NIST does not consider the cost of implementing security standards, so NIST is rarely used except for US government affairs.

The ISO27000 series and the COBIT are both safety standards and frameworks that do not include specific implementation details.

Among them, the ISO27000 series is one of the internationally recognized safety standards. It provides best-practice guidance for highly compatible security systems and information security management. The ISO27000 series is also one of the most widely cited and frequently discussed safety models, published initially as the UK standard BS 7799, later as ISO / IEC 17799, and then as ISO / IEC 27002.

The initial purpose of ISO / IEC 27002 is to provide guidance on managing information security for individuals responsible for the security plans of their organizations. According to 27000.org, the standard was “intended to provide a common basis for developing organizational security standards

and effective security management practice and to provide confidence in inter-organizational dealings”

COBIT (Control Objectives for Information and related Technology) provides a framework for internal control for security managers, which is more focused on internal control and audit.

Founded in 1992 by the Information Systems Auditing and Control Association (ISACA) and the IT Governance Institute (ITGI), COBIT provides five principles focusing on IT governance and management in the organization: meeting the needs of stakeholders; covering enterprise end to end; applying a single, integrated framework; adopting a holistic approach; and separating governance from management.

ITIL (Information Technology Infrastructure Library) has been made into a series of books, each covering an IT management topic. Since it contains a detailed description of many important IT-related practices, ITIL customization to many IT organizations is a standard framework for improving the quality of service, and security is only a factor affecting service quality. Therefore, ITIL will think more about how to improve the efficiency of the company's research and development and management, giving only relatively basic attention in terms of confidentiality, availability, and integrity.

The above safety standards and frameworks, in addition, guide the safety construction of enterprises, and also provide evaluation services. The purpose of the evaluation, on the one hand, is to help the company realize its own safety level, and on the other hand, it is also a benchmark for the company's external publicity. In China, for example, the most popular test is the ISO27001. Companies have passed the ISO27001 test to show their users and partners that their safety level has reached a relatively mature level. This is a manifestation of external publicity.

III. CASE ANALYSIS

One of the best and most sought-after blends in the world, Jamaican coffee, is offered for sale by CoffeeBlend. CoffeeBlend is widely present throughout the world. To provide IT services to its employees and customers, the business leverages cloud services. Nearly 95% of the company's network, according to estimates, is wireless. To advertise its activities, the company also maintains a sizable web and social media presence. The company has recently faced intense pressure to let both its personnel and customers utilize their personal devices to access the company's network and resources due to its sizable staff and multinational customer base. The company's top priority is the security of the personal data of its employees and clients. The business is also worried about safeguarding its priceless intellectual property. The corporation places a high focus on information security, but things are chaotic. Their demand for security is not covered by any existing policies.

In this part, investigate the current situation and demand of the CoffeeBlend network, understand the current situation and security requirements of users' network information system, conduct an in-depth demand analysis based on the six aspects of ensuring network information security, and formulate the

security mechanism of the network information security scheme. After the analysis of the security mechanism and related technologies, the relevant security technologies to be adopted in the scheme are determined, including anti-virus, host control, network security audit, identity authentication, unified security management, information encryption, firewall, intrusion detection, etc. Secondly, according to the security mechanism of the company, design the network information security system. Then, according to the company's network information security scheme, the implementation scheme of each subsystem is described in detail, and the system linkage characteristics are elaborated.

CoffeeBlend's network information system interacts with the group headquarters network information system through WAN, During the process of information transmission, Facing the threat of eavesdropping, tampering, and destruction of information; At the company's man and WWAN boundaries, The man is faced with foreign malicious attacks, virus invasion and unauthorized access from the wan; The subnet of various service users and their internal computer terminals are faced with threats such as user counterfeiting and virus invasion; The company has a number of computer terminals, Random input and output behavior of computer terminal information, It may also lead to the loss of core information within the company. In order to improve the security of the company's network information system, we use various technical means to achieve the goal of network information security, that is, to ensure the reliability, availability, confidentiality, integrity, non-repudiation, and controllability of the transmission, exchange and stored information in the network information system. According to the company network status and demand research, at present, the network information security system needs to have key prevent eavesdropping, prevent information forgery, information loss or damage, attacks, antivirus, unauthorized access, prevent user fake, denial, denial of service security protection ability, so as to improve the security of the company network information system. Requirements analysis is shown in the table.

TABLE I. REQUIREMENT ANALYSIS OF THE NETWORK INFORMATION SECURITY SYSTEM OF COFFEEBLEND

	confidentiality	integrity	facticity	nonrepudiation	serviceability	reliability
anti-eavesdrop	√					
Anti-information forgery			√	√		
Prevent information loss or damage		√	√	√	√	
Affordable attack	√			√	√	√
antivirus					√	√
Non-authorized access	√			√	√	
Prevent users from counterfeiting	√	√	√	√	√	
Anti-denial				√		
Anti-refusal service					√	√

In order to meet the security needs of the company network information system, to ensure that the network information security system with eavesdropping, information forgery, information loss or destruction, against attacks, antivirus, unauthorized access, user counterfeiting, denial, denial of service security protection ability, the company information security system should have information encryption, digital signature, intrusion detection, network behavior audit, virus detection and protection, access control, host control, user authentication, log audit security mechanism.

Next, on the basis of the relevant information security technology research, combined with the company's network information security mechanism, the architecture structure of the company's network information security scheme was formulated, as shown in Fig. 1.

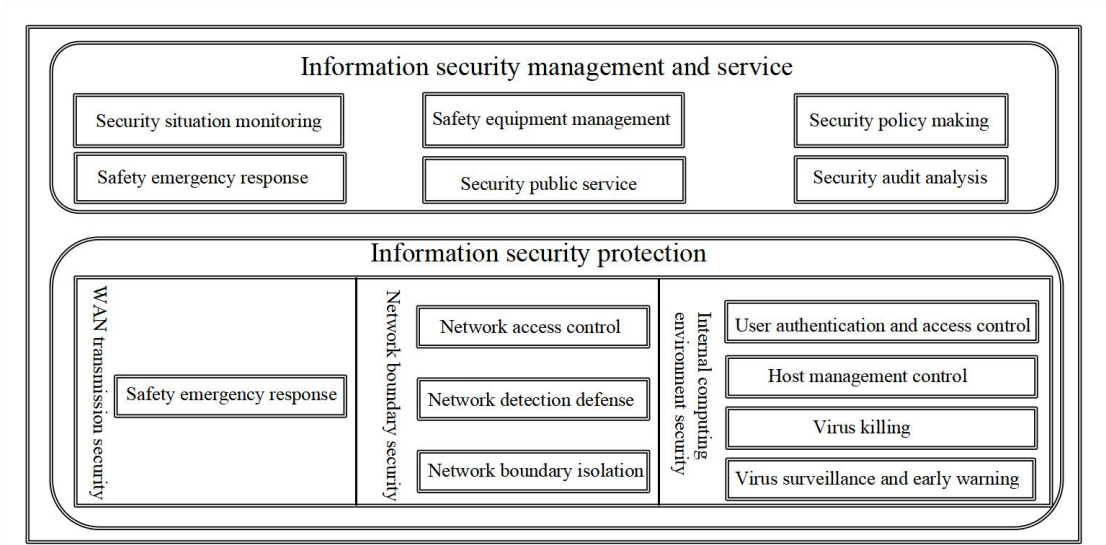


Fig. 1. The architecture of CoffeeBlend Company's information security scheme

The company's network information security system architecture consists of two functions: information security management and service and information security protection.

The information security management and service layer include the following six functional modules: security situation monitoring, that is, monitoring, fusion, correlation analysis, and early warning of the information security situation, to provide a complete information security situation. Safety equipment management, that is, to provide centralized and unified management for all kinds of safety equipment (systems), including the management of equipment status, system resources, usage conditions, and all kinds of services provided by safety equipment. Security strategy formulation, that is, for different information security management objects, to provide the formulation and distribution of the corresponding information security strategies. Safety emergency response, that is, provides emergency response measures and carries out information security emergency response processing. Security public service, that is, to provide all kinds of information security public services, such as virus library, patch library upgrade, update services, all kinds of information security software, hardware upgrade services, and update services. Security audit analysis, that is, through the audit records and statistical analysis of information security data, provides the ability to track and trace security events.

The information security protection layer includes the following three areas of security protection: WAN transmission security, that is, WAN information confidentiality provides encryption and decryption functions for information transmission in the WAN, mainly using network IP encryption and decryption technology to prevent information from being lost or stolen in the process of WAN transmission. Network boundary security, including network access control, network detection and prevention, and network boundary isolation. Network access control and network boundary isolation mainly provide access control and network isolation for the internal resources of external users' access area, so as to prevent external attacks, protect the security and security of boundary isolation, and protect their own network, which is mainly realized by firewall. Network detection and prevention provides analysis, detection, record, and alarm for the transmitted information content, mainly using intrusion detection technology. Internal computing environment security, that is, including user authentication and access control, host management control, antivirus and virus warning, and software system security. User authentication and access control provide the identity authentication of the network access users. The host management control provides the operation behavior control means for the terminal to prevent the illegal input and output of information, and mainly adopts the input and output control technology of the terminal host. Antivirus and virus early warning provide virus detection and killing of the computer system, network monitoring, analysis, and early warning, mainly using computer antivirus software technology and virus early warning and detection technology. The client software system achieves the purpose of protecting the server and the terminal by troubleshooting and improving the vulnerabilities of the server and the terminal operating system, and mainly adopts vulnerability scanning technology to achieve it.

Through the relevant information security technology to the architecture in-depth research, designed the company's network information security scheme. The company's network information security scheme is composed of wide area network transmission security protection, network boundary security protection, information security management nodes, and internal computing environment security protection.

The WAN transmission security protection subsystem consists of IP security machines deployed between the company's man and the WAN. When the information is exchanged with the man of the company, the information transmitted by the WAN is not leaked and the confidentiality protection of the WAN information transmission is realized.

The network boundary security protection subsystem consists of firewall equipment and intrusion detection equipment. The firewall device is deployed between the WAN and WAN to realize detection and prohibition illegal access from WAN; ensure safe information interaction between the WAN and WAN to prevent illegal access. Intrusion detection devices are deployed on the company's main core switches to identify malicious use of computer and network resources, including intrusion actions from external users and unauthorized activities of internal users.

The information security management node of CoffeeBlend belongs to the secondary information security management node in the information security system of the group. It accepts the services and management provided by the information security management node of the group headquarters, is mainly responsible for the relevant management of the company's information security facilities, and

provides public information security services for the subnets of various business users. The company's information security management node will be the subsystem server or management background access to the network through the access switch, including a unified security management platform, identity authentication, anti-virus, virus warning, host control, and network security audit in six parts. The unified security management platform provides the company's network information system security situation information and security event collection, analysis, and display functions provides the unified management of all kinds of security equipment (systems) and their configuration strategies, provides the emergency response processing to security incidents, and provides the duty management of the security system. The identity authentication system provides the functions of issuing, maintaining, inquiring, and verifying the user certificate information of the company's network information system, and uploads the latest certificate information to the group headquarters certificate server (CA). The antivirus system collects the latest virus library information issued by the primary information security management node of the group headquarters and is responsible for the virus library distribution of the subnets of various business users of the company. The virus early warning system detects and comprehensively analyzes the interactive data on the company's metropolitan area network, monitors the spread of the virus in real time, shows the virus situation of the company's network information system, and manages the virus early warning strategy. The host control system formulates the host control strategy of the company's network information system and controls the behavior of the host, and uploads the control situation to the host control system of the group headquarters; collects the latest patch information issued by the host control system of the group headquarters, and is responsible for the implementation of patch distribution of the business subnets of the company. The network security audit system develops the security audit strategy of the whole network, audits the users' behavior, and uploads the audit information to the security audit system of the group headquarters.

The internal computing environment security protection subsystem includes virus warning probes and security audit probes deployed on the company's core switches, identity authentication USB Key, host control, and antivirus client software deployed in the subnetwork terminals of various business users. Through these security protection facilities, prevent external virus intrusion between the subnetworks of the man and man; collect, identify, and audit legitimate data, and dangerous or illegal network behavior, and support the backtracking and audit of network behavior. Ensure the security of the computer terminal, and prevent users from causing illegal outreach, illegal access, illegal copy, and virus transmission due to incorrect operations.

Finally, the system linkage characteristics are introduced. The first is the antivirus and virus early warning linkage. Single-alone antivirus client software in the face of the network information system of viruses, bad infection situation, there is no way to protect the security of the computer terminal. Users have no way to accurately find the specific spread of viruses through the terminal anti-virus software. The network virus early warning system can solve the above problems. Through bypass access to the core of the network switch, the network of various virus transmission, attacks, and suspicious traffic for real-time monitoring, both realize the global virus detection based on the network, and single virus protection of the traditional anti-virus software complement each other, and implements the fine positioning of network virus behavior and traceability, to assist users to quickly processing network virus events. Whether it is a mail worm, bug worm, password guesses worm, and another worm, or through HTTP, FTP, TFTP, NETBIOS, and another protocol transmission Trojan and other harmful

programs, there is no escape in front of them. For a specific detected security event, by tracing the attack source, attack target, and attack path, accurately locate the affected risk nodes in the network, and lock the IP and MAC address, to assist users in quickly processing the event. At the same time, the discovered virus body and the warning history association query can determine the transmission source and transmission path of the virus in the network. Therefore, the system can not only remove the currently infected virus terminals but also directional detect and kill all the infected terminals in the transmission path in combination with the antivirus client. The virus early warning system ensures the virus detection rate through interaction with the superior cloud server.

The second is the invasion, attack analysis, and positioning. A unified security system can quickly locate network intrusion and network attacks. The unified security management system can receive the attacks or intrusion behaviors reported by the firewall and intrusion detection system. The unified security management system can analyze and count network attacks and intrusion behaviors, associate them, and generate graphics, reports, and other formats for security administrators to view and locate. The system can locate the IP address of the attack and intrusion source, and find the responsible person in the asset management of the unified security management system through the IP address. The security administrator can quickly notify the responsible person to view the status of the computer and assist in locating the security problem.

The third is the operating system patch management. Most of the computer terminals in the company's network information system use Windows systems. The windows are characterized by a lot of patches. If the operating system can not be patched in time, viruses and Trojan horses easily exploit the vulnerabilities of the system to destroy the company's network and computer terminals. The operator also has the possibility of not actively going to the upgrade because of the neglect of the importance of the upgrade patch. In this case, network security has caused some security risks to network security. Therefore, for the management of patches, a complementary solution is adopted, that is, both the host control system and the private cloud security system have patch upgrade management. The patch upgrade function of both systems will notify the user of the patch upgrade in time. If the user does not upgrade for a long time after the notification, report it to the competent unit for processing.

Fourth, the terminal security access strategy setting. In the security access policy of the company's host control system, the terminal must install the private cloud antivirus client software to allow the terminal to enter the company's network. In this way, the security access strategy of the host control system can ensure that each network access terminal is installed with anti-virus software, so as to ensure that the information input terminal of the entire network information system has the virus protection ability.

IV. CONCLUSION

This operation studies the existing defects and remedial measures of CoffeeBlend company's network information security. Although the operation has achieved the expected goal, due to the network information security research environment not qualified, and my knowledge and technology level being limited, this operation only discusses the issues of network information security mentioned above and does not involve all fields of information security, in many details also need to be in-depth research and

improvement. In the new network information security protection means continue to appear at the same time, and more powerful invasion and attack means will also appear. It is also necessary to update network security regulations and standards regularly. Therefore, anyone network information security system can not solve all network information security problems forever. Network information security construction is a very long dynamic change process, which cannot be accomplished overnight. How to give greater play to the role of the network information security system through the management system, how to make the network information security system each subsystem more intelligent linkage, how to make the implementation strategy automatically adjust with the change of the network environment, these are what we need to solve in the future network information security solutions.

REFERENCES

- [1] N. Miloslavskaya and A. Tolstoy, "Application of big data, fast data, and data lake concepts to information security issues," in Proc. IEEE Int. Conf. Future Internet Things Cloud Workshops, 2016, pp. 148–153.
- [2] D. Rawat and K. Z. Ghafoor, Smart Cities Cybersecurity and Privacy. Amsterdam, The Netherlands: Elsevier, Dec. 2018.
- [3] E. Bertino, "Big data security and privacy," in Proc. IEEE Int. Congr. Big Data, 2015, pp. 757–761.
- [4] A. D. Mishra and Y. B. Singh, "Big data analytics for security and privacy challenges," in Proc. Int. Conf. Comput. Commun. Autom., 2016, pp. 50–53.
- [5] Y. Gahi, M. Guennoun, and H. T. Mouftah, "Big data analytics: Security and privacy challenges," in Proc. IEEE Symp. Comput. Commun., 2016, pp. 952–957.
- [6] S. Chandra, S. Ray, and R. Goswami, "Big data security in healthcare: Survey on frameworks and algorithms," in Proc. IEEE 7th Int. Adv. Comput. Conf., 2017, pp. 89–94.
- [7] S. Anandaraj and M. Kemal, "Research opportunities and challenges of security concerns associated with big data in cloud computing," in Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud), 2017, pp. 746–751.
- [8] Y. Wang, B. Rawal, and Q. Duan, "Securing big data in the cloud with integrated auditing," in Proc. IEEE Int. Conf. Smart Cloud, 2017, pp. 126–131.
- [9] S. Bahulikar, "Security measures for the big data, virtualization and the cloud infrastructure," in Proc. 1st India Int. Conf. Inf. Process., 2016, pp. 1–4.