International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 4, Jul-Aug 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Organizational Security: An Introduction

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Our present dive into the digital age has now placed online businesses and most organizations at ever-increasing risks. Cyber threats are becoming increasingly common. Hence the need to urgently take proactive steps to reduce or mitigate the attacks. A way to carry out this is by implementing a robust organizational policy that covers all possible vulnerabilities. Data security is very essential for organizations/businesses that deal with highly sensitive information on a regular basis. The organizations that are conscious of cyber threats and encourage as well as promote the culture of security, and educate their employees on what to do to avoid them can still make mistakes. The paper introduces us to what organizational security is all about, the challenges they face, the benefits, and the way forward.

KEYWORDS: *Organizational security, cyber threats, organizational security policy, data security, information security, operations security, cyber resilience, workplace*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Organizational Security: An Introduction" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-4, August 2024, pp.88-95, URL: www.ijtsrd.com/papers/ijtsrd67127.pdf

IJTSRD67127

INTRODUCTION

Organizational security policy is usually a key document for defining the scope of a business or organization's cyber security efforts. This document contains information on goals, responsibilities, the structure of the security program, compliance, and the approach to risk management. The document is essential for ensuring that everyone knows their role in protecting the organization from cyber threats in the age of digital collaboration. The adoption of the right data security model is therefore critical for organizational security, as shown in Figure 1[1].

HISTORICAL BACKGROUND

Information Security (IS) is designed to protect the confidentiality, integrity, and availability of data from those with malicious intentions of misusing that data. These are set of techniques used for managing the tools and policies to prevent and detect information stored in digital or non-digital media. It is most often confused with cyber security, but IS is a crucial part of cyber security, which refers exclusively to the processes designed for data security. Cyber security is a more general term that includes Information Security as crucial part of itself.

Today and in every individual's life, information plays a significant and important role to us whether as a high profile businessman or a small shop owner. Information is generated in different forms, from our smartphones to transaction receipts and buying patterns, which serves as ways of opportunities for criminally minded people to steal data. This is why information security is a necessity.

The historical evolution of information security is presented as follows:

The 1960s: Offline sites security – During this period, information security was limited to the access points, where computers were stored/located, since they used to be large in sizes requiring large area to be stored and operated. Multiple layers of security were installed over terminals with passwords and other security measures.

The 1970s: Evolution of personal computer and hackers – During this period, there was no massive global network connecting every device that wanted to be connected. Only large organizations, especially governments, were starting to link computers via telephone lines and people started seeking different

ways to intercept the information flowing through those telephone lines in order to steal the data, becoming the first group of hackers.

The 1980s: Evolution of cybercrime – Hacking and other forms of cyber crimes skyrocketed during this period with people finding different ways to break into the computer systems and being no strict regulation against the hackers. Hacking became a booming craze for the youths. Many government and military groups were on the receiving end of these crimes with loss of over millions of dollars from U. S. Banks. In response to this, the government started pursuing the hackers.

The 1990s: "Hacking" becoming an organized crime – After the worldwide web was made available in 1989, and with people starting to put their personal information online, hackers took advantage of this as a potential revenue source, and then started to steal data from people and governments via the web. However, as firewalls and antivirus programs helped to protect against this, the web was mostly unsecured with hackers finding different ways to infiltrate the targets devices.

The 2000s: Cybercrime becoming a serious issue – With the emergence or evolution of hacking and the dangers they posed (which was not as serious as in the late 80's), governments started chasing the cyber criminals. Strong measures were taken against cyber criminals with hackers being jailed for years as punishment for cyber criminal activities and cyber security cells were formed in order to deal with the issues involving any form of cyber crime.

The 2010s: Information security as we know it – Despite the different measures in the form of firewalls and antivirus programs designed to protect the devices/data from attacks, the hackers were efficient and skilled enough to breach the systems anyway. Different cryptographic algorithms and encryption techniques are being used in order to protect data over network and other transmission mediums. Also security policies were implemented by different organizations to prevent or avoid human errors of breaching the data in different ways. Software and antivirus programs are installed on PC's to protect them from outside attacks.

Furthermore, the history of information security can be traced back to the early days of computer; the first electronic computers were developed in the 1940s and 1950s. At the time, security was not a major issue or concern, since computers were primarily used by government and military organizations, with access limited to a small number of authorized individuals. However, as computers became more widespread in the 1960s and 1970s, security concerns began to emerge. With the advent of the Internet in the late 1960s, it was then possible for computers to communicate with one another, making it easier for malicious actors to infiltrate/access sensitive information.

In the 1980s and 1990s, information security began to gain more attention as a distinct discipline. The development of personal computers cum the rise of the Internet made it possible for individuals to access information from anywhere in the world – leading to increase in security breaches and other security incidents and requiring the need for better security measures.

Early 2000s witnessed continuity in security threats, and organizations taking more proactive approach to information security. Regulations such as the Sarbanes-Oxley Act (SOX) in the US and the Data Protection Act (DPA) in the UK were introduced to encourage organizations to take information security more seriously. Today, information security is a critical concern for all organizations of all sizes, and even individuals. With the proliferation of mobile phones/devices, cloud computing, and the Internet of Things (IoT), organizations must be extra-vigilant in protecting their sensitive information from a wide range of security threats (insider and outsider threats) [2].

FOCUS ON ORGANIZATIONAL AND OPERATIONAL SECURITY

Organizational and operational security is mostly concerned with people, processes, and procedures. The people within an organization can represent the greatest or biggest threat, which could be intentional or unintentional. The use of technology can be used to enforce processes and procedures, but while a lot of it has to do with user education and training. The organization needs to ensure that employees know what to do in certain situations. When there is some sort of security incident or natural disaster, all employees need to understand their roles and responsibilities and the procedures to follow. Having a plan provides structure and helps in preventing confusion and committing mistakes. The formalization of policies and procedures are crucial in ensuring that all employees understand and follow the security guidelines. An end user education program helps to drive home the key themes and message of a security policy. After all, what good or use are policies and procedures if no one knows about them? It is well known that there will always be security-related incidents which may be small or big, no matter how well or hard we plan. Nonetheless, one must still have a plan, since no plan at all can have a

devastating effect or huge impact on the organization. It is also very imperative to note that when a plan is developed, it should be put to test for validation, because a plan that does not work is just as bad as not having a plan at all [3].

Operations Security (OPSEC) is a security and risk management process and strategy that classifies information and then determines what is required to protect sensitive information and prevent it from getting into wrong hands. OPSEC gets information technology (IT) and security managers to view their operations and systems as potential attackers would. OPSEC includes analytical activities and processes, such as social media monitoring, behavior monitoring and security best practices. This involves five major steps which are [4, 5]:

- Identifying critical information,
- Analyzing threats,
- Analyzing vulnerabilities,
- Determining/assessing risks, and
- Planning/applying countermeasures.

Operations security is also centered on people, data, media, and hardware, all of which are elements that need to be considered from a security perspective. The best technical security infrastructure in the world can be rendered useless if an individual with privileged access decides to turn against the organization and the organization has no preventive or detective controls in place to defend itself. The organizational diligence required to build a comprehensive Business Continuity Planning (BCP)/Disaster Recovery Planning (DRP) can pay many dividends, through the thorough understanding of key business processes, asset tracking, prudent backup and recovery strategies, and the use of standards.

CYBER RESILIENCE

Cybersecurity-related studies have variously stated contending that the management approach towards security lacks clarity, is outdated, inadequate, and fails to comprehensively address organization's security requirements. They also argue that cybersecurity frameworks primarily focus on security-related regulations and standards, adopt a traditional perspective of protection and prediction, and prove inefficient in a highly uncertain environment and a volatile cyberspace with unknown risks. This now prompts the question of how to effectively establish cyber resilience within an organization, hence the dare need to explore cyber resilience.

Cyber resilience is an organization's continuous ability to achieve its intended outcomes despite adverse cyber events [6, 7]. NATO defines cyber resilience as the ability to prepare for, adapt to, withstand, and rapidly recover from disruptions resulting from deliberate attacks, accidents, or naturally occurring threats or incidents. The World Economic Forum report [8] defines cyber resilience as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery. A recent research has suggested that an adaptive approach and anticipating future challenges are necessary for resiliency. Some researchers more broadly define it as the ability to efficiently reduce the magnitude and duration of deviations from targeted system performance levels during a disruptive event. To this end, the U.S. Department of Health and Human Services (HHS) will take the following concurrent steps to advance cyber resiliency in the healthcare sector [9]:

1. Establish voluntary cybersecurity goals for the healthcare sector.
2. Provide resources to incentivize and implement these cybersecurity practices, via:
   - An upfront investments program, and
   - An incentives program.
3. Implement an HHS-wide strategy to support greater enforcement and accountability.
4. Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity.

As a result of the rise of technological advances and cyber-dependency, this has caused a corresponding increase in cyber-related issues [10]. To address these problems, the Malaysian Communications and Multimedia Commission has urged organizations to improve security measures for users and service providers. The National Policy Document recommends implementing ISO/TEC 27001:2013 Information Security Management System (ISMS) or equivalent security best practices to reduce the risk of cybersecurity incidents. Some of the existing Cyber Security Models and Resilience Frameworks are [11]:

1. Organization Resilience Frameworks ISO22316. The International Organization for Standardization (ISO) developed ISO 22316 Security and Resilience to provide principles and guidelines for establishing organizational resilience.
2. Information Security Management System (ISMS) – ISO27001:2013 and ISO27001:2022. The concepts stated in the ISO27001 standard can be used to access and manage cybersecurity risks and contribute towards cyber resilience.
3. NIST (National Institute of Standards and Technology) – This is a high-level, voluntary framework consisting of standards, guidelines,

and practices for managing and improving critical infrastructure cybersecurity. The framework is said to be voluntary because of the absence of enforcement or mandatory controls, unlike the ISO 27001 Standard, that requires specific controls as mandatory.

4. NLAC (Network-level access control) – This model is a framework developed by the National Infrastructure Advisory Council of the United States to address the need for resilience in critical infrastructure. The model provides a high-level resilience goal from the perspective of the industry-specific sector.
5. Cyber Resiliency Engineering Framework – CREF: this framework, also known as CREF, was developed by MITRE approximately a decade ago in 2011 to manage cyber threats [12, 13]. The goals, objectives, practices, costs, and metrics for resilience by CREF are designed to protect an organization against cyber threats using resilience engineering, mission assurance engineering, and cybersecurity concepts.

CHALLENGES TO ORGANIZATIONAL SECURITY

There are some challenges which confront and impact organizational security via compliance, security, and productivity. These challenges are: lack of traditional security perimeters, time consuming manual business process, and no agile access management strategy. Today, the way we work is changing from clearly defined perimeters with well-defined boundaries that could be controlled and monitored by IT, to a fluid business environment involving more stakeholders in the day-to-day operations. For this reason, there is need for Identity and Access Management (IAM) making it increasingly important in the enterprise space, especially when it comes to compliance, security, and productivity successfully aligning.

Number 1 challenge of the lack or elimination of traditional perimeters is what each user and devices are allowed to do on the company network which needs to be strictly monitored and restricted. This will lead to a Zero Trust architecture, as shown in Figure 2, which cannot function without a robust IAM policy platform. If this is not put in place, it would be hard to document compliance and upkeep security – not to mention allowing employees the flexibility to work productively on the corporate network across locations.

Number 2 challenge is that manual business processes are time-consuming, error prone, leading to high costs, and are expensive to maintain because they require a lot of manual work for employees; as the employees increase, some important tasks can be under-prioritized or even forgotten. This is true for large organizations with complex processes. Additionally, manual business processes do not have built-in security features like authorization management or access control – lack of these features makes it easy for unauthorized users to access sensitive information or perform unauthorized actions on your system using your IT infrastructure.

Number 3 challenge is the lack of overview over which employees have access to which resources. In large organizations this becomes problematic where many people need to be able to access confidential information in various ways. The lack of an overview can lead to security breaches or compliance issues. As a result of this, employees will end up having too many unnecessary accesses, which is a liability. Missing overview and no automatic way to handle access permissions across the organization will also result in productivity issues, so when they have fewer accesses to corporate resources than they need to work efficiently with, then productivity will suffer as a result [14].

SOLUTIONS TO THESE CHALLENGES

The following steps are recommended for organizations to effectively strengthen their cybersecurity and information security management system [15]:

1. The Chief Information Security Officer (CISO) must report directly to the CEO, who emphasizes the strategic importance of cyber security in an organization. The CISO needs to actively participate in board meetings and regularly provide them with updated information on threats, preparedness, and response plans.
2. Regular conduct of internal cyber security policy review cum independent objective assessment to ensure the validity of the cyber security policy and the measures taken. The board of directors and all internal stakeholders of the company should be involved in this process so that full support and agreement are achieved.
3. Ensure that the organizations' cyber security processes and control mechanisms are reliable. Security controls must be integrated and compliant with the NIST Cybersecurity Framework.
4. It is necessary to be familiar with all legal and normative acts related to the circulation of information in organizations and in its protection, as well as cyber security processes. At the same time, the obligation to disclose personal data to

employees should not be violated, and GDPR requirements should be observed.

5. Correct, targeted, and sufficient budgeting of cyber security is necessary. In practice, this should be about 10-12% of the total budget of the information technology direction of organizations. Room for increase in the budget should be in place in case of an event in the increase in risks and threats.
6. A comprehensive incident response strategy should be developed and regularly updated. This allows organizations' critical infrastructure to be on constant alert for cyber incidents. In the development of response plans against incidents, the participation of other structural units of organizations and their active involvement is necessary.
7. It is also necessary to have constant contact with partners, suppliers and clients of organizations, to introduce and provide them with advanced methods of ensuring cyber security within the framework of this relationship, and it is necessary to demand maximum compliance with established requirements and rules from their side. This is to reduce risks, and ensure better protection of organizations infrastructure.

IMPORTANCE OF WORKPLACE SECURITY

Workplace security strategy is for the defense of a business's critical data and information from hackers and other cyber security threats. It ensures being compliant with updated laws and regulations in the country or region where the organization is located. In today's modern workplace, we have a lot of things to protect, most importantly the employees' safety and health, as shown in Figure 3; ranging from tangible to intangible things, and of which not everything is visible to the eye or even easy to spot. Some of the reasons and import of workplace security among others are that:

- Workplace security keeps both the employees and visitors safe.
- It protects company data and systems.
- It controls access to the building, and
- It keeps the organization compliant.

Besides, there is the need to engage the necessary tools that will assist the workplace accomplish the security goals, aside having well trained security guards. There are a lot of efficient technologies available in the market, some of which are:

- Access control technology – access control is the selective restriction of access to a place or other resource, as shown in Figure 4; and while access management describes the process [16]. This comes in different forms, of which the common ones are badges and tokens (used to differentiate internal and external peoples), QR codes, facial recognition, or touch ID. When one is able to control who enters a building and with what level of permission, gives one ease of mind that people and property are protected/safe.
- Sensors and alarms – this is by installing sensors and alarms in the workplace to help detect potential security breaches. Motion sensors can trigger an alarm when someone or an intruder enters a restricted area, and while smoke detectors can alert staff to potential fires. Through the use of sensors and alarms, staff can quickly respond to security threats and prevent damage and theft.
- Password protection tools – password protection tool like Okta ensures that the passwords on shared company accounts are walled off behind multiple authentications. This allows that only staff/employees to access those accounts. In addition, encouraging employees to use strong passwords and change them regularly can go a long way in protecting intellectual property.
- Visitor Management System (VMS) – it ensures that only authorized visitors are allowed into the workplace, screening out unwanted guests to avoid security breaches. The VMS to be used must include features like blocklists (or blacklists) and ID verification that automatically protect against unwanted guests discreetly in the background.
- Security lighting – this is used to deter or detect intrusions or other criminal activities occurring on a property or site, as well as to increase a feeling of safety e.g. the use of floodlights, low pressure sodium vapor lights, high-intensity discharge lamps, etc. [17].
- Physical surveillance – this is useful to monitor critical entry points such as entrance, exit, IT rooms, critical data center, and while others should be fully monitored through robust CCTV surveillance systems, as shown in Figure 5.

A robust workplace security environment improves the efficiency and productivity of the company, directly impacting customer satisfaction and retention. This will as well reduce the company's liabilities, insurance, compensation and other social security expenses to be paid to the stakeholders, consequently increasing the business revenue and reducing operational charges that incur on the business budgets [18, 19].

CONCLUSION

Generally speaking, the paramount importance of organizational security cannot be overemphasized due to its cost implications if not put in place. It is very crucial that all employees of an organization must understand the importance of security, health, and safety in the workplace in order to maintain a high level of security consciousness, such that everyone can quickly and appropriately respond to new developments, changes, or attacks. To this end, all security strategies, measures, and management plans must be in place to guard against both physical and digital security threats proactively.

REFERENCES

[1] "Organizational security: How to keep your data safe?" (November 1, 2022), https://www.rocket.chat/organization-security-how-to-keep-your-data-safe

[2] "Principle of information system security: History," https://www.geeksforgeeks.org/principle-of-information-system-security-history

[3] Derrick Rountree, "Organizational and Operational Security," In: Security for Microsoft Windows System Administrators, 2011, https://www.sciencedirect.com/organizational-and-operational-security

[4] Jason Andress, "Operations Security," In: The Basics of Information Security, Second Edition, 2014, https://www.sciencedirect.com/operations-security

[5] Linda Rosencrance, Ben Cole, "OPSEC (operations security)," https://www.techtarget.com/opsec

[6] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors*, vol. 19, no. 1, pp 19, 2018.

[7] H. Maziku, S. Shetty, and D. Nicol, "Security risk assessment for SDN-enabled Smart Grids," *Computer Communications*, vol. 133, pp. 1-11, 2019.

[8] World Economic Forum, "Annual Report 2020-2021," https://www.weforum.org/reports/annual-report-2020-2021, 2020

[9] "Healthcare sector cybersecurity – ASPR – HHS.gov," https://aspr.hhs.gov/healthcare-sector-cybersecurity

[10] R. Loheswar, "Major data breaches in Malaysia in the past 24 months," *Malay Mail*, https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past24-months/47722, 2022.

[11] Thavaselvi Munusamy, Touraji Khodadadi, "Building Cyber Resilience: Key factors for enhancing organizational cyber security." *Journal of Informatics and Web Engineering*, vol. 2, no. 2, pp. 59-71, September 2023.

[12] Division of Banks, "Know the types of cyber threats," https://www.mass.gov/know-the-types-of-cyber-threats

[13] Kurt Baker, (May, 2024), "12 most common types of cyberattacks," https://www.crowdstrike.com/12-most-common-types-of-cyberattacks

[14] SIVIS Group, (November 24, 2023), "The 3 challenges that impact your organization's compliance, security, and productivity," https://get.sivis.com/the-3-challenges-that-impact...

[15] Vladimer Svanadze, and Sergiy Gnatyuh, "Challenges and Solutions for Cybersecurity and Information Security Management in Organizations," March 2024, https://www.researchgate.net/publication/challenges-and-solutions-for-cybersecurity-and-information-security

[16] "Access control," https://en.m.wikipedia.org/access-control

[17] "Security lighting," https://en.m.wikipedia.org/Security-lighting

[18] Amy Kirkham, (July 25, 2023), "The importance of workplace security: what it is and why you need it," https://envoy.com/the-importance-of-workplace-security

[19] "Here's the importance of security in the workplace and why you need to know it," https://www.getkisi.com/here's-the-importance-of-security

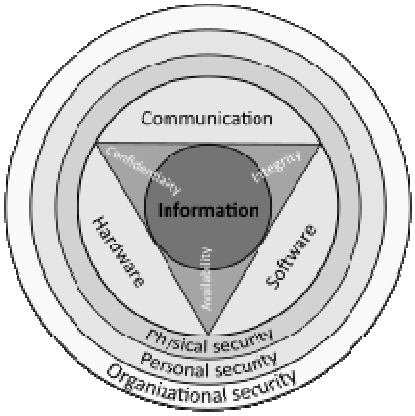

Figure 1 Information security.

Source:https://www.google.com/search?sca_esv=0a31b4c8707f31fc&sxsrf=ADLYWIKNiHDVb83looALLxliyC5Jt5o2Hw:1718651834531&q=images+on+organizational+security+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWERaHdBms7ttHL1116ec0FnDIxrxgGhNFSZEtYqV91R7Rf5ozRZtUy-fvojSh_GljrRCJ2kiQcYKrvZa7eH2W4J4-Irat4x8NFnigYG4D8K7dw8_peQUvGq7T1W2PG_keWF6WHldIsVuL3flNYqI5yjR9qhiiJwNxMdKzcBwt7h91Vh&sa=X&ved=2ahUKEwjDwtuAreOGAxXPRPEDHYRtA8YQ0pQJegQIDRAB&biw=1366&bih=580&dpr=1#imgrc=bUNZePUfN5D3tM

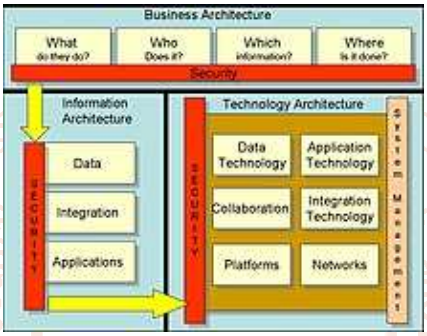

Figure 2 Enterprise security information architecture.

Source:https://www.google.com/search?sca_esv=b3f599f2fec3adbb&sxsrf=ADLYWILnrCYuYDT3bfog3ldIZHkE5Xj8Wg:1718672664574&q=images+on+organizational+security+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWERaHdBms7ttHL1116ec0FnDIxrxgGhNFSZEtYqV91R7Rf5ozRZtUy-fvojSh_GljrRCJ2kiQcYKrvZa7eH2W4J4-Irat4x8NFnigYG4D8K7dw8_peQUvGq7T1W2PG_keWF6WHldIsVuL3flNYqI5yjR9qhiiJwNxMdKzcBw-t7h91Vh&sa=X&ved=2ahUKEwjsvKDN-uOGAxW3VKQEHSu-AV4Q0pQJegQICRAB&biw=1034&bih=539&dpr=1#imgrc=E086IHfc-i2lnM

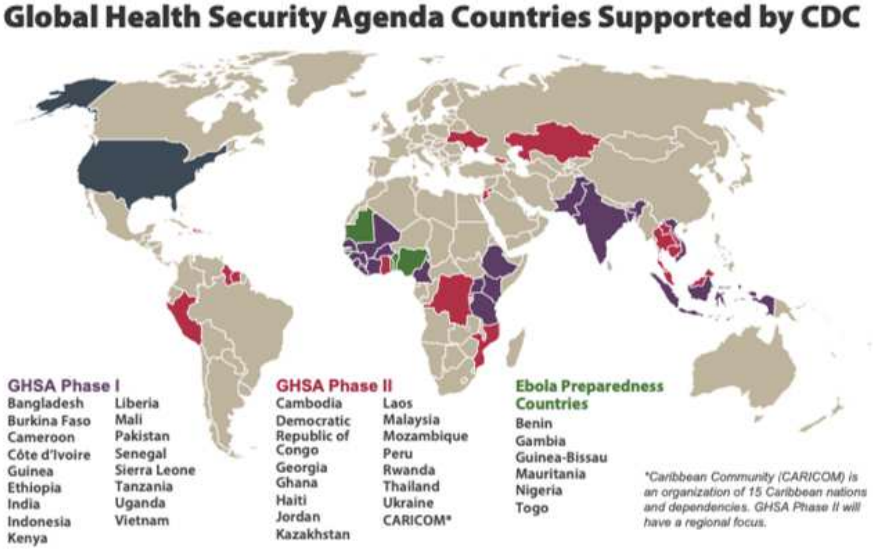

Figure 3 Global Health Security Agenda.

Source:https://www.google.com/search?sca_esv=b3f599f2fec3adbb&sxsrf=ADLYWILnrCYuYDT3bfog3ldIZHkE5Xj8Wg:1718672664574&q=images+on+organizational+security+by+wikipedia&tbm=isch&source

=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWERaHdBms7ttHL1116ec0FnDIxrxgGhNFSZEtYqV91R7Rf5ozRZtUy-fvojSh_GljrRCJ2kiQcYKrvZa7eH2W4J4Irat4x8NFnigYG4D8K7dw8_peQUvGq7T1W2PG_keWF6WHldIsVuL3flNYqI5yjR9qhiiJwNxMdKzcBw-t7h91Vh&sa=X&ved=2ahUKEwjsvKDN-uOGAxW3VKQEHSu-AV4Q0pQJegQICRAB&biw=1034&bih=539&dpr=1#imgrc=FBctsP6qotBk3M

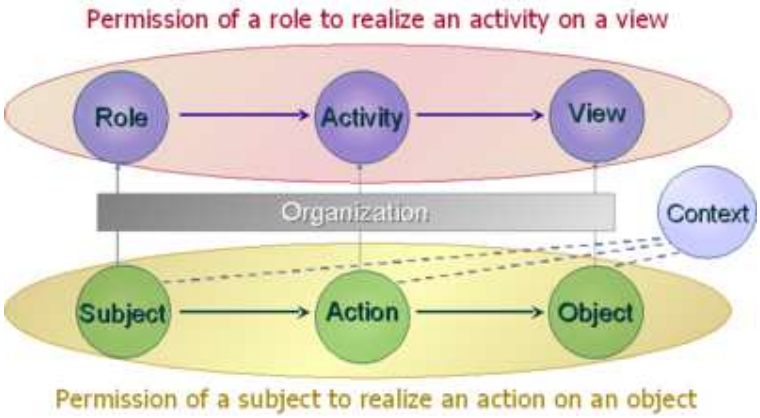

Figure 4 Organization-based access control.

Source:https://www.google.com/search?sca_esv=b3f599f2fec3adbb&sxsrf=ADLYWILnrCYuYDT3bfog3ldIZHkE5Xj8Wg:1718672664574&q=images+on+organizational+security+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWERaHdBms7ttHL1116ec0FnDIxrxgGhNFSZEtYqV91R7Rf5ozRZtUy-fvojSh_GljrRCJ2kiQcYKrvZa7eH2W4J4Irat4x8NFnigYG4D8K7dw8_peQUvGq7T1W2PG_keWF6WHldIsVuL3flNYqI5yjR9qhiiJwNxMdKzcBw-t7h91Vh&sa=X&ved=2ahUKEwjsvKDN-uOGAxW3VKQEHSu-AV4Q0pQJegQICRAB&biw=1034&bih=539&dpr=1#imgrc=t5PhFDQ_B89kdM

Figure 5 Surveillance

Source:https://www.google.com/search?sca_esv=b3f599f2fec3adbb&sxsrf=ADLYWILnrCYuYDT3bfog3ldIZHkE5Xj8Wg:1718672664574&q=images+on+organizational+security+by+wikipedia&tbm=isch&source=lnms&fbs=AEQNm0Aa4sjWe7Rqy32pFwRj0UkWERaHdBms7ttHL1116ec0FnDIxrxgGhNFSZEtYqV91R7Rf5ozRZtUy-fvojSh_GljrRCJ2kiQcYKrvZa7eH2W4J4Irat4x8NFnigYG4D8K7dw8_peQUvGq7T1W2PG_keWF6WHldIsVuL3flNYqI5yjR9qhiiJwNxMdKzcBw-t7h91Vh&sa=X&ved=2ahUKEwjsvKDN-uOGAxW3VKQEHSu-AV4Q0pQJegQICRAB&biw=1034&bih=539&dpr=1#imgrc=X6i80HIWlgQGaM