Enhancing Cyber Security: The Role of Networking, Coordination, and Trusted Information Sharing in Organizational Resilience

Duncan Nyale
School of Computing & Mathematics
The Co-operative University of Kenya
Nairobi, Kenya
Email: duncannyale [AT] gmail.com

Charles Katila
School of Computing & Mathematics
The Co-operative University of Kenya
Nairobi, Kenya
Email: ckatila [AT] cuk.ac.ke

***Abstract*— Organizations must take proactive measures to strengthen their cybersecurity posture as cyber-attacks continue to develop and become more sophisticated. Networking, coordination, and the sharing of trustworthy information among entities and organizations have become essential tactics for achieving this goal. This article gives a general overview of how networking, coordination, and trusted information sharing can improve an organization's cybersecurity posture. It covers the most recent advancements and trends in this field and analyses the advantages, difficulties, and best practices for putting these ideas into effect. The article's conclusion emphasizes the necessity of a cooperative, all-encompassing strategy for cybersecurity that incorporates networking, coordination, and reliable information exchange.**

Keywords: Cybersecurity, Networking, Coordination, Information Sharing, Security Measures, Security Posture, Incident Response, Threat Intelligence, Network Segmentation, Access Control, Insider Threats, Information Overload, Standardization, Collaboration Defence, Competing Priorities, Trust Relationships, Data Breach, Vulnerability Assessment

I. INTRODUCTION

In order to improve an organization's cybersecurity posture, networking, coordination, and trusted information exchange are essential elements. Entities and organizations can detect vulnerabilities, reduce risks, and create attack response tactics by effectively communicating, working together, and exchanging information about potential cybersecurity threats.

Networking

Establishing and sustaining links between various entities/organizations is referred to as networking. Networking in the context of cybersecurity entails establishing connections with other businesses that could offer assistance and information in the event of a cyber-attack. For instance, firms can collaborate with cybersecurity providers, trade groups, and governmental bodies to share threat information and best practices. By doing so, it will be possible to create a complete image of the cybersecurity landscape and spot emerging dangers before they spread widely.

Coordination

The process of gathering resources and activities to accomplish a single objective is referred to as coordination. Coordination in the context of cybersecurity refers to coordinating the actions of various entities and organizations to recognize and reduce cyber hazards. This can involve creating incident response strategies, carrying out routine security checks, and exchanging details on cybersecurity-related occurrences. Entities and organizations can create a more thorough and effective cybersecurity plan by combining their efforts.

Trusted Information Sharing

The communication of private information in a secure, private manner between entities or organizations is referred to as trusted information sharing. Identifying possible risks and creating mitigation methods entail exchanging threat intelligence, vulnerabilities, and best practices in the context of cybersecurity. To act as a focal point for information exchange and incident response, the US government, for instance, established the Cybersecurity and Infrastructure Security Agency (CISA). This organization collaborates with businesses in the private sector to exchange knowledge about potential dangers and create countermeasures.

Numerous studies have shown how networking, coordination, and trusted information sharing can improve cybersecurity posture. Information sharing and collaboration, according to a research by the National Institute of Standards and Technology (NIST), can assist firms in identifying and combating cyber threats more rapidly and proficiently (NIST, 2015). Organizations that regularly collaborate and coordinate actions are more likely to have successful incident response plans and stronger cybersecurity postures, according to a different study by the Center for Internet Security (CIS). (CIS, 2021).

An effective cybersecurity strategy must also include networking, coordination, and trusted information sharing. Organizations can gain a more complete understanding of the cybersecurity landscape and spot emerging threats by establishing relationships with other entities/organizations, coordinating their efforts, and sharing information. This can aid in risk mitigation, the creation of efficient incident response strategies, and eventually improvement of the organization's overall cybersecurity posture.

II. METHODOLOGY

This study examined the ways in which collaboration, networking, and trusted information sharing among entities/organizations improve an organization's cyber security posture. A thorough evaluation of previous research, reports, and case studies served as the foundation for the study design, which was a desktop method. Data was gathered from a variety of web sources, and content analysis was used to analyze the data. The study's findings are summarized in this report, along with suggestions for entities and organizations wishing to strengthen their cyber security posture.

III. LITERATURE REVIEW

A. *The Role of Networking in Enhancing the Cyber Security Posture of an Organization*

In order to share resources, information, and knowledge, many entities and organizations are connected through the process of networking. By giving an organization access to a wider range of resources, such as cyber security tools and knowledge, networking can improve its cyber security posture. Networking also enables businesses to engage with other entities and businesses to identify and reduce cyber dangers.

Networking is essential for improving an organization's cybersecurity posture. Organizations must create a thorough and effective security strategy that covers networking and communication protocols in light of the rising number of cyber threats. This tactic may consist of:

- Network Segmentation

Network segmentation is one of the key elements of a strong cybersecurity strategy. By separating the network into smaller subnetworks, network segmentation restricts access to sensitive data. As they won't have access to the full network, this helps stop lateral movement by cyber attackers in the event of a breach. Network segmentation is a key component in preventing data intrusions, according to a Verizon analysis. Organizations without sufficient network segmentation are more likely to suffer a data breach, according to the survey (Verizon, 2020).

- Network Monitoring

Network monitoring is a crucial component of improving cybersecurity posture. Monitoring a network entails keeping track of network activities and quickly spotting any security risks. This enables enterprises to react to security problems promptly and guard against data breaches. Network monitoring, according to a Ponemon Institute study, can lower the cost of a data breach by up to 35%. (Ponemon Institute, 2019).

- Access Control

Another essential element of network security is access control. Based on user roles and permissions, access control entails limiting access to sensitive data and resources. Access control is one of the most successful cybersecurity strategies, according to a survey by Accenture, with a potential ROI of 40 to 1. (Accenture, 2019).

- Encryption

Data can be secured via encryption by being changed into an unreadable format that can only be accessed with a decryption key. Encryption guards against unauthorized access to sensitive data and can lower the cost of a data breach by up to 16 percent, per a Ponemon Institute study (Ponemon Institute, 2019).

Benefits of networking in enhancing cyber security posture of an organization

- Segmentation and Isolation

Segmenting and isolating networks are important procedures for boosting cybersecurity posture. An enterprise can manage resource access and reduce the attack surface by segmenting the network into smaller chunks and isolating sensitive assets. Network segmentation, according to the National Institute of Standards and Technology (NIST), is a crucial security measure that can stop malware from spreading and lessen the damage of a cyberattack (NIST, 2018).

- Access Control

Through access control technologies like firewalls and virtual private networks (VPNs), networking can help improve cybersecurity posture. While VPNs can encrypt traffic between remote users and the network to shield it from interception and eavesdropping, firewalls can stop unauthorized traffic from accessing the network. To secure network traffic, the Cybersecurity and Infrastructure Security Agency (CISA) advises using firewalls and VPNs (CISA, 2021).

- Intrusion Detection and Prevention

In order to identify and stop cyberattacks, networking can also make it easier to deploy intrusion detection and prevention systems (IDPS). In real time, IDPS can detect unusual activities in network traffic and stop malicious traffic. The SANS Institute describes IDPS as a crucial security measure that can assist firms respond to security problems and provide early warning of cyberattacks (SANS, 2021).

- Monitoring and Analytics

Networking can also make it possible to gather and analyze network traffic data, which can give important insights into the cybersecurity posture of the company. Organizations can spot possible threats and vulnerabilities prior to an attack by monitoring network traffic and looking for anomalies and patterns. Network traffic analytics are advised by the National Cybersecurity Center of Excellence (NCCoE) for the detection and mitigation of cyber threats (NCCoE, 2021).

- Secure Infrastructure

Networking provides a secure infrastructure that helps businesses to defend their valuable assets and sensitive data from online threats. In order to ensure that data is delivered safely and that only authorized users have

access to it, a well-designed network can provide secure connectivity across various devices and systems. Firewalls, intrusion detection systems, and other security features integrated into the network architecture are used to do this. Network security, which serves as the basis for securing data and applications throughout the company, is a crucial part of overall cybersecurity posture, according to a report by Cisco. (Cisco, 2020). This emphasizes how crucial it is for an organization's entire cyber security plan to have a secure network architecture.

Challenges of networking to the cyber security posture of an organization

- Network complexity

It is difficult to safeguard modern networks properly due to their complexity. It can be difficult to monitor and administer networks because they can have thousands of devices and connections. In 2020, 60 percent of data breaches were the result of configuration errors, many of which were connected to network security, according to a Verizon analysis (Verizon, 2021).

- Vulnerabilities in network devices

Firewalls, switches, and other network devices may have security flaws that hackers might use against them. These flaws may be brought on by programming errors, setup errors, or weak passwords. The Cybersecurity and Infrastructure Security Agency (CISA) released a warning in 2020 regarding a flaw in a well-known network device that might enable an attacker to run any arbitrary code (CISA, 2020).

- Insider threats

Networking can result in insider threats. Insiders may misuse their access to the network to steal important information, interfere with business processes, or introduce malware. Insider threats caused 17% of data breaches, according to the 2021 Verizon Data Breach Investigations Report (Verizon, 2021).

- Lack of network segmentation

If a network is not properly segmented, an attacker who gains access to one area can move laterally and gain access to additional areas. This may result in serious data breaches. The 2020 Cost of Insider Threats Global Report estimates that a network segmentation failure caused a data breach of $1.6 million (Ponemon Institute, 2020).

- Inadequate network monitoring

A company may be unable to identify security incidents and take appropriate action if its network monitoring is insufficient. The mean time to detect a breach was 212 days, while the mean time to contain a breach was 75 days, according to the 2021 Cost of a Data Breach Report (IBM, 2021).

Best Practices for networking

The operations of any organization depend on networking and cybersecurity. A strong network architecture can increase productivity and facilitate efficient communication, but it can also expose a company to online threats like phishing scams, malware attacks, and data breaches. Consequently, it is crucial to put best practices into practice in order to improve networking and cybersecurity posture. Here are some recommendations for an organization's networking and cybersecurity posture:

- Use strong passwords and multi-factor authentication (MFA)

For the majority of systems and applications, passwords serve as the primary authentication method. Unauthorized access can be considerably decreased by using MFA and strong passwords. To improve cybersecurity posture, the National Institute of Standards and Technology (NIST) suggests adopting lengthy, complicated passwords and deploying MFA (NIST, 2017).

- Implement firewalls and intrusion detection/prevention systems (IDS/IPS)

IDS/IPS and firewalls are critical elements of network security. While IDS/IPS monitor network traffic and spot potential dangers, firewalls serve as a barrier between internal and external networks. Using these technologies can dramatically improve network security posture (Cisco, 2020).

- Regularly update software and operating systems

Updates for software and operating systems frequently include security patches that fix identified flaws. Software and operating system updates on a regular basis can improve cybersecurity posture and lower the risk of cyberattacks (CISA, 2023).

- Conduct regular security awareness training

One of the biggest causes of cybersecurity incidents is human error. Employees who receive regular security awareness training can recognize and stay away from phishing scams and other online hazards (SANS Institute, n.d).

- Monitor Network Activity

Regular network activity monitoring is necessary to spot any suspicious behavior or anomalies. This can involve keeping an eye out for odd data transfers, login attempts, and network traffic patterns. Potential risks can be found by monitoring before they develop into significant security events.

- Implement a data backup and recovery plan

Losing data can be disastrous for a company. Putting in place a data backup and recovery plan helps lessen the effects of data loss and minimize downtime (Symantec, 2023).

- Conduct regular vulnerability assessments and penetration testing

Regular penetration tests and vulnerability assessments can help find potential security holes in the network architecture. Taking these flaws into account helps improve cybersecurity posture (MITRE, 2019).

- Conduct a Risk Assessment

Finding potential weaknesses and threats to a network and its systems requires doing a risk assessment. It aids in locating the locations where security precautions need to be improved. All facets of the organization's infrastructure, such as its hardware, software, and human resources, should be thoroughly assessed for risks. It should also think about how a cyberattack would affect the business's operations, standing, and finances.

Networking is essential for improving an organization's cyber security posture. It offers a secure infrastructure, makes it possible to monitor and identify cyber threats in real-time, and enables the use of access controls and authentication procedures. Network security must be given top priority by enterprises as part of their entire cyber security strategy as cyber threats continue to develop and become more sophisticated.

B. *The Role of Coordination in Enhancing the Cyber Security Posture of an Organization*

The practice of directing several entities or organizations toward a shared objective is referred to as coordination. Coordination can improve an organization's cyber security posture by ensuring that all parties are working toward a unified objective. Additionally, coordination makes sure that resources are used effectively and that no effort is repeated.

The cybersecurity posture of a company must include coordination. The organization is able to recognize and handle potential cybersecurity issues before they have a chance to cause harm thanks to effective collaboration.

Coordination in Cybersecurity

Collaboration between various teams and stakeholders within an organization is required for cybersecurity coordination in order to properly identify and manage cybersecurity risks. Coordination between IT teams, security teams, management, and any other stakeholders who might be involved in cybersecurity is part of this. Clear communication, shared objectives, and a shared comprehension of the risks facing the company are all necessary for effective coordination.

The following are some essential components of cybersecurity coordination:

- Incident response planning

A well-defined plan should be in place for organizations to handle cybersecurity issues. All relevant stakeholders should be included in this plan, which should be frequently updated to reflect evolving threats and risks.

- Information sharing

For successful collaboration, sharing information regarding cybersecurity risks and threats is crucial. This covers information exchange with internal partners and stakeholders as well as external partners and stakeholders.

- Training and awareness

Every employee needs to receive training on cybersecurity best practices and be made aware of the dangers to the organization. By doing this, you can both ensure that events don't happen and that staff members are prepared to handle them when they do.

Benefits of coordination in enhancing cyber security posture of an organization

- Efficient Communication

Effective communication between various departments and stakeholders in a company is made possible by coordination. The organization's overall cybersecurity posture improves when everyone is aware of the potential cybersecurity dangers and knows how to handle them. Effective communication and information exchange are essential for cybersecurity, according to a PwC analysis (PwC, 2018).

- Better Preparedness

Organizations can better prepare for cybersecurity risks through coordination. Organizations can make sure that their staff members are informed of the most recent dangers and prepared to handle them by routinely upgrading their policies, processes, and training programs. Coordination among stakeholders may help firms respond to attacks and preserve their systems and data, according to a Deloitte research (Deloitte, 2019).

- Enhanced Detection and Response

Organizations can detect and address cybersecurity threats more quickly and proficiently when they are coordinated. They can recognize possible dangers and react to them more rapidly when several departments collaborate and share information. Coordination between various security tasks may considerably boost an organization's ability to detect and respond to attacks, according to a Gartner assessment (Gartner, n.d).

- Improved Risk Management

Organizations can manage cybersecurity threats more effectively through coordination. Organizations can recognize possible risks and put mitigation strategies in place by working together and sharing information. According to a McKinsey analysis, cooperation between various activities can aid firms in identifying and prioritizing cybersecurity threats and creating efficient risk management plans (McKinsey, 2023).

Coordination challenges to the cyber security posture of an organization

- Lack of communication and collaboration

For an organization to maintain a solid cyber security posture, effective communication and coordination between various teams are essential. However, a lack of coordination and communication across various departments can result in security gaps in many organizations. In a research by the Ponemon Institute, 47% of firms said that poor communication was a major

obstacle to having an effective cyber security posture (Ponemon Institute, 2018).

- Complex and fragmented IT infrastructure

It can be challenging to manage and secure the numerous systems and devices when an organization's IT infrastructure is complicated and dispersed over many different areas. As a result, there can be security openings and weaknesses that criminals could take advantage of. According to a survey by the Cloud Security Alliance (CSA), one of the major obstacles to cloud security for enterprises is the complexity of IT infrastructure (CSA, 2019).

- Limited resources

The absence of resources, such as funds, personnel, and time, is another problem that organizations must deal with. A Cisco study found that 45% of firms reported having insufficient funding for cyber security, and 53% of them said they were short on cyber security employees (Cisco, 2019). Implementing and upholding a robust cyber security posture may be challenging as a result.

- Compliance requirements

Regulatory compliance requirements, which are imposed on many firms, can be difficult to understand and put into practice. Complex technical and procedural controls are frequently a part of compliance requirements, and failing to comply can have serious financial and legal repercussions. According to a Tripwire poll, 61% of businesses said that compliance was the biggest obstacle to cyber security (Tripwire, 2019).

Best Practices for coordination

The NIST Cyber Security Framework and ISO Access Control recommendations state that for any business to effectively secure its assets and data from cyber-attacks, robust cybersecurity posture and effective coordination are essential. Coordination and cybersecurity best practices include:

- Develop a comprehensive cyber security strategy

Any firm must have a clear and comprehensive cyber security strategy. All facets of cyber security, including as risk assessment, incident response, access control, and data protection, should be covered. The plan should be periodically reviewed and revised and should be in line with the organization's overarching goals and objectives.

- Assign cyber security roles and responsibilities

Each employee inside the company needs to be well aware of their roles and responsibilities in relation to cyber security. This comprises supervisors, workers, independent contractors, and outside suppliers. Everyone should be aware of their responsibility for safeguarding the information and assets of the company.

- Train employees on cyber security best practices

The weakest link in a company's cyber security chain is frequently its employees. Employees can learn the best practices for setting secure passwords, avoiding phishing scams, and reporting suspicious behavior through routine training sessions that will help them comprehend the significance of cyber security.

- Implement access controls

Access controls should be put in place to guarantee that only people with the proper authorization can access sensitive data and systems. This includes role-based access controls, multi-factor authentication, and password policies.

- Conduct regular security audits and assessments

A company's cyber security posture can be identified with the aid of routine security audits and assessments. All facets of cyber security, including network security, physical security, and staff knowledge, should be covered in these examinations.

- Implement incident response plans

To enable quick and efficient responses to security problems, incident response strategies should be in place. These plans ought to be periodically examined, revised, and tested.

To improve an organization's cybersecurity posture, coordination is essential. Coordination enables effective communication, increased readiness, enhanced detection and reaction, and improved risk management, which assists organizations in reducing possible cybersecurity risks.

C. The Role of Trusted Information Sharing in Enhancing the Cyber Security Posture of an Organization

Information sharing between entities or organizations that is secure and trusted is referred to as trusted information sharing. By giving an organization access to timely, pertinent information that can assist in identifying and mitigating cyber risks, trusted information sharing can improve the firm's cyber security posture. Organizations can work together with other entities and organizations to combat cyber risks thanks to trusted information sharing.

A key component of cybersecurity for enterprises is trusted information exchange, especially in the linked world of today when cyber threats are continuously changing. To strengthen overall cybersecurity posture, this entails sharing information on cyber-attacks, vulnerabilities, and best practices across enterprises, government agencies, and other stakeholders.

- The capacity to recognize and counteract cyber threats more skillfully is one of the primary benefits of trusted information exchange. Organizations can better comprehend the threat landscape and take preventative measures to safeguard their networks and systems when they share information regarding cyber-attacks, vulnerabilities, and best practices. Information sharing is essential to a thorough cybersecurity strategy, according to a report by the Center for Internet Security (CIS), and can help

firms increase threat detection, incident response, and overall resilience (CIS, 2021).

- By encouraging collaboration and cooperation across stakeholders, trusted information sharing can aid companies in enhancing their cyber resilience in addition to boosting threat identification and response. A culture of trust that promotes cooperation and cooperation amongst stakeholders is necessary for efficient information sharing, claims a paper from the National Institute of Standards and Technology (NIST) (NIST, 2018). Organizations can collaborate more successfully to identify and mitigate cyber dangers by developing this culture of trust.
- Many organizations take part in Information Sharing and Analysis Centers (ISACs) and other cooperative platforms to promote the sharing of trustworthy information. In addition to building cooperation and trust among stakeholders, these organizations offer a venue for exchanging information regarding cyber risks, vulnerabilities, and best practices. ISACs are a crucial aspect of the national cybersecurity strategy, and they can aid enterprises in strengthening their cybersecurity posture, according to a Department of Homeland Security (DHS) report (DHS, 2020).

In order to improve threat detection, incident response, and overall resilience, trusted information exchange is an essential component of cybersecurity for enterprises. Organizations should take part in platforms for collaboration like ISACs and promote a climate of trust and cooperation among stakeholders if they want to help people share information effectively.

Benefits of trusted information sharing in enhancing cyber security posture of an organization

- Early Threat Detection and Mitigation

Organizations are able to exchange threat intelligence with one another thanks to trusted information sharing. This helps them to quickly identify and neutralize any threats. A research by the Ponemon Institute found that prompt cyberattack detection and remediation can dramatically lower the overall cost of a data breach (Ponemon, 2018).

- Improved Incident Response

Organizations can coordinate their crisis response activities with other organizations thanks to trusted information sharing. This can make it easier for them to quickly and successfully respond to threats. In order to lessen the damage of a cyberattack, a coordinated incident response is crucial, according to a study by the National Institute of Standards and Technology (NIST, 2012).

- Enhanced Threat Intelligence

Organizations can obtain more threat intelligence thanks to trusted information sharing. They can utilize this information to better their cybersecurity posture by identifying new threats and trends. A research by the Cyber Threat Alliance found that businesses can spot risks that they otherwise would not have been able to through exchanging threat knowledge (Cyber Threat Alliance, 2017).

- Collaborative Defense

Collaboration between organizations is made possible through trusted information sharing in the fight against cyber threats. This strategy is referred to as collaborative defense. Collaborative defense is a successful strategy for enhancing cybersecurity posture, according to a study by the Center for Internet Security (CIS, 2018).

Challenges of trusted information sharing in enhancing cyber security posture of an organization

- Trust and Collaboration

Building collaboration and trust between many groups is one of the main obstacles to information sharing. This is because firms are reluctant to share cybersecurity information with others due to its sensitivity. One of the major obstacles to information sharing, according to a research from the National Cybersecurity Center of Excellence (NCCoE), is the problem of building trust and cooperation among stakeholders (NCCoE, 2019).

- Legal and Regulatory Compliance

Making sure that information exchange complies with legal and regulatory obligations presents another challenge. Organizations must be aware of the numerous laws and rules governing cybersecurity information sharing, such as the Health Insurance Portability and Accountability Act and the Computer Fraud and Abuse Act. Penalties for breaking these rules include both legal and financial repercussions (NIST, 2016).

- Information Overload

Organizations may easily experience data overload as a result of the growing volume of cybersecurity information being created. This may result in information overload, which may result in the omission or disregard of crucial information. The National Institute of Standards and Technology (NIST) reported that companies may find it challenging to make timely and efficient decisions due to information overload (NIST, 2016).

- Lack of Standardization

For enterprises, the absence of standards in information exchange can be problematic. Organizations could find it difficult to understand and apply the information they get without a consistent strategy. The lack of standardization in the distribution of cybersecurity information between businesses results in wasteful and unproductive sharing, according to a report by the Cyber Threat Alliance (CTA) (CTA, 2019).

Best Practices for trusted information sharing

Information sharing is essential to cybersecurity because it enables organizations to stay informed about the newest risks and trends and to work together to protect against cyberattacks. However, there are risks associated

with sharing sensitive information that must be controlled. Some best practices for enhancing cyber security posture and communicating trusted information include, as per (CIS, 2018 & NIST, 2017):

- Implement a secure communication system

Only authorized parties or organizations are given access to sensitive information thanks to secure communication networks. Utilizing secure communication channels like Secure Sockets Layer (SSL) or Transport Layer Security (TLS) is one approach to accomplish this (SSL).

- Implement access controls

Access controls can be used to restrict unauthorized personnel's access to sensitive information. Role-based access controls (RBAC), multi-factor authentication (MFA), and strong password restrictions can all be used to accomplish this.

- Implement a data classification system

A data classification system aids in identifying the degree of information sensitivity and the necessary security precautions. This makes it possible to guarantee that only people with permission can access sensitive information.

- Conduct regular cybersecurity training

Data breaches can be avoided by educating personnel on cybersecurity best practices. Employees' awareness of potential dangers and their responsibility for protecting sensitive data can both be improved with regular training.

- Participate in Information Sharing and Analysis Centers (ISACs)

ISACs are groups that make it easier for their members to share cybersecurity threat intelligence. Being a member of an ISAC can give a business access to current threat intelligence and cybersecurity best practices.

Organizations that seek to safeguard themselves against cyber risks must have reliable information sharing practices and a robust cyber security posture. Organizations can lower their risk exposure and enhance their capacity to respond to cyberattacks by creating clear policies and procedures for information sharing and putting in place a robust cyber security posture. In order to keep ahead of new threats, it is crucial for enterprises to stay informed about the newest cyber security risks and trends. They should also continually assess and strengthen their cyber security posture.

IV. ANALYSIS & FINDINGS

TABLE I: SUMMARY OF BENEFITS, CHALLENGES AND BEST PRACTICES FOR NETWORKING, COORDINATION AND TRUSTED INFORMATION SHARING

Aspect	Networking	Coordination	Trusted Information Sharing
Benefits	- Improved visibility and awareness	- Efficient use of resources	- Early threat detection and response
	- Access to additional expertise	- Faster incident resolution	- Enhanced threat intelligence
	- Shared knowledge and experience	- Better risk management	- Better decision-making
	- Increased resilience	- Reduced duplication of efforts	- Improved incident response
	- Better threat detection	- Enhanced trust and collaboration	- More comprehensive risk assessment
Challenges	- Risk of exposure to new threats	- Communication barriers	- Legal and regulatory compliance
	- Complexity and management overhead	- Resistance to sharing information	- Lack of standardization
	- Potential for misconfiguration	- Data ownership and confidentiality	- Cultural differences
	- Limited resources and capabilities	- Competing priorities	- Lack of trust
Best Practices	- Use of secure communication	- Clear roles and responsibilities	- Adoption of industry standards
	- Segmentation of networks	- Establishment of trust relationships	- Use of data anonymization
	- Implementation of access controls	- Adoption of common language and tools	- Use of trusted third parties
	- Regular testing and validation	- Consistent reporting and feedback	- Clear policies and procedures
	- Sharing of threat intelligence	- Incident response planning	- Regular auditing and compliance

TABLE II: COMPARATIVE ANALYSIS OF NETWORKING, COORDINATION AND TRUSTED INFORMATION SHARING

Networking and Coordination	Trusted Information Sharing	Cyber Security Posture
Collaboration between entities/organizations helps in identifying and addressing security gaps and vulnerabilities. This allows organizations to implement security measures to prevent potential attacks.	Sharing trusted information, such as threat intelligence, helps organizations stay up-to-date with the latest threats and vulnerabilities. This enables organizations to prepare and respond to cyber-attacks effectively.	Networking, coordination, and trusted information sharing enhance an organization's cyber security posture by providing a collaborative approach to security.
Networking allows for the sharing of resources, such as personnel, technology, and knowledge. This helps organizations leverage their combined strengths to detect and prevent cyber-attacks.	Trusted information sharing ensures that organizations are not duplicating efforts, which can save resources and reduce the risk of gaps in security coverage.	Improved cyber security posture can help organizations avoid costly data breaches, maintain the trust of customers and partners, and avoid reputational damage.
Coordination between organizations can help in responding to cyber-attacks more effectively. For example, sharing incident response plans and coordinating responses can reduce the time it takes to identify and mitigate threats.	Trusted information sharing can also help organizations identify emerging threats, allowing them to implement preventative measures proactively.	A strong cyber security posture can help organizations comply with regulations and standards, such as GDPR, HIPAA, and PCI-DSS.
Networking and coordination can also help organizations pool resources to invest in advanced security technologies and tools. This can improve an organization's ability to detect and respond to cyber-attacks.	Trusted information sharing can help organizations build trust and establish partnerships with other organizations in their industry.	A strong cyber security posture can also help organizations attract and retain customers and partners by demonstrating their commitment to protecting sensitive information.

TABLE III: NETWORKING AND CYBER SECURITY POSTURE

Networking Component	How it Enhances Cyber Security
Firewalls	Firewalls act as a barrier between the internal network and external networks, filtering out potentially malicious traffic and preventing unauthorized access to the network.
Intrusion Detection and Prevention Systems (IDPS)	IDPS can detect and prevent network attacks, including denial of service (DoS) attacks, intrusion attempts, and malware. They can also alert security teams to unusual network activity, allowing them to investigate and respond to potential security incidents.
Virtual Private Networks (VPN)	VPNs encrypt traffic between a remote user and the organization's network, protecting the data from interception or eavesdropping by unauthorized third parties. This is especially important for remote employees who need to access sensitive company data while working from home or on the go.
Network Segmentation	By dividing the network into smaller, more manageable segments, network segmentation can limit the potential impact of a cyber-attack. If one segment is compromised, the damage is limited to that area, and it becomes easier to isolate and contain the threat.
Access Control	Network access control mechanisms can enforce policies that restrict access to the network to only authorized personnel and devices, reducing the risk of unauthorized access and potential cyber-attacks1.
Monitoring and Logging	By monitoring network traffic and logging events, organizations can detect suspicious activity and identify potential security incidents. Network monitoring can also provide valuable insights into the organization's overall security posture, helping security teams identify areas that require improvement

TABLE IV: COORDINATION AND CYBER SECURITY POSTURE

Aspect of Cyber Security	Importance	Coordination Enhancements
Risk Assessment	High	Coordination among various departments (e.g. IT, legal, compliance, etc.) can lead to a more comprehensive risk assessment. Each department can provide their unique insights to identify and assess risks, leading to a more thorough analysis.
Incident Response	Critical	Coordination among different teams (e.g. IT, security, legal, PR, etc.) can help streamline the

		incident response process. Effective communication and collaboration can help contain the incident quickly and minimize the impact.
Access Management	High	Coordination among IT, HR, and other departments can help ensure that employees have the appropriate access rights and permissions. This can prevent unauthorized access and reduce the risk of data breaches.
Security Awareness Training	High	Coordination between IT and HR can help ensure that all employees receive regular security awareness training. This can help reduce the risk of human error and increase overall security awareness.
Threat Intelligence	High	Coordination among different security teams (e.g. internal and external) can help share threat intelligence and identify emerging threats. This can help the organization stay ahead of potential attacks and improve their overall security posture.
Compliance	High	Coordination between legal and IT can help ensure that the organization complies with relevant regulations and standards. This can help prevent legal and financial penalties and improve overall security posture.

TABLE V: TRUSTED INFORMATION SHARING AND CYBER SECURITY POSTURE

Aspect of Cyber Security	How Trusted Information Sharing Enhances it
Threat Intelligence	Trusted information sharing allows organizations to receive relevant and timely threat intelligence from trusted sources, which can help them proactively identify and mitigate potential cyber threats. By sharing information about emerging threats, organizations can stay up-to-date on the latest tactics, techniques, and procedures used by cybercriminals, and take steps to prevent attacks before they happen.
Incident Response	When a cyber-attack occurs, trusted information sharing enables organizations to respond quickly and effectively by providing them with valuable information about the attack, including the type of malware used, the tactics used by the attackers, and the vulnerabilities exploited. This information can help organizations to contain the attack, mitigate its impact, and prevent similar attacks from occurring in the future.
Collaboration	Trusted information sharing facilitates collaboration between organizations, allowing them to work together to improve their cyber security posture. By sharing information about threats and vulnerabilities, organizations can collaborate to develop more effective security strategies and countermeasures. Additionally, trusted information sharing enables organizations to share best practices and lessons learned, helping them to stay ahead of emerging threats and better protect their systems and data.
Compliance	Many regulations and standards require organizations to share information about cyber threats and incidents. By participating in trusted information sharing networks, organizations can ensure that they are compliant with these regulations and standards. Additionally, sharing information about cyber incidents can help organizations to demonstrate due diligence and minimize their legal and reputational risks.

V. CONCLUSION

For a business to strengthen its cyber security posture, networking, coordination, and trusted information sharing are all essential. Through networking, one has access to more knowledge and experience, increased visibility and awareness, and improved visibility. Coordination makes it possible to deploy resources more effectively, deal with incidents more quickly, and manage risks better. Early threat identification and response, improved threat intelligence, and better decision-making are all made possible via trusted information sharing.

These techniques do come with certain challenges, though, including the potential for exposure to fresh risks, difficulty in communicating, and compliance with laws and regulations. Organizations should adopt industry standards, employ encrypted communication, segment networks, and use other best practices to overcome these issues. Clear policies and procedures, regular testing and validation, and the exchange of threat intelligence are also critical. Ultimately, building trusting relationships and using a shared language and tools are necessary for effective networking, coordination, and trusted information sharing.

VI. RECOMMENDATIONS

Cybersecurity dangers are evolving and growing more prevalent in the current digital era. To safeguard their priceless assets from cyberattacks, organizations must be proactive. Utilizing networking, coordination, and trusted information sharing among entities and organizations is one successful strategy. The suggestions listed below are meant to help enterprises improve their cyber security posture.

- Build a network of trusted partners

Organizations should create a network of reliable partners they can rely on for assistance in the event of a cyber-attack. This network may consist of businesses in the same sector, governmental entities, and security professionals. Organizations can share knowledge about new risks, best practices, and mitigation techniques by developing these ties. This network can act as a testing ground for innovative cyber security concepts and methods.

- Foster coordination and collaboration

Collaboration and coordination are necessary for efficient cyber security. Organizations need to ensure that their partners have open lines of communication and that their approaches to cyber security are consistent. Regular gatherings, team activities, and information exchange can help with this. Organizations can discover possible risks and create pro-active mitigation solutions by cooperating.

- Establish a trusted information sharing platform

Organizations should create a secure platform for information exchange that enables them to communicate about new threats, best practices, and mitigation techniques. All network participants should be able to access, trust, and use this platform. Organizations may respond swiftly to new threats and take preventative action to safeguard their assets by exchanging information in real-time.

- Develop a common language for cyber security

A common language is necessary to allow successful communication amongst partners in the complicated sector of cyber security. All network participants should be able to communicate in a standard language for cyber security within organizations. Key phrases, definitions, and concepts related to cyber security should be used in this language. Partners can successfully communicate with one another and build a shared understanding of cyber security threats and mitigation techniques by using the same language.

- Invest in technology and training

To strengthen their position in terms of cyber security, organizations should invest in technology and training. Implementing cutting-edge security technology like firewalls, intrusion detection systems, and encryption tools is part of this. Additionally, it entails regularly educating staff members on cyber security best practices, including how to spot phishing emails, make secure passwords, and report suspicious behavior.

REFERENCES

[1] NIST. (2015). Framework for improving critical infrastructure cybersecurity. Retrieved from https://www.nist.gov/cyberframework

[2] Center for Internet Security (CIS). (2021). The CIS Controls. https://www.cisecurity.org/controls/

[3] CISA. (2021). Network Security. CISA. https://www.cisa.gov/news-events/news/home-network-security

[4] NCCoE. (2021). Network Traffic Analytics. https://www.nist.gov/publications/network-security-traffic-analysis-platform-design-and-validation

[5] NIST. (2018). NIST SP 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[6] SANS. (2021). Intrusion Detection and Prevention. https://www.sans.org/blog/favoring-frameworks-for-intrusion-detection-and-prevention/

[7] Cisco. (2020). Security resilience for the unpredictable https://www.cisco.com/c/en/us/products/security/network-security.html

[8] CISA. (2020). Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[9] IBM. (2021). 2021 Cost of a Data Breach Report. https://www.ibm.com/security/data-breach

[10] Ponemon Institute. (2020). 2020 Cost of Insider Threats Global Report. https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2020/12/UK-VR-Proofpoint-Report-2020-Cost-of-Insider-Threats.pdf

[11] Verizon. (2021). 2021 Data Breach Investigations Report. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf

[12] Deloitte. (2019). Navigating cybersecurity. https://www2.deloitte.com/uk/en/blog/cyber-risk/2023/navigating-cyber-security.html

[13] Gartner. (n.d). The IT Roadmap for Cybersecurityhttps://www.gartner.com/en/information-technology/trends/the-it-roadmap-for-cybersecurity

[14] McKinsey. (2023). Building a cybersecurity culture. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/building-a-culture-that-grows-with-the-business-lessons-from-tibber

[15] PwC. (2018). Global State of Information Security Survey 2018. https://www.pwc.com/sg/en/publications/assets/gsiss-2018.pdf

[16] Ponemon Institute. (2018). The Cyber Security Readiness Report. https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

[17] Cloud Security Alliance. (2019). Top Threats to Cloud Computing. https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/

[18] Cisco. (2019). CISO Benchmark Study: 2019 Report. https://search.cisco.com/search?query=CISO%20Benchmark%20Study:%202019%20Report&locale=enUS&bizcontext=&cat=&mode=text&clktyp=enter&autosuggest=false&istadisplayed=false&tareqid=&categoryvalue=

[19] Tripwire. (2019). Why Cyber Security is Key to Enterprise Risk Management for all Organizations. https://www.tripwire.com/state-of-security/cyber-security-enterprise-risk-management-erm-organizations

[20] Ponemon Institute. (2018). 2018 Cost of a Data Breach Study: Global Overview. https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf

[21] NIST. (2012). Computer Security Incident Handling Guide. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[22] Cyber Threat Alliance. (2017). Sharing is Caring: Why the Industry Must Work Together to Combat Cybercrime. https://cyberthreatalliance.org/wp-content/uploads/2017/05/CTA_Sharing-is-Caring.pdf

[23] Center for Internet Security. (2018). CIS Controls Version. https://www.cisecurity.org/controls/cis-controls-list/

[24] National Cybersecurity Center of Excellence (NCCoE). (2019). Information Sharing. https://csrc.nist.gov/glossary/term/information_sharing

[25] NIST. (2016). Guide to Cyber Threat Information Sharing. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf

[26] Cyber Threat Alliance (CTA). (2019). Improving Cybersecurity Information Sharing: A Call to Action. https://www.cyberthreatalliance.org/improving-cybersecurity-information-sharing-a-call-to-action/

[27] Center for Internet Security. (2021). Information Sharing. https://www.cisecurity.org/ms-isac

[28] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[29] Department of Homeland Security. (2020). Information Sharing and Analysis Organizations. https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos

[30] NIST. (2017). Cybersecurity Framework Version 1.1. https://www.nist.gov/news-events/events/2018/04/webcast-cybersecurity-framework-version-11-overview

[31] Cisco. (2020). Firewall and intrusion detection and prevention system. https://www.cisco.com/c/dam/global/en_au/assets/pdf/at-a-glance-c45-735895.pdf

[32] MITRE. (2019). Vulnerability assessment and penetration testing. https://attack.mitre.org/tactics/TA0005/

[33] NIST. (2017). Digital identity guidelines. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[34] SANS Institute. (n.d). Security awareness training. https://www.sans.org/security-awareness-training

[35] Symantec. (2023). Data backup and recovery. https://knowledge.broadcom.com/external/article/159322/backup-and-restore-dcs-database-for-disa.html

[36] CISA. (2023). Understanding patches and software updates. https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

[37] International Organization for Standardization. (2013). ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls. https://www.iso.org/standard/54533.html

[38] Verizon. (2020). 2020 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdfx

[39] Ponemon Institute. (2019). Cost of a Data Breach Report 2019. https://www.ibm.com/downloads/cas/RDEQK07R

[40] Accenture. (2019). Cybercrime Costs Projected to Reach $5 Trillion Annually by 2024. https://newsroom.accenture.com/news/cybercrime-could-cost-companies-us-5-2-trillion-over-next-five-years-according-to-new-research-from-accenture.htm