**Fundamental Cybersecurity Technologies for Enterprise Protection**

Nithish Sunkara

IS 5700 – Information Security and IT Governance

Indiana Institute of Technology  
Changhao Chenli

April 22, 2025

**Introduction**

Modern society presents organizations with intensifying issues when they attempt to secure their critical information resources. Multiple security layers become essential because enterprise data moves through networks and exists in volatile memory while settling in various systems. Organizations depend on standard security technologies that both defend against threats while protecting their data quality and preserving secret information access. The research examines modern enterprise cybersecurity technologies through a thorough analysis of storage protection systems and network protection functionalities, and usage protection methods.

**Storage Protection Technologies**

Storage systems become the top priority for cyberattacks because they maintain essential organizational data, which consists of intellectual property alongside personally identifiable information (PII). The encryption method has become a standard practice that creates unreadable data for those who do not possess legitimate access rights. Organizations require both encryption methods for stored data through at-rest encryption, together with in-transit encryption when data moves across networks. Organizations implement the efficient encryption technology AES specifically because of its strong protection capabilities.

Storage security requires the implementation of various access control systems to maintain proper protection. Access to storage elements occurs through file permissions as well as RBAC permissions based on user identities and MFA authentication models. Data loss prevention (DLP) technologies do real-time monitoring of data transfers to prevent unauthorized movements of sensitive data between internal systems and external storage tools.

Backup and recovery methods play a vital role during cybersecurity processes. Data recovery processes that use snapshots together with redundant systems and disaster recovery-as-a-service represent essential solutions to restore data after ransomware or system failure attacks.

**Network Protection Technologies**

Recipients of cyber threats frequently encounter them through their enterprise networks. The firewall operates as a basic security technology by monitoring all network traffic entering or exiting the system with defined security rules in place. Technology beyond basic firewalls exists with next-generation firewalls (NGFW) by adding features like deep packet testing and intrusion blocking abilities.

Intrusion Detection and Prevention System (IDPS) delivers supplemental cybersecurity through systems that examine activities for both abnormal actions and recognized attack patterns. IDPS technologies monitor system activities to detect brute-force attacks, together with port scanning activities and malware and can activate warning notifications that trigger automatic threat responses.

VPN’s establish essential security protocols through encrypted traffic encryption, together with IP address masking, which decreases vulnerability to man-in-the-middle attacks. Enterprises are currently switching to Zero Trust Network Access (ZTNA) as it replaces traditional VPNs in modern networks. By default, ZTNA operates without trust assumptions while performing ongoing checks of users and devices regarding their identity and their state and actions.

Network Access Control technologies acts as security measures through which devices must receive authentication before endpoint compliance checks allow network permission.

**Usage Protection Technologies**

The equivalent importance lies in preserving both information access security and utilization methods. Emergency endpoint response systems deliver immediate endpoint examinations that detect both security intrusions and access violations. The implementation of Endpoint Detection and Response (EDR) solutions involves behavioral analytics that simultaneously help detect infected devices and prevent them from connecting to the network.

User Behavior Analytics implements AI together with machine learning to track user activities so that tunneling insider threats, along with account compromise, can be identified.

Enterprise user identity management depends on Identity and Access Management (IAM) systems to operate effectively. SSO and MFA enable IAM technologies to establish secure and easy access control through their combined integration.

Security Information and Event Management (SIEM) systems merge multiple data sources to present united threat detection capabilities and event monitoring as well as incident response features. Storage Security Information Event Management tools maintain essential status as organizational compliance systems under GDPR and HIPAA regulations, among others.

**Personal Experience and In class reference**

In class we have covered essential cybersecurity ideas about cryptography alongside understanding COBIT (Control Objectives for Information and Related Technologies) alongside targets on organizational information assets. The IBM video presentation underscored the priority of implementing data security policy with its components which include discovery and protection and compliance requirements and intrusion detection. I have already dealt with multi-factor authentication (MFA) during my regular usage of applications including WhatsApp and Gmail. The platforms implement security measures that demand users to authenticate their identity using double validation methods including SMS code delivery services and application-based approval procedures. Enterprise-level Identity and Access Management systems heavily depend on secure access control because its benefits become increasingly evident through this implementation.

**Conclusion**

The modern digital world develops endlessly while offering new security challenges for businesses across the board. Enterprises need a comprehensive security system which requires the implementation of several basic cybersecurity technologies operating at multiple levels. All businesses need to establish a unified protective framework which secures network traffic as well as data storage encryption alongside endpoint anomaly detection and identity management capabilities. All enterprise cybersecurity systems today depend on a combination of encryption with firewalls and IDPS and EDR and IAM and SIEM for operational continuity and trust management.

**References**

Stallings, W. (2023). *Effective Cybersecurity: A Guide Using Best Practices and Standards*. Addison-Wesley Professional.

National Institute of Standards and Technology (NIST). (2020). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>  
In class reference video  
[*https://youtu.be/N8xEgSe5RwE?feature=shared*](https://youtu.be/N8xEgSe5RwE?feature=shared)