Network & Cyber Security: Tools, Costs, and Efficiency

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

IT 315 – Introduction to Networking and Security

September 28, 2025

Instructions

Discuss how companies and organizations are securing their information systems and network technology.

- What tools are they using?
- What is the cost of securing information systems and network technology?
- What is the cost of not securing information systems and network technology?
- What are the most effective techniques of securing information systems and network technology?
- What are the least effective techniques of securing information systems and network technology?

Network & Cyber Security: Tools, Costs, and Efficiency

Organizations secure their data, network, and information systems through a multi-layered approach (i.e., defense-in-depth) by combining modern technologies, streamlined policies, and human education. Organizations will use tools such as firewalls, antivirus software, intrusion detection/prevention systems (IDS/IPS), Unified Threat Management (UTC), Network Access Control (NAC) systems, and encryption to protect against threat actors (Panko, 2020; Kim & Solomon, 2021).

The cost of securing data and networks will vary widely depending on the size and type of industry the organization operates in; however, in general, the costs are significant (Fathima, 2024; Verizon, 2024). On average and as a good "rule-of-thumb," IT experts and researchers agree that organizations should allocate at least 7-10% of their IT budget to cybersecurity (Violino, 2019; BitLyft, 2025). The cost of IT security includes technology (i.e., hardware and software), personnel (e.g., security analysts, CISO, security guards), and training.

The cost of ***not*** securing an organization's data and network systems is often far greater (IBM, 2025). A data breach can result in massive financial losses from remediation, legal fees, regulatory fines, and theft (e.g., the 2013-2014 Target and Yahoo data breaches, and the 2017 Equifax data breach). Indirect costs (such as damage to reputation, business disruption, and the loss of customer trust and base, and business disruption) can be even more devastating and ultimately lead to a company's bankruptcy and indefinite closure (Swinhoe, 2019).

The most effective techniques are a combination of technological and procedural or operational measures (Panko, 2020; Kim & Solomon, 2021; Nelson et al., 2022). Some security techniques include the following:

1. Regular software and firewall patching.
2. Multi-factor and biometric authentication (MFA).
3. Network segmentation.
4. Implementing VPNs for remote workers to safely access sensitive data and dialogue.
5. Implementing different firewall types (e.g., packet filtering, stateful inspection, Application Proxies, and screened borders or DMZs).
6. Proactive employee training on phishing and security awareness.

Least effective techniques often involve relying on single security measures, such as basic firewalls (without flood guards and loop protections), or neglecting fundamentals like updating software and using default or reusing old passwords for the same and/or multiple accounts (Violino, 2019; Panko, 2020; Kim & Solomon, 2021; Nelson et al., 2022; BitLyft, 2025). Single security countermeasures are risky because the moment that the single point crumbles is when everything (including whatever network it relies on) becomes exposed and vulnerable to the world, including threat actors. Finally, human error continues to rise within organizations due to inadequate training, which is a predominant risk and a leading cause for most data breaches (Verizon, 2024; IBM, 2025).

References

BitLyft. (2025, August 25). *The Cost of Cybersecurity and Creating an Achievable Security Budget*. Retrieved September 22, 2025, from https://www.bitlyft.com/resources/the-cost-of-cybersecurity-and-creating-an-achievable-security-budget

Fathima. (2024, December 28). *Understanding the costs of cyber security services companies*. DigitDefence. https://digitdefence.com/blog/understanding-the-costs-of-cyber-security-services-companies

IBM Corporation & Ponemon Institute. (2025). *Cost of a Data Breach Report 2025: The AI Oversight Gap*. IBM Corporation.

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2022). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61r3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Panko, R. R., & Panko, J. L. (2020). Business data networks and security (11th ed.). Pearson.

Swinhoe, D. (2019, May 30). *Why businesses don't report cybercrimes to law enforcement*. CSO Online. https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html

Verizon Business. (2024, June). 2024 Data Breach Investigations Report. Retrieved September 12, 2025, from https://www.verizon.com/business/resources/reports/dbir/#top-takeaways

Violino, B. (2019, August 20). How much should you spend on security? CSO Online. https://www.csoonline.com/article/567633/how-much-should-you-spend-on-security.html