

## METHODS OF ENSURING INFORMATION SECURITY IN CORPORATE NETWORKS

**Ergashev Marufjon Mamurjon o`g`li**

Master's degree, Faculty of Cyber-Security,  
Tashkent University of Information Technologies  
named after Muhammad al-Khwarizmi, Uzbekistan

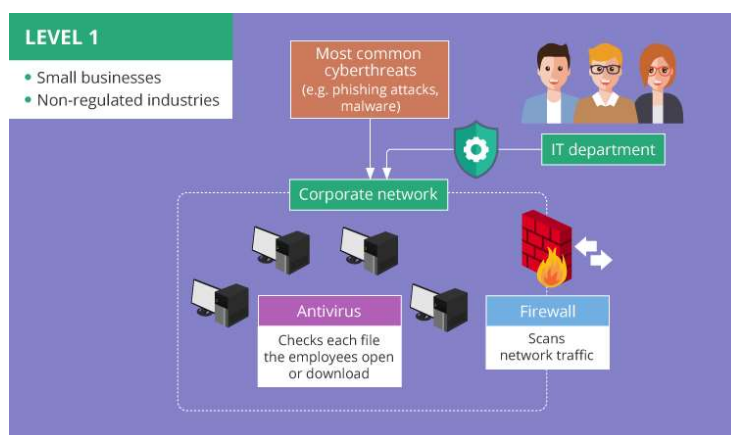
**Abstract:** Any company that uses a corporate network for both internal and external interaction needs to pay utter attention to its security. The possibility of data leaks or cyber-attacks may cost a company millions of dollars and a ruined reputation. In order to protect sensitive data and prevent possible threats, companies need to follow the basics of corporate network security. We collected the most common practices that will help safeguard one's corporate network and prevent the threat actors from intruding it. Before discussing the best practices of combatting cyber threats, it is important to understand the most common types of these threats. In this way, you will have a clear picture of what might be threatening your network and thus will be able to build a solid security strategy.

**Keywords:** Intrusion detection systems (IDSs), Neural networks (NNs), corporate networks, Back-propagation (BP).

**Introduction.** As cyberthreats are constantly evolving in complexity and volume, the battle against them implies ‘spreading’ the protection across all the systems in the corporate network – servers, databases, services, installed software, etc. What's more, attention should be paid to ensuring that the company's employees understand and follow cybersecurity principles, and will not (un)intentionally compromise the corporate network security with their actions. However, cybersecurity measures applied inside the organization may differ depending on the company's size, its financial capabilities, the industry it operates in (regulated or non-regulated), the information it has to deal with in the course of business activities, etc. Bearing in

mind these and other factors, we managed to determine *three main cybersecurity protection levels*. Depending on their complexity, these levels can be established with the assistance of a company's IT department or a cybersecurity services provider.

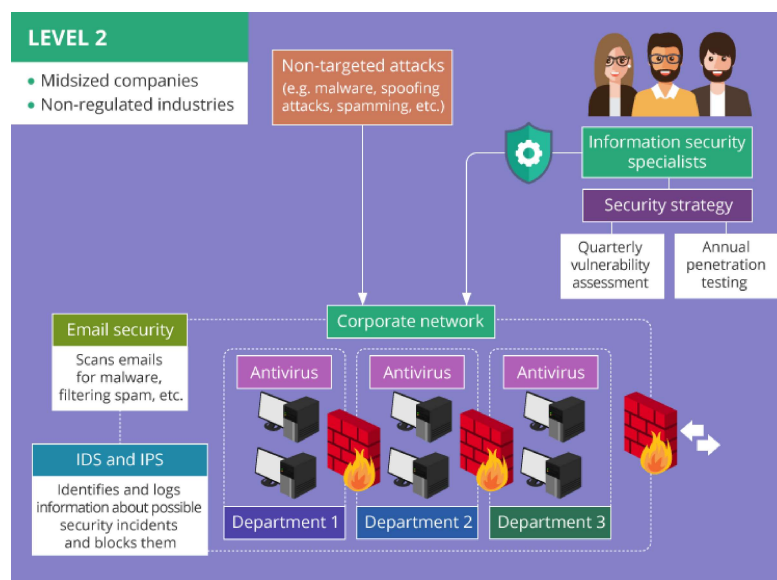
#### Level 1 – minimal protection



The key point of Level 1 cybersecurity is to ensure the protection of the corporate network from the **most common cyberthreats**, e.g., *phishing attacks* (links to malicious websites or downloads infected with viruses are attached to emails or instant messages and sent to a company's employees) and *malware* (malicious software reaching a company's network via internet or email and existing in the form of spyware, ransomware, browser hijackers, etc.). Minimal protection applies to **small businesses** operating in **non-regulated industries** and having **strictly limited financial resources**. Small and not widely-known (at least not yet) companies that don't deal with information valuable for hackers (e.g., customer personal data like credit card numbers, passwords, etc.) may hardly become targets of sophisticated cyberattacks like DDoS (Distributed Denial of Service) or spear phishing. The minimum of cybersecurity measures essential for the implementation is a properly **configured firewall protection** working together with **regularly updated antivirus software**. Firewalls scan network traffic to detect anomalous packets or packet fragments. Antiviruses ensure protection from such cyberthreats as ransomware, worms, spyware, etc. by checking each file the employees open or download from the internet or other sources. To apply these security measures, there's no need in organizing a separate cybersecurity department. A company's **IT department** can

take responsibility for this, as implementing firewall protection, installing antivirus software and continuously maintaining their performance does not require cybersecurity-related skills. Nevertheless, the protection level of a corporate network should be regularly checked. Conducting vulnerability assessment and penetration testing **annually** is enough for a small organization carrying out their business in a non-regulated industry. These cybersecurity services performed on an annual basis won't result in heavy expenses for a company with a limited budget. At the same time, these activities can help system administrators to stay aware of occurring security weaknesses inside the company's network.

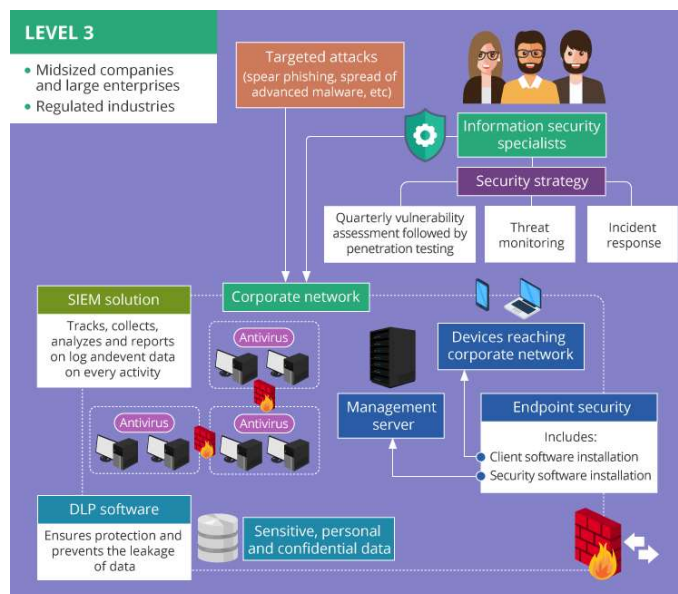
## Level 2 – advanced protection



Level 2 cybersecurity ensures the protection of the corporate network from **non-targeted attacks**, e.g., malware sent to a range of email addresses, spoofing attacks, spamming, etc. In this case, attackers' goal is to steal any valuable information from any IP address susceptible to known security weaknesses possibly existing in the corporate network.

The probability that **midsized companies** will fall victim to non-targeted attacks is great. Since such organizations have no need to comply with regulatory standards, they may be likely to neglect strong cybersecurity measures in their networks. Thus, they may be easy to compromise.

### Level 3 – maximal protection



The key task of Level 3 cybersecurity is to ensure the protection of the corporate network from targeted attacks. This type of cyberattacks (spear phishing, the spread of advanced malware, etc.) implies specifically developed campaigns conducted against a particular organization. To maintain this level of network security, a company needs *information security specialists* responsible for detecting and managing cybersecurity risks, developing security procedures and policies, etc. For these purposes, the company may arrange their own **information security department** or turn to a **managed security service provider (MSSP)**.

**Material.** Network security is a comprehensive subject to discuss. It involves many aspects: both external threats that need to be addressed and internal threats related to the employees' knowledge of security basics. Therefore, any company that wishes to safeguard its network and protect the data needs not only to deploy suitable tools but also to educate the employees on the basic practices of network security. In this way, the company will create a secure working environment and will minimize the potential risks of the network intrusion.

**Method.** Network security is important for your business. It combines complex measures that provide security. Network security helps to protect sensitive data, improve network efficiency, and prevent cybercrime. Also, take steps to restrict network access, educate your staff and create a data recovery plan. Whether your an

in house team looking for outsource business network security services or you are a company that is starting from square one, Computronix Has been building and securing networks for 25 years. Contact us today to make sure your business network is secure! To control the efficiency of cybersecurity protection, a carefully designed **security strategy** should provide for *quarterly* vulnerability assessment and *annual* penetration testing to detect, mitigate and manage cybersecurity risks. A company needs a cybersecurity strategy as it focuses on protecting the corporate network taking into account the staff using their personal mobile devices and laptops for business purposes (BYOD), wide use of cloud computing, etc. and provides direct guidance for company employees about acceptable behavior inside the corporate network.

**Results.** To ensure advanced protection of the corporate network, in addition to the elements of minimal protection – firewalls and antivirus – the following components should be applied:

Threat monitoring involves constant monitoring of the corporate network and the endpoints (servers, wireless devices, mobile devices, etc.) for the signs of cybersecurity threats, e.g., intrusion or data exfiltration attempts. Nowadays, threat monitoring is becoming even more important with the tendency at the enterprises to hire employees remotely and apply BYOD policy, which puts the protection of the corporate data and sensitive information under an additional risk.

Incident response (IR) deals with the situations when security breaches have already occurred. Thus, a company needs a special in-house or outsourced team prepared for the incidents, ready to detect actual events, find the causes and respond to cybersecurity threats with the least possible damage and the minimum time needed to recover from the attack. IR activities prevent small issues from transforming into bigger ones, such as data breach or system outage.

**Conclusion:** Corporate network security is not something that can be organized according to a general pattern equally suitable for any company. The choice of cybersecurity activities should depend on the size of a company, their budget, and the area they operate in. To ensure cyberprotection of a small corporate network, if there



is no necessity to secure their customers’ personal or financial data, applying firewall protection and antiviruses may be quite enough. However, if a company takes a relatively significant place in the area they operate in and may easily become a target of cyberattacks, they must be ready to extend the cybersecurity measures and apply email security, network segmentation, endpoint security, etc. Installing DLP and SIEM systems may also become a must-do, especially for organizations carrying out their activities in regulated industries. To maintain the chosen cybersecurity level, a company should conduct vulnerability assessment and penetration testing on a regular basis.

### **References:**

1. Morgan, Steve. “Global Cybercrime Damages Predicted to Reach \$6 Trillion Annually by 2021.” Cybercrime Magazine. Dec. 7, 2018. <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
2. Truta, Filip, Paul Vallee, Bill Ho, Roy Horev, Richi Jennings, and Michael Vizard. “Average Cost of a Cyberattack Now Exceeds \$1 Million, Research Shows.” Security Boulevard. January 17, 2019. <https://securityboulevard.com/2019/01/average-cost-of-a-cyberattack-now-exceeds-1-million-research-shows/>.
3. “Hiscox Cyber Readiness Report 2018.” Hiscox. February 2018. [https://www.hiscox.co.uk/sites/uk/files/documents/2018-02/Hiscox\\_Cyber\\_Readiness\\_Report\\_2018\\_FINAL.PDF](https://www.hiscox.co.uk/sites/uk/files/documents/2018-02/Hiscox_Cyber_Readiness_Report_2018_FINAL.PDF).
4. Forrest, Conner. “66% of SMBs Would Shut down or Close If They Experienced a Data Breach.” TechRepublic. October 2, 2017. <https://www.techrepublic.com/article/66-of-smbs-would-shut-down-or-close-if-they-experienced-a-data-breach/>