Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.01.2025.02

ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

# TYPES OF CYBERATTACKS TARGETING HR COMPANIES

**Mihaela Barhalescu[1], Alexandra Raicu[1]**

[1]Constanta Maritime University, Faculty of Naval Electro-Mechanics, 104 Mircea cel Batran Street, 900663, Constanta, Romania, e-mail address: mihaela.barhalescu@cmu-edu.eu, alexandra.raicu@cmu-edu.eu

***Abstract:*** Cyberattacks on a human resources company's Wi-Fi networks can expose client data and internal systems, damaging the company's reputation. This article outlines the major attack types and the implemented security measures by the company against cyberattacks, in the context of Wi-Fi network protection. A scenario of an attack is presented, aiming to prevent and minimize cyber risks and attacks. The measures discussed lead to improved security of networks and systems, strengthened data protection, and the development of a system capable of facing the constantly evolving cyber threats. They reduce risks of unauthorized access, financial losses, and reputational damage. To maintain a high level of security, employee education and constant monitoring are crucial. Furthermore, the managers of a human resources company can use the results of this study to protect clients, employees, and the company's confidential data, thereby improving business efficiency.
***Key words:*** Attacker techniques, cyberattack, cyber risk mitigation, cyber vulnerabilities, minimizing the risks of cyberattacks, security measures, security threats.

## 1. INTRODUCTION

Today, due to our increasing reliance on technology and internet access, Wi-Fi networks have become a vital part of our daily lives. However, a simultaneous rise in cyber threats has led to the emergence of a critical area of research and study, cyberattacks targeting Wi-Fi networks. These attacks pose a serious threat to both users and organizations, as they can compromise the confidentiality, integrity, and availability of data transmitted through Wi-Fi networks.

Wi-Fi networks are targeted by cyber attackers who use a variety of sophisticated techniques to gain unauthorized access to networks and compromise their security. They may exploit vulnerabilities in Wi-Fi security protocols such as WEP, WPA, or WPA2 to obtain encryption keys to intercept data traffic. Additionally, they may use brute force techniques to crack access passwords and infiltrate protected networks. Attackers can also perform 'man-in-the-middle' attacks, where they intercept and modify communication between users and Wi-Fi access points.

To protect their Wi-Fi networks against cyberattacks, defenders must consider a range of security measures and techniques, such as:

- Using strong security protocols, like WPA3, which provides enhanced encryption and more secure authentication.
- Implementing multi-factor authentication (e.g., two-factor authentication) to add an additional layer of protection.
- Properly configuring and regularly updating network equipment, including Wi-Fi access points, to fix vulnerabilities and apply the latest security patches.
- Monitoring networks for suspicious activities and implementing intrusion detection systems (IDS) to alert administrators in the event of a potential attack.
- Training users on security best practices, like steering clear of unsecured Wi-Fi networks and refraining from accessing suspicious websites or downloading files from untrusted sources.

Cyberattacks targeting Wi-Fi networks represent a significant risk, requiring heightened awareness from both attackers and defenders. By learning the methods employed by cybercriminals and adopting strong security protocols, we can protect Wi-Fi networks and sensitive information from such threats.

## 2. COMMON CYBERATTACKS ON HR COMPANIES

The most encountered cyberattacks can be classified in several ways, depending on the techniques used, the attack's purpose, or its source. [4]

A. According to the attack technique, cyberattacks can be:

- Phishing, when the attacker sends fake messages (via email, messenger, or WhatsApp) that appear to come from trusted sources, such as friends, courier companies, partners, employees, or banks and other companies, to convince the victims to reveal access

Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.01.2025.02
ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

credentials, personal information, or client data, such as passwords or credit card numbers of the company or its clients

- Malware, which is a type of software that can include viruses, Trojans, ransomware, spyware, etc., and is specifically designed to interfere with or compromise the functioning of a program.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, which involve overloading a server or network with artificial traffic, there by blocking business activities and making the system inaccessible to customers and company users
- Cross-Site Scripting (XSS) it is an attack method that involves embedding harmful code (typically JavaScript) into a webpage in order to steal information from user sessions.
- SQL Injection occurs when the attacker injects malicious SQL commands into a web application to manipulate or extract data from a company's database.

B. According to the purpose of the attack:

- The most common type of attack is data theft, which aims to acquire sensitive information, such as financial data, personal information of customers, or confidential details regarding products or services purchased by clients.
- Data destruction or alteration is a technique used by attackers to compromise an organization's operations or those of its clients.
- Extortion (ransomware) is perhaps the most common type of cyberattack, in which the attacker blocks access to a company's data or IT systems and demands a ransom for decryption.
- Defamation or reputation compromise is a type of attack typically aimed at damaging a company's reputation by exposing sensitive information or launching an attack that portrays the company as insecure or irresponsible.[2]

C. According to the source of the attack:

- Internal attacks originate from within the company, typically carried out by employees or individuals with access to the internal network.
- External attacks are launched by attackers attempting to breach the company from the outside, as they lack direct access to its internal networks.

## 3. CYBERATTACK SCENARIO IN AN HR COMPANY

In the current conditions, [5] the most predictable types of cyberattacks against a human resources company would be:

*"Customer Data Theft" attack*

An attacker manages to infiltrate the company's Wi-Fi network. Using network monitoring techniques, they intercept traffic and gain access to customers' personal data, including names, addresses, contact information, and payment details. The attacker exploits weak encryption protocols, misconfigured network settings, or unsecured access points to eavesdrop on data transmissions, capturing sensitive customer information in real-time before it reaches its intended destination. This information can later be used for fraud, selling the details, creating fake identities, or even blackmailing the customers in the database.

*"Ransomware" attack*

The attacker sends an email to an employee of the company containing a malware attachment disguised as a seemingly legitimate document. Due to the employee's inattention or lack of preparation, they open the attachment, allowing the malware to infiltrate the network.[1] The ransomware also spreads laterally across the network, exploiting vulnerabilities in unpatched systems or weak security configurations, potentially shutting down critical business operations and escalating the impact of the attack. The ransomware encrypts all of the company's important files and demands a sum of money to unlock them. If the demands are not met, the attacker threatens to publish the customers' data.[3]

*Denial of Service (DoS) attack*

The attacker can overload the servers with excessive traffic, thus affecting the HR company websites. As a result of this type of attack, online services may be disrupted, impacting customers' access to important information and affect the company processes.[8] In more sophisticated cases, the attacker may use a Distributed Denial of Service (DDoS) attack, leveraging a botnet of compromised devices to generate massive amounts of traffic, making it even harder to mitigate and prolonging service downtime.

*Payment system attack*

The attacker targets payment processing systems, gaining access to customers' credit card data.[4] This kind of attack is especially harmful, as it has the potential to cause widespread financial fraud and substantial losses for both customers and the company. The attacker can use Man-in-the-Middle (MitM) attacks to intercept information transmitted between the customer and the payment system or install physical devices on POS terminals or ATMs to copy customers' card data.

## 4. CYBERSECURITY BEST PRACTICES FOR HR COMPANIES

To protect customer data and the company's files, it must consider certain defence measures such as:

- *Wi-Fi network protection*: The company must ensure that the Wi-Fi network is secured with a strong protocol, such as WPA3, and use a different, unique and complex passwords for each user. Additionally, a multi

Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.01.2025.02
ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

factor authentication can be implemented to add an extra layer of security for Wi-Fi.

• *Firewall and security solutions*: Installing a firewall and updated security solutions can help protect the network against malware and ransomware attacks. These solutions must be regularly updated and configured to block any potential cyber threats.

• *Security policies and procedures*: The company should develop and implement clear cybersecurity policies and procedures. These should provide employees with guidelines on handling unsolicited emails or suspicious attachments and emphasize the importance of strong passwords and encourage regular updates of systems and software.

• *Data Encryption: Encrypting sensitive data both at rest on devices and during transmission* (including server and cloud data) is a crucial security measure. Additionally, it is essential to guarantee that all critical communications are encrypted end-to-end to safeguard against unauthorized access.

• *Employee Training and Awareness*: Providing employees with comprehensive training on cybersecurity threats and best practices is vital. This could involve educating them on how to identify phishing emails, avoid visiting insecure websites, and promptly report any suspicious activities. Regular cybersecurity drills and simulated phishing tests can also help reinforce awareness and ensure employees are prepared to respond effectively to potential threats.

• *Utilizing Strong Passwords and Multi-Factor Authentication (MFA):* Implementing long, intricate, and unique passwords for each account or application provides a robust layer of security that is highly effective. Furthermore, enabling multi-factor authentication (MFA) for all accounts that offer this feature adds an additional safeguard.[7],[9]

• *Access Control and User Permissions*: It is crucial for organizations to grant employees access exclusively to the data and resources they need to perform their duties, adhering to the principle of least privilege in order to mitigate potential risks. Conducting regular access audits is essential to verify that only authorized personnel have access to sensitive information. Additionally, regularly updating access passwords is an effective approach. An even more efficient way to manage access is through the implementation of an Identity and Access Management (IAM) system, which would allow centralized and streamlined access control.

• *Mobile Device Management*: If employees use their personal devices for work purposes, BYOD (Bring Your Own Device) policies can be put in place. In such cases, it is important to establish clear security and access guidelines to prevent data loss or theft. Implementing Mobile Device Management (MDM) solutions allows for better control and protection of mobile devices, ensuring enhanced security levels.

• *Data backup and recovery*: Implementing a data backup and recovery system can help the company protect its important information in case of a ransomware attack. Periodic backups should be created and stored in separate and secure locations.

• *Outsourcing data management to a cloud service, to a company specializing in data security and potential recovery in the event of any incident*.

• *Network Capacity Amplification*: The company should ensure it can handle a surge in traffic during a DoS attack by provisioning extra bandwidth. This helps minimize the risk of services being entirely disrupted during the attack.

• *Rate limiting*: To restrict the number of requests sent by a client within a time, the company can implement rate-limiting measures, especially in cases where the DoS attack is based on traffic volume.

• *Separating critical devices* (servers, IoT equipment, production networks) *into different sub-networks reduces the impact of a potential attack*.

• *Implementing AI driven threat intelligence solutions can help detect suspicious patterns and block attacks in real-time*.

By implementing these security measures and promoting a cybersecurity culture, the HR company can minimize the risks of cyberattacks and protect both customer data and its reputation in the industry.

To demonstrate that the cybersecurity measures taken by a company are correct and sufficient, it is important to follow a comprehensive approach that includes the following aspects:

• *Penetration testing*: A cybersecurity agency or security professional can conduct penetration tests to assess the HR company security system. These tests involve simulating a real attack to identify potential vulnerabilities and evaluate the effectiveness of the implemented security measures. The results of the tests can be used to highlight any issues and take additional corrective actions.

• *Network activity monitoring*: Implementing network activity monitoring solutions enables the detection and alerting of suspicious behaviour or potential cyberattacks. The logs and reports generated by these solutions can be analysed to evaluate the effectiveness of security measures and identify any attempted attacks.

• *Security audits*: Conducting periodic security audits by specialized third parties can provide an objective assessment of the security measures implemented in the HR company. These audits may include evaluating the network infrastructure, security policies and procedures, as well as the level of employee awareness and training.

• *Constant updating*: Keeping systems, software, and network equipment up to date with the latest security patches is essential to fix known vulnerabilities and benefit from the latest protection measures. Where is

Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.01.2025.02
ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

possible, configure automatic updates to minimize the risk of leaving systems vulnerable.

- *Security incident analysis*: If a security incident or an attempted attack occurs, analysing it can provide valuable insights into the effectiveness of the security measures. This analysis can help identify weak points and further improve the security system.
- *Ongoing employee training through case studies and outlining the steps to be taken in avoiding, resolving, or closing such situations*.
- *Risk assessment*: The company can identify vulnerabilities in systems, networks, and applications by conducting periodic cybersecurity risk assessments. This way, security measures can be prioritized.
- *Collaboration with Third Parties and Vendors*: Special attention must be given to evaluating the security of third parties, as they can pose potential risks. It is necessary to check the security measures of third parties or vendors who have access to the company's data or infrastructure and, if necessary, negotiate security measures. Subsequently, it must be verified that partners and vendors comply with the previously established cybersecurity standards and implement appropriate data protection protocols.
- *Security Incident Management*: Creating a detailed incident response plan that includes steps to follow in case of a cyberattack or security breach is essential for any company, as well as training a dedicated team within the company to be responsible for managing and quickly remediating security incidents.
- *Testing security systems*: To verify the systems and employees' response in the face of a real attack, the company must conduct cybersecurity attack simulations, such as penetration tests (pen testing).

By combining these measures and constantly testing the IT infrastructure, the company can reduce the mentioned attacks and protect the business.[6]

## 5. CONCLUSIONS

Cyberattacks on Wi-Fi networks represent a serious threat, requiring efforts from both attackers and defenders.

By understanding the techniques used by attackers and implementing appropriate security measures, we can contribute to protecting Wi-Fi networks and our sensitive data against these threats.

In conclusion, demonstrating that these measures are correct and sufficient to protect a human resources company from cyberattacks relies on a comprehensive and continuous approach to cybersecurity.

It is important to regularly assess the effectiveness of security measures and make updates and improvements based on changes in the cyber threat landscape.

Furthermore, fostering a cybersecurity aware culture within the organization is crucial. Employees should be continuously trained to recognize and respond to threats, while security policies and technologies must be regularly updated to counter evolving attack methods. A proactive and layered defence strategy, integrating advanced threat detection, encryption, and access controls, is essential to ensure the resilience of HR companies against cyber threats.

## 6. REFERENCES

[1] Laitinen, M., Armstrong-Smith, S. 2022, *Tackling cybercrime and ransomware head-on: Disrupting criminal networks and protecting organizations*, Cyber Security: A Peer-Reviewed Journal, 5(3), 190-205

[2]https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

[3]https://www.altospam.com/en/news/what-are-the-costs-of-a-cyber-attack-in-company/

[4] Chagadama, J., Luamba, D.S., Mutamba,E.,2022, *Cyberattacks: A Huge Concern for Small Business Sustainability*, Global Scientific and Academic Research Journal of Economics, Business and Management ISSN: 2583-5645 (Online)

[5] Slusky, L., 2020, *Cybersecurity of onlineproctoring systems*, Journal of International Technology and Information Management, 29 (1).

[6]https://www.researchgate.net/publication/372034587_The_Impact_of_Cyber_Security_on_Business_How_to_Protect_Your_Business

[7]https://www.researchgate.net/publication/367437452_Cybersecurity_of_Online_Proctoring_Systems

[8]https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[9] Bârsan, E., Anechitoaie, C., Bârsan, F.V., Iordanoaia, F., 2009, *Economical implications of the new international court of justice maritime delimitations in the Black Sea*, Journal of Marine Technology and Environment, vol.2, p.7-8, 2009, Nautica Publish House, Constanta, Romania.