Cybersecurity Questionnaire Report

Questionnaire Link:
https://forms.gle/wZvA1Bh5kEySYAC07

Brock Alexiadis ID:220256787

Contents

Purpose

This cybersecurity questionnaire is a thorough tool for evaluating employee understanding, adherence, and readiness about cybersecurity procedures across all of its branches. This 20-question survey, which aims to assess the degree of adherence to security rules and the efficacy of current security measures, covers a wide range of important cybersecurity topics.

In addition to covering more complex subjects like data encryption, social engineering knowledge, and incident reporting protocols, the questionnaire also covers basic cybersecurity hygiene themes like password management, device security, and software updates. It guarantees a comprehensive assessment of the organization's security posture by including inquiries about both digital and physical security procedures.

These questions help staff members to think critically about their own cybersecurity processes, pinpoint areas where they might be able to improve, and solidify their knowledge of security best practices. The questionnaire also functions as a teaching tool, informing users about prevalent dangers and offering advice on efficient risk mitigation.

Method

Google Forms will be used effectively to conduct the cybersecurity questionnaire. Employees can access the questionnaire from any internet-connected device by using a personalized link that will be sent to them via email or other communication channels. The security team can quickly and accurately compile well-organized responses with Google Forms' integrated data validation and response tracking tools. In addition, team members can collaborate more easily on analysis and follow-up tasks based on the questionnaire answers thanks to the platform's smooth connection with other Google Workspace applications. This approach not only optimizes the administrative procedure but also raises the cybersecurity assessment's general efficacy within the company.

Questions

The questions included in the questionnaire are:

1. Do you use strong, unique passwords for all your accounts, including work-related ones?
2. Are you aware of the company's password policy, including requirements for complexity and regular updates?

3. Do you lock your computer screen when stepping away from your desk?
4. Have you received cybersecurity training within the past year?
5. Are you familiar with common social engineering tactics, such as phishing emails, and do you know how to recognize and report them?
6. Do you regularly update your software and operating systems to ensure they are protected against known vulnerabilities?
7. Are you aware of the risks associated with using unsecured public Wi-Fi networks for work-related tasks?
8. Do you encrypt sensitive data before transferring it over the internet or storing it on portable devices?
9. Are you using multi-factor authentication for accessing company systems and applications?
10. Do you have antivirus software installed and regularly updated on your devices?
11. Are you aware of the company's policy regarding the use of personal devices for work purposes, especially regarding security measures like antivirus and encryption?
12. Have you enabled firewalls on your devices to block unauthorized access?
13. Do you avoid clicking on suspicious links or downloading attachments from unknown sources?
14. Are you familiar with the procedures for reporting security incidents or potential breaches to the IT security team?
15. Do you use a secure VPN connection when accessing company resources remotely?
16. Are you aware of the risks associated with using USB drives and other external storage devices and the precautions to take when using them?
17. Do you regularly review access permissions and revoke access for former employees or contractors?
18. Are you mindful of physical security measures, such as not leaving sensitive documents unattended or properly disposing of them when no longer needed?
19. Do you conduct regular backups of important data, and are you aware of the procedures for restoring data in case of loss or corruption?
20. Have you received any suspicious emails or encountered any unusual behavior on your devices that could indicate a security threat?

Results

We received six responses from employees indifferent departments inside our organization. The replies we received varied and provided insight into our security posture as a whole. While some staff members exhibited a thorough understanding of cybersecurity best practices and actively incorporated them into their everyday work, others indicated areas in which further education and awareness are required. The majority of employees mentioned employing strong passwords, upgrading software frequently, and being wary of social engineering techniques like phishing. Others have, however, occasionally acknowledged to being unaware of the organization's password policy or failing to use multi-factor authentication when logging into company networks. A small number of respondents also expressed confusion over the risks involved in utilizing public Wi-Fi networks and the appropriate channels for reporting security incidents.

Conclusion/Suggestions

Our company's security procedures have both strengths and room for development, as evidenced by the responses to the cybersecurity questionnaire. In order to reduce potential hazards and improve our overall cybersecurity posture, it is advised that we consider the following findings and recommendations:

- **Ongoing Education and Training:** Hold frequent cybersecurity training sessions to make sure all staff members are knowledgeable about corporate guidelines and recommended procedures. This ought to cover subjects like managing passwords, identifying social engineering techniques, and being aware of the dangers posed by different cyberthreats.
- **Enforce business policies:** uniformly throughout all branches, including those pertaining to the usage of personal devices for work, multi-factor authentication, and password complexity. Audits and reminders on a regular basis can strengthen compliance.
- **Improved Protocols for Responding to Incidents:** Examine and improve the protocols for reporting any security breaches or events. In the event of a security crisis, employees should know exactly who to contact and what to do. This will enable a prompt and well-coordinated reaction to minimize any harm.
- **Better Access Management:** To reduce the possibility of illegal access to confidential company information, periodically evaluate and update the access permissions for contractors, former employees, and other parties. This includes removing access as soon as an employee quits the company or changes positions.
- **Enhanced Risk Awareness:** Continue to educate people about the dangers of utilizing public Wi-Fi, downloading dubious attachments, and other prevalent cybersecurity issues. Workers must be armed with the information and resources necessary to recognize such hazards and take appropriate action.
- **Investing in Security Tools:** To strengthen defenses against emerging cyber threats, think about making investments in additional security tools and technologies, such as sophisticated antivirus software, endpoint detection and response (EDR) solutions, and secure file transfer protocols.

Through the implementation of preventative measures and addressing these areas, our organization may enhance its cybersecurity posture and more effectively safeguard its assets, data, and reputation against possible threats. To make sure we continue to be robust against new cyberthreats, it is imperative that we cultivate a culture of cybersecurity awareness and vigilance among all employees.