Problem Statement No:- 161

Cyber Hygine for Students (Ministry of Electronics and Information Technology (MEITY).)

As cyberattacks have increased around the world—interrupting businesses and government operations, and often leading to massive ransomware payouts and damaged corporate reputations—cyber hygiene has become a key method for creating operational resilience. Consider the disruption caused by the COVID-19 pandemic, which created opportunities for criminal hackers through email phishing, supply chain attacks, and password and malware attacks that preyed on millions of remote workers’ devices. Already in the first half of 2021, the global ransomware attacks have hit 304.7 million, surpassing last year’s total of 304.6 million.Devise a way to impart knowledge in children about cyber hygiene by fabrication of a cyber network that can be sustained through crowdsourcing.This project aims to create awareness about cyber hygiene in children. It requires the creation of a cyber network for children that can be sustained through crowdsourcing.

Materials

**Cyber hygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks. It’s like personal hygiene, where you develop a routine of small, distinct activities to prevent or mitigate health problems. Cyber hygiene practices include the inventory of all endpoints connected to a network, vulnerabilities management, and the patching of software and applications.**

As cyberattacks have increased around the world—interrupting businesses and government operations, and often leading to massive ransomware payouts and damaged corporate reputations—cyber hygiene has become a key method for creating operational resilience.

Consider the disruption caused by the COVID-19 pandemic, which created opportunities for criminal hackers through email phishing, supply chain attacks, and password and malware attacks that preyed on millions of remote workers’ devices. Already in the first half of 2021, the global ransomware attacks have hit [304.7 million](https://www.itproportal.com/news/previous-ransomware-records-already-obliterated-in-2021/), surpassing last year’s total of 304.6 million.

In response, the White House[has urged](https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf) government and business leaders to protect themselves by implementing foundational cyber hygiene best practices, noting that it is their critical responsibility to protect against threats with a strengthening of our nation’s resilience against cyberattacks. That’s because cyber hygiene is one of the surest ways to improve any organization’s overall security posture and defend against threats now and in the future.

**What are the benefits of cyber hygiene?**

Good cyber hygiene offers several benefits that ultimately put your organization in a better position to defend against cyberattacks. Specifically, it helps you:

* **Locate unmanaged assets:** You can’t protect what you can’t see. That’s why an accurate inventory of all your assets is the foundation for strong cybersecurity. Good cyber hygiene practices allow you to maintain an up-to-date [asset inventory](https://endpoint.tanium.com/what-is-it-asset-discovery-inventory/), identify vulnerabilities associated with any particular asset, and quickly resolve security gaps.
* **Protect customer data:**Cyber hygiene supports a range of proven security practices, such as patch management, password discipline, appropriate administrator privileges, and other measures that improve data protection.
* **Find outdated administrator privileges:** It’s easy to lose track of administrative rights as people move from one role or department to another or leave the company. But high-level administrative controls pose a significant security risk, so it’s important to regularly audit who has administrative privileges and how often they’re used. Outdated or long-forgotten privileges need to be immediately updated or revoked.
* **Identify rogue software:** Remote work has led many workers to install [unsanctioned software](https://endpoint.tanium.com/what-is-software-management/) on the devices and endpoints they use to connect to your network. That’s a problem. Chances are, that software hasn’t been properly configured, patched, updated, or secured, making it an attractive target for attackers. Cyber hygiene helps IT administrators gain visibility into all the software installed and used on their network so they can manage it or remove it.
* **Meet compliance requirements:** By identifying and prioritizing security risks and empowering IT teams to quickly remediate them, cyber hygiene makes it easier to track and report your organization’s security status and ensures it’s always aligned with regulatory and compliance requirements.

### What are the risks of poor cyber hygiene?

The results of poor cyber hygiene can cascade through your IT environment, resulting in multiple security vulnerabilities and potential attack vectors. Some of these include:

* **Data loss:** If local hard drives and online storage aren’t regularly backed up and maintained, important data can be lost through hardware failure, data corruption, improper handling, or ransomware and theft. The last carries a particularly dire cost: According to the Ponemon Institute’s most recent *Cost of a Data Breach Report*, for 2020, the overall [average cost of a ransomware breach is $4.44 million](https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/). And that was before the massive hacks on SolarWinds, Colonial Pipeline, and many other businesses.
* **Misplaced data:** Data that aren’t organized in a proper file system are vulnerable to being misplaced, and the problem increases exponentially as the organization grows.
* **Software vulnerabilities:** Poor patch management and old or out-of-date software are a common cause of breaches at organizations of all sizes. Software developers regularly release patches and updates to fix known vulnerabilities in their products, but if an organization doesn’t have a process for applying them on a timely basis, hackers can potentially exploit these applications to gain access to the network.
* **Malicious software:**[More than 350,000 new malicious programs](https://www.av-test.org/en/statistics/malware/) are registered every day. If antivirus and other security products aren’t regularly updated to keep pace with this constantly changing landscape, hackers can use a range of malicious software to get inside the company network and set up more targeted attacks.
* **Inadequate vendor risk management:**With today’s hybrid IT environments, focusing on your own security posture is not enough. You have to consider the potential security risks posed by [third-party vendors and service providers](https://www.tanium.com/blog/measuring-risk-using-supply-chain-approach/) that have access to your network and process your sensitive data. Failing to understand and manage the level of risk your vendors introduce can leave you further exposed to service disruptions and breaches.
* **Lack of compliance:** The issues resulting from poor cyber hygiene can be compounded, leaving gaps in your compliance with PCI, DSS, HIPAA, or other regulatory frameworks.
* **Security breach:**The worst outcome of poor cyber hygiene is a successful cyberbreach. Improper configuration management, poor vulnerabilities management, and weak security policies and threat response procedures can leave your organization exposed to data theft, business disruption, and massively expensive ransomware payouts. Ultimately, these can result in huge financial costs, a damaged reputation, and a loss of customer loyalty.