Volume 2 Issue 5

Date: 01.06.2025

Cybersecurity Digest

Bi-Weekly update by the CISO Section of Meghalaya Rural Bank

Threat:

A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system. Examples of threats include computer viruses, Denial of Service (DoS) attacks, data breaches, etc.

Vulnerability:

In cybersecurity, a vulnerability is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals. In some very rare cases, cyber vulnerabilities are created as a result of cyberattacks, not because of network misconfigurations. Even it can be caused if any employee anyhow downloads a virus or a social engineering attack.

Risk:

Cyber risk is a potential consequence of the loss or damage of assets or data caused by a cyber threat.

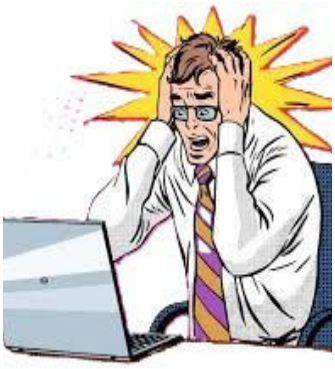
Human Cyber Risk– The First Line of Defence

Humans are often regarded as the weakest link in a cybersecurity program. Whether resulting from manipulative cybersecurity tactics or limited cybersecurity awareness, human errors remain the most prevalent attack vectors in every information security program, no matter how sophisticated your cybersecurity stack may be.

Human cyber risk refers to potential human behaviors that could result in a cyber incident. These could include clicking on malicious phishing email links or providing sensitive internal information to unauthorized persons.

In cybersecurity, a human vulnerability is any area of weakness that could result in a security breach. Unlike digital cyber threats, which could be exploited programmatically by reverse engineering software flaws, human vulnerabilities are exploited by manipulating human behavior.

The human element is complex, and not all individuals share the same vulnerabilities—some are more susceptible to a phishing attack than others. An experienced cybercriminal determines each person's unique area of weakness and devises a plan to exploit that weakness to advance their cybercrime objectives.



Human risk factors in Cybersecurity

Human risks are predominantly concentrated at the IT security boundary, at the interface of cybercriminals, and in an organization's private network. This is why human errors usually facilitate initial network access to unauthorized users. Cybercriminals aim to exploit this gateway, and they have cultivated their tactics to exploit the human factors of cybersecurity with the following types of attacks:

Phishing email attacks: When hackers send emails containing links infected with credential-stealing malware to employees to gain access to the corporate network.

Social engineering attacks: When hackers try to trick employees into exposing sensitive internal information, either via a phone, in-person conversation, or an internal messaging tool, such as Slack.

Poor Cyber Hygiene Actions

Even without prompting from hackers, human errors can permeate the information technology boundary with the following poor cyber hygiene actions:

- **Shadow IT practices:** When applications and external hardware are connected to corporate networks and devices without first being approved by the IT department. Such practices create attack surface bloats security teams are unaware of, making these regions of the digital surface perpetualy vulnerable to cybercriminal compromise.
- **Accidental data sharing:** Sending sensitive internal information, such as customer data, to the wrong email address.
- **Neglecting Multi-Factor Authentication (MFA):** Failing to set up MFA for critical business accounts.
- **Ignoring security warnings:** Bypassing browser security alerts (e.g., ignoring "*This connection is not secure*" warnings) or disabling antivirus software to remove interruptions associated with a desired action.
- **Delayed software updates:** Postponing or ignoring prompts for system and software updates.
- **Insider threats:** When an employee abuses their internal credentials to access sensitive internal information that is then leaked outside of the corporate network.
- **Neglecting secure communication protocols:** Discussing confidential business matters over unsecured or public channels, such as personal email accounts, messaging apps, or during in-person interactions.
- **Inadvertent social media disclosures:** Employees sharing too much information about their workplace position and activities, such as company projects or upcoming corporate travel plans, could arm hackers with enough intelligence to launch a targeted phishing attack.

Best practices for reducing Cyber Human Risk

Personalised, role-specific training: Training isn't a one-size-fits-all solution. Make sure content is being adapted to each employee's role, location and cyber knowledge level..

Leadership commitment: Ensure that leadership demonstrates a commitment to cybersecurity, setting an example for the rest of the organization.

Open communication: Encourage open communication about security issues and make it easy for employees to report suspicious activities without fear of repercussions.

Recognition and rewards: Recognize and reward employees who demonstrate positive security practices.

Incident response plans: Develop and regularly update incident response plans to ensure a swift and effective response to security incidents.

Regular software updates: Ensure all software and systems are regularly updated and patched to protect against known vulnerabilities.

Secure browsing practices: Educate employees about secure browsing habits and the risks of downloading software from untrusted sources.

Physical security: Emphasize the importance of physical security measures, such as locking screens when away from desks and securing sensitive documents.

Multi-factor authentication (MFA): Require MFA for accessing sensitive systems and data to add an extra layer of security.

Cyberattack via Picture? No OTP, No Link—Hackers Just Need One WhatsApp Image Now

In the digital age where phishing links and OTP frauds are the usual suspects, a new threat has emerged—one that hides in plain sight. Hackers are now using WhatsApp images as Trojan horses to deliver malware directly into users' devices. Unlike conventional scams, this technique relies on steganography, a method where malicious code is embedded within seemingly harmless image files.

Once the infected image is opened, the malware installs silently on the victim's phone. From there, it can siphon sensitive data—banking credentials, one-time passwords, and even carry out unauthorized financial transactions—without the user's knowledge.