Cybersecurity Risks: A Growing Threat to Business Stability

Muhammad Shahab Iqbal
Assistant Vice President / Head of Business Applications
Al Meezan Investments

A chain is only as strong as its weakest link – and in today's era, where most of our lives have been transformed into a digital landscape, one weak password, unpatched system, or lack of cybersecurity awareness can be the breaking point, resulting in a cascading effect that impacts multiple systems and causes significant data, reputational, and financial loss. Cybercriminals don't need to defeat the entire defense system; they can find and exploit that one weakest link in the chain to gain access to critical systems and information. In this article, we'll explore how cyber threats expose these vulnerabilities, their impact, and what measures we can take to strengthen our systems and safeguard our digital identity.

Imagine your digital world as a Jenga tower, where each block represents a digital element such as cloud services, IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service), IoT devices, digital wallets, third-party services, and many more. The higher the tower goes, the more unbalanced and vulnerable it becomes, where the black hat only needs to pull out one block to dismantle the entire ecosystem.

Each technological innovation or layer comes with its own risk, adding more complexity to the systems and making it harder to monitor and secure each endpoint, gap, and doorway for ransomware, data breaches, and thefts to occur. With this, it's becoming increasingly important for businesses to balance the innovation and usage of technology with the required security strategies like continuous monitoring, threat intelligence, user awareness, and a Zero Trust policy. With increasing digital adoption, attackers now have an enormous attack surface available to exploit vulnerabilities. These threats may occur individually or in various combinations of the following, out of the wide range already available and new ones constantly being developed:

a) **Malware –** Software designed to penetrate systems to steal data, disrupt operations, and gain unauthorized system access. These include viruses, worms, trojans, ransomware, and spyware.

b) **Phishing –** Deceptive communication, such as emails, messages, and chats, used to trick people into revealing sensitive information like personal details, account credentials, PINs, and access codes, or installing malware that either steals or encrypts the data—against which a huge ransom is then demanded for decryption.

c) **Denial-of- Service (DoS) Attack –** Overloading a system with bot-generated traffic to make it unavailable to legitimate users. This attack exhausts network resources due to the high volume of requests received, resulting in the system becoming unresponsive. DoS attacks can take various forms—such as ICMP flood, SYN flood, and UDP flood—but all share a common goal: to drain network resources. Distributed Denial of Service (DDoS) is a more severe version, as the attack originates from multiple sources, making it more complex and difficult to mitigate.

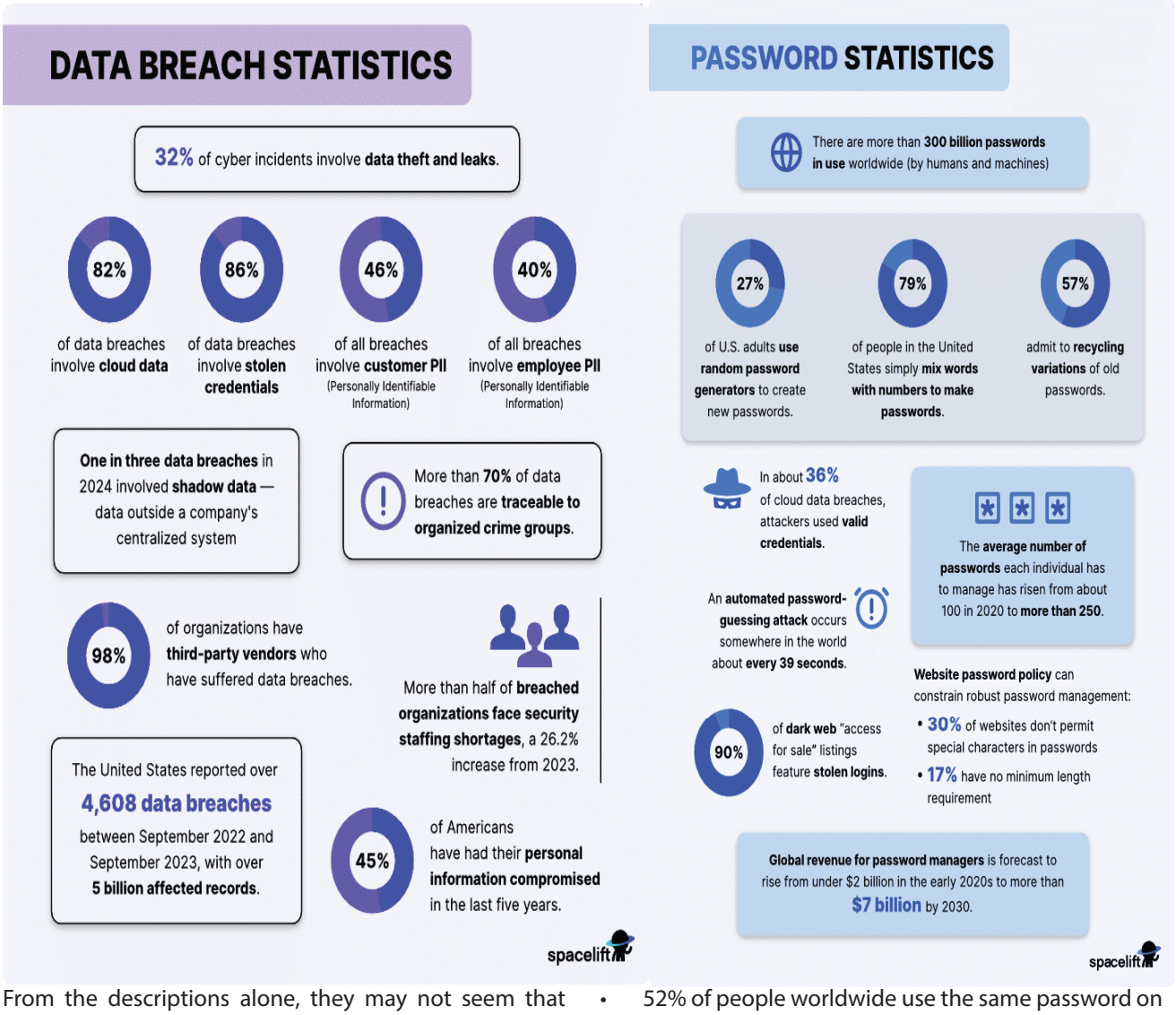
d) **Man-in-the-Middle (MitM) Attack –** This type of attack works by intercepting communication between two points, allowing attackers to eavesdrop, modify the data, mimic legitimate requests, and compromise data integrity.

e) **Cross-Site Scripting (XSS) Attack –** Attackers embed malicious scripts on websites that get executed on users' web browsers. This can result in stealing personal information, credentials, and credit card details, modifying website content and appearance, or exploiting browser vulnerabilities to install malware and gain system access.

f) **Zero-Day Exploits –** Like human systems, digital systems also possess weaknesses. Many reaches production unnoticed, and these can be exploited by attackers.

At times, these exploits can have severe impacts because they are previously unknown in the system before being used by attackers—and remain vulnerable until a patch is deployed.

g) **Brute Force Attack –** A trial-and-error method to guess passwords, login credentials, PINs, and encryption keys until one attempt succeeds. Once cracked, not only is the individual system compromised, but other connected systems can also be exposed and exploited.



From the descriptions alone, they may not seem that impactful or severe—unless we delve into some global statistics and facts.

Human Error Element

- 74% of all breaches involve human involvement, whether through error, privilege misuse, stolen credentials, or social engineering.
- Phishing remains a prevalent threat, accounting for 44% of social engineering incidents.
- More than 50% of social engineering incidents involve Business Email Compromise (BEC) attacks, in which criminals attempt to dupe a senior executive or budget holder into transferring money or disclosing sensitive information.

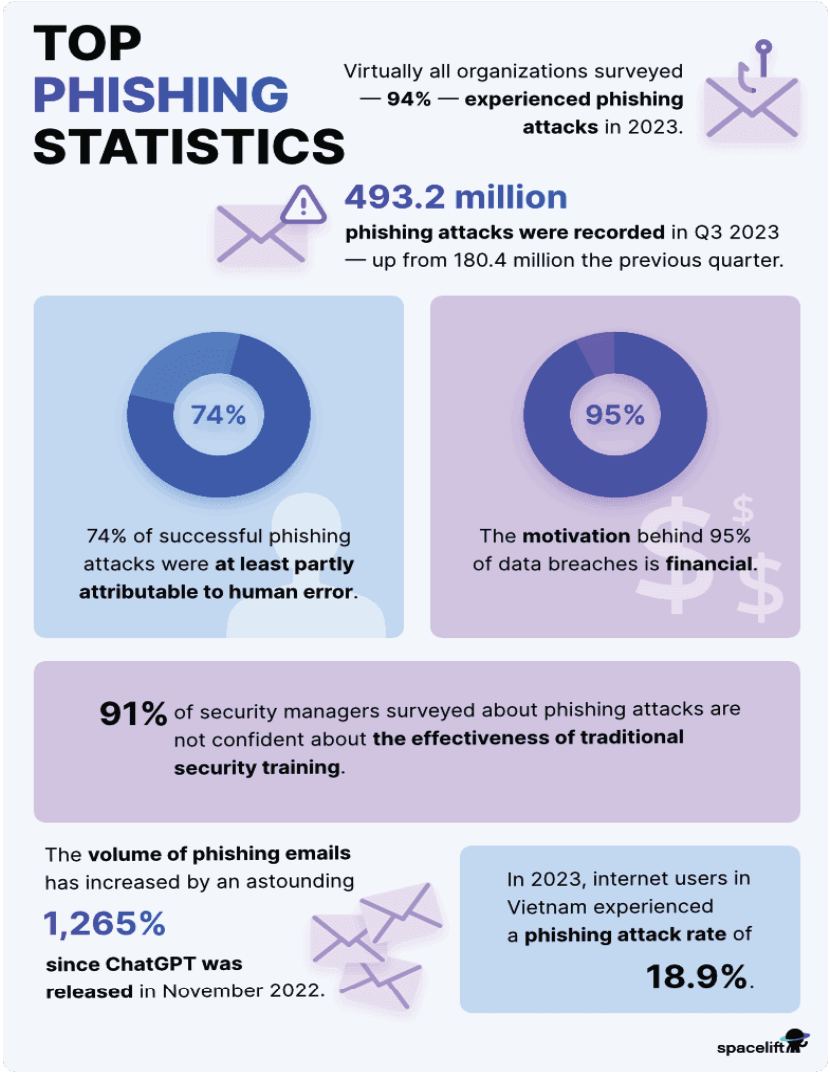
Password Statistics

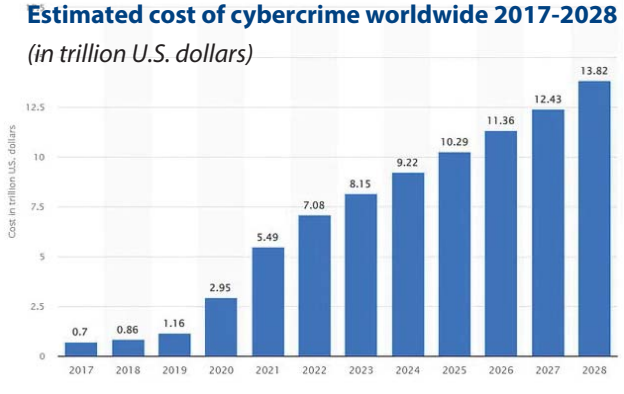
- Globally, 78% of people admit to reusing the same passwords.
- Almost 24 billion usernames and passwords were reported as compromised in 2022 alone.
- 52% of people worldwide use the same password on at least three accounts.
- 44% of internet users rarely or never change their passwords.
- 34% of people use slight variations of the same password repeatedly (e.g., adding numbers or symbols to an old password).
- More than 36% of internet users write passwords down on paper.
- Only 15% use a password manager.
- 53% of IT professionals have shared passwords via email in plaintext.
- In 2023, the most common password was "123456." It can be cracked in under a second.
- 88% of passwords used in successful attacks were 12 characters or fewer.
- 35% of victims of an account takeover enabled two-factor authentication afterward.

Price Tag

When data and/or systems are compromised, the financial aftermath can be severe and, at times, lead to irreversible damage and devastation. Costs include legal issues, regulatory and compliance fines, system recoveries, and other expenses, all of which significantly impact routine operations, stock values, and partnerships. Lastly, the most severe consequence of all is the erosion of customer trust—something no budget can restore or repair. According to sources:

- The cost of cybercrime worldwide is predicted to reach $10.29 trillion in 2025, with a 15% annual increase.
- In 2024, the average cost of a single data breach hit an all-time high of $4.88 million—a 10% jump from the previous year.
- On average, a data breach costs $165 per record.
- Organizations employing fewer than 500 people spent 13.4% more on managing data breaches in 2024, with the average cost now standing at $3.31 million.





Cyber Warfare

According to the Microsoft Digital Defense Report 2024, over 600 million cyberattacks occur every single day, targeting sensitive information and critical infrastructure. The report also highlighted the emerging alliance between cybercrime gangs and nation-state-affiliated threat actors, who are now collaborating to support geopolitical conflicts by sharing tools and techniques to increase the sophistication and impact of their attacks.

History is full of high-profile cyberattacks that have immobilized business operations for days or even weeks, resulting in massive financial losses, service disruptions, and the exposure of sensitive information. In many cases, the affected organizations had no option but to pay substantial ransom amounts to regain access to their systems and resume operations.

A few notable examples include:

- **NotPetya and WannaCry (2017) –** NotPetya impacted major companies and organizations worldwide, disrupting operations for several days. WannaCry encrypted Windows operating systems globally, demanding large ransom payments.
- **Equifax Data Breach (2017) –** Exposed the personal data of 148 million people. A settlement was reached with the company, offering compensation and assistance to affected users.
- **Colonial Pipeline Ransomware Attack (2021) –** A major U.S. fuel pipeline was targeted in a cyberattack that compromised several computerized systems managing the pipeline. The attack led to a severe fuel shortage, and the company paid approximately $5 million to restore operations.
- **SolarWinds Supply Chain Attack (2020) –** Attackers exploited a vulnerability in a software update distributed to thousands of organizations, including government agencies and corporations, gaining remote access to their networks. The financial impact was estimated to be an average of $12 million per affected company.

Cyberattacks have increasingly become a component of traditional warfare. During the Pak-India conflict, both countries engaged in cyber warfare alongside conventional exchanges. The Securities and Exchange Commission of Pakistan (SECP) issued warnings to local companies about heightened cybersecurity threats, advising strict access controls, regular vulnerability assessments, and a comprehensive response plan to counter potential attacks.

Safeguarding Your Digital Assets

While the technological aspect enhances the sophistication and innovation of these increasingly complex attacks—which have a significant impact—the fundamental safeguards against them remain unchanged. Users must adhere to these practices to avoid unpleasant experiences that could compromise their identity, personal data, or lead to financial losses.

- **Data Backups –** Regularly back up your data both online and offline. Utilize available auto-backup options or trustworthy third-party utilities to ensure backups aren't missed. Frequently practice restoring these backups so you're familiar with the necessary steps.
- **Strong Passwords and MFA –** Use a lengthy, complex, and difficult-to-guess combination of mixed-case letters, numbers, and special characters as your password. Change it at least every two months, avoid reusing passwords across platforms, and use a password manager to generate and store them. Wherever possible, enable and use Multi-Factor Authentication (MFA).
- **Antivirus and Firewall –** Use these to protect yourself from malware, prevent unauthorized system access, and control network traffic. Most importantly, never skip updates for your operating system, applications, and security software.
- **Network Security –** Secure your Wi-Fi with a strong password and avoid using public Wi-Fi networks.
- **Phishing Awareness –** Be cautious with suspicious emails, attachments, and links. Only proceed after verifying that the source is legitimate. No authentic communication will ever ask for your password, OTP, PIN, or MFA code.

When it comes to organizations, they must go beyond basic measures to ensure protection of critical assets and readiness to counter incidents. A few actions that can be taken—alongside regular security audits, dark web monitoring for leaked credentials, awareness sessions, cyberattack drills, and incident preparedness—include:

- **Zero Trust Policy –** Always verify, assuming that breaches can come from both external and internal sources.
- **Micro-Segmentation –** Divide the network and environments into granular security zones to restrict attacker movement and reduce the blast radius in case of a breach.
- **Least Privilege Access –** Provide only Just-In-Time (JIT) and Just-Enough-Access (JEA) to users.
- **Behavioral Biometrics –** Monitor how users interact with systems for continuous background identity verification. Trigger step-up authentication if there are anomalies like unusual typing rhythm, scroll speed, access to critical systems at odd hours, etc.
- **Deceptive Technology –** Deploy honeypots (fake assets) to deceive attackers and trigger alerts when they interact with them.
- **Privileged Access Management (PAM) –** Implement PAM to control, monitor, and secure access to highly critical systems and accounts.
- **Encrypted Traffic Analysis & Homomorphic Encryption –** Detect malicious activity in encrypted traffic and process data without decrypting it to preserve privacy.
- **Q-Day –** With emerging technology, we are not far from the anticipated quantum apocalypse. A day predicted in 2030 by the National Institute of Standards and Technology (NIST), when a quantum computer could break current encryption algorithms, thereby compromising critical data, systems, and infrastructures. Organizations worldwide are researching and preparing for a transition to quantum-safe environments.

Future of Cybersecurity

Even with all of this, the coming times will reveal a shocking progression as AI-powered defense systems confront AI-powered threats. There will be a paradigm shift in the cybersecurity landscape, with AI-backed deepfake social engineering, bypassing biometric authentication, impersonations, social media analysis to time attacks, poisoning machine learning models, polymorphic malware, algorithmic swarming, LLMs generating custom exploits, fake videos, invoices, receipts, reports—every possibility imaginable.

To survive, this era will demand more than tools—it will require a reshaping of security strategies and adaptation to new technologies. Organizations that embrace this shift, find the right balance between human and artificial intelligence, and transition accordingly will thrive. Those that fail will stand defenseless against threats powerful enough to bring them down in a matter of minutes.

Patch installed – the vulnerability landscape proliferates

About the Author: *The author is a certified PMP®, CSM®, AWS®, and MPM professional with over 13 years of experience in technology leadership and project management. He currently serves as Assistant Vice President and Head of Business Applications at Al Meezan Investments, where he leads strategic digital transformation initiatives, modernizes core systems, and aligns technology with business objectives across fintech, AI, cybersecurity, and related sectors.*