Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

MEGHALAYA RURAL BANK

Vol 2 Issue 24
Date: 16-03-2026

Cybersecurity is a shared responsibility

Risks associated with inadequate cybersecurity measures:

1. Reputational Damage
2. Data Breaches
3. Financial Losses
4. Disruption of Business Operations
5. Legal and Regulatory Consequences

Data Breach

A data breach is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information).

The terms "data breach" and "breach" are often used interchangeably with "cyberattack." However, not all cyberattacks are data breaches. Data breaches include only those security breaches where someone gains unauthorized access to data.

For example, a distributed denial of service (DDoS) attack that overwhelms a website is not a data breach. A ransomware attack that locks up a company's customer data and threatens to

leak the stolen data unless the company pays a ransom is a data breach. The physical theft of hard drives, USB flash drives or even paper files containing sensitive information is also a data breach.

Why data breaches happen

Data breaches are caused by:

- **Innocent mistakes**, such as an employee emailing confidential information to the wrong person.
- **Malicious insiders**, including angry or laid-off employees who want to hurt the company or cause reputational damage, and greedy employees who want to profit off the company's data.
- **Hackers**, malicious outsiders who commit intentional cybercrimes to steal data. Hackers can act as lone operators or part of an organized ring.

Financial gain is the primary motivation for most malicious data breaches. Hackers steal credit card numbers, bank accounts or other financial information to directly drain funds from people and companies.

Some attackers steal personally identifiable information (PII)—such as Social Security numbers and phone numbers—for identity theft, taking out loans and opening credit cards in their victims' names. Cybercriminals can also sell stolen PII and account information on the dark web, where they can fetch as much as USD 500 for bank login credentials.

A data breach can also be the first phase of a larger attack. For example, hackers might steal the email account passwords of corporate executives and use those accounts to conduct business email compromise scams.

Data breaches might have objectives other than personal enrichment. Unscrupulous organizations might steal trade secrets from competitors, and nation-state actors might breach government systems to steal information about sensitive political dealings, military operations or national infrastructure.

How data breaches happen

Most intentional data breaches caused by internal or external threat actors follow the same basic pattern:

1. **Research**: The threat actor identifies a target and looks for weaknesses that they can use to break into the target's system. These weaknesses can be technical, such as inadequate security controls, or human, such as employees susceptible to social engineering.
2. **Attack**: The threat actor starts an attack on the target by using their chosen method. The attacker might send a spear-phishing email, directly exploit vulnerabilities in the system, use stolen login credentials to take over an account or leverage other common data breach attack vectors.
3. **Compromise data**: Inside the system, the attacker locates the data they want and does what they came to do. Common tactics include exfiltrating data for sale or use, destroying the data or locking up data to demand a ransom.

Data breach prevention and mitigation

According to the *Cost of a Data Breach 2025* report, it takes an average of 241 days to identify and contain an active breach across all industries. Deploying the right security solutions can help organizations detect and respond to these breaches faster.

Standard risk management measures, such as regular vulnerability assessments, scheduled backups, timely patching and proper database configurations, can help prevent some breaches and soften the blow of those that occur.

However, many organizations today implement more advanced controls and best practices to stop more breaches and significantly mitigate the damage they cause.

Data security tools

Organizations can deploy specialized data security solutions to automatically discover and classify sensitive data, apply encryption and other protections and gain real-time insight into data usage.

AI and Automation

Organizations that extensively integrate artificial intelligence (AI) and automation into security operations resolve breaches 80 days faster than those that don't, according to the *Cost of a Data Breach 2025* report. The report also found that security AI and automation reduce the cost of an average breach by USD 1.9 million or a savings of over 34% (as compared to organizations that don't use security AI and automation).

Many data security, data loss prevention and identity and access management tools now incorporate AI and automation.

Employee training

Because social engineering and phishing attacks are leading causes of breaches, training employees to recognize and avoid these attacks can reduce a company's risk of a data breach. In addition, training employees to handle data properly can help prevent accidental data breaches and data leaks.

Identity and access management (IAM)

Password managers, two-factor authentication (2FA) or multifactor authentication (MFA), single sign-on (SSO) and other identity and access management (IAM) tools can protect employee accounts, VPNs and credentials from theft.

Organizations can also enforce role-based access controls and the principle of least privilege to limit employee access to only the data that they need for their roles. These policies can help stop both insider threats and hackers who hijack legitimate accounts.