BLOG POST

mimecast

Preventing a Data Breach

It's difficult to understate the true impact of data breaches, after all, the most famous have cost billions

AUGUST 11, 2026

Key Points

- Understanding how data breaches occur and implementing proactive strategies like strong access controls, regular software updates, and employee training are essential for preventing them.
- Common causes of data breaches include phishing attacks, weak passwords, unpatched software, insider threats, physical theft, and malware.
- Staying informed about emerging threats and continuously adapting cybersecurity measures are crucial for maintaining robust data protection.

While data breaches may seem like an inescapable part of our online lives, there are ways to prevent and mitigate their impact and ensure that your organization and its users are protected.

To achieve this, it's important to understand how data breaches work, some of their most common causes, and how to start implementing strategies that allow your organization to work proactively and responsively toward elimination and mitigation.

What is a data breach?

A data breach occurs when sensitive, protected, or confidential data is accessed, disclosed, or stolen by an unauthorized entity through various means, including hacking, insider threats, malware, or even physical theft. The consequences of a data breach can be severe, leading to financial losses, legal penalties, and damage to an organization's reputation. Generally speaking, the kinds of data that are stolen or held for ransom include:

- Personal information: Including names, addresses, Social Security numbers, and other personal identifiers.
- Financial information: Including credit card numbers, bank account details, and transaction records.
- Health information: Including medical records, health insurance details, and other health-related data.
- Intellectual property: Including proprietary business information, trade secrets, and research data.

Common causes of data breaches

Understanding the common causes of data breaches is essential for developing effective prevention strategies. Data

breaches can occur through various means, often exploiting weaknesses in an organization's security posture — and increasingly, they exploit people rather than technology. Human touchpoints are now the fastest-growing attack vector, with phishing accounting for a large majority of attacks as adversaries scale their use of AI. Identifying these causes helps address vulnerabilities and implement measures to protect sensitive information. The following are some of the most common causes of data breaches today:

- **Phishing attacks:** Phishing involves tricking individuals into providing sensitive information by pretending to be a trustworthy entity. AI has made these attacks faster to produce and harder to spot.
- **Weak passwords:** Inadequate password policies and weak passwords can make it easy for attackers to gain unauthorized access.
- **Unpatched software:** Software vulnerabilities can be exploited by attackers if not regularly updated and patched.
- **Insider threats:** Employees or contractors with access to sensitive data can intentionally or unintentionally cause a data breach.
- **Physical theft:** Loss or theft of devices such as laptops, smartphones, or USB drives can lead to data breaches.
- **Malware:** Malicious software can infiltrate systems and exfiltrate sensitive information.

Strategies to prevent data breaches

Preventing data breaches requires a proactive and comprehensive approach, combining advanced technology, robust policies, and informed employee practices. Because a small fraction of users often account for the majority of security incidents, the most effective programs focus on managing human risk — giving security teams visibility into who is risky and empowering them to intervene before a mistake becomes a breach. By understanding and implementing key strategies, your organization may be able to significantly mitigate the risks of unauthorized access and data loss. The following strategies outline essential measures to strengthen your organization's defenses against potential breaches, however, it's important to remember that, as cyberthreats grow more advanced, your strategies should evolve along with them.

1. Implement strong access controls

Access control mechanisms ensure that only authorized individuals have access to sensitive information. This can be achieved through:

- Role-based access control (RBAC): Assign permissions based on the user's role within the organization.
- Multi-factor authentication (MFA): Require multiple forms of verification before granting access.
- Least privilege principle: Grant users the minimum level of access necessary to perform their job functions.

2. Regular software updates and patch management

Keeping software up to date is crucial for protecting against known vulnerabilities. Establish a regular schedule for:

- Patch management: Prioritize patches and updates to ensure you address the highest risks as soon as possible.
- Vulnerability scanning: Regularly scan systems for vulnerabilities and address them promptly.

3. Employee training and awareness programs (security behavior management)

Human error is a significant factor in many data breaches. Rather than relying on one-size-fits-all annual training, educate employees through risk-based programs that focus intervention where it matters most. Mimecast Engage delivers real-time, behavior-driven interventions and adaptive training — powered by the Human Risk Command Center — to help employees make better decisions at the right moment, including:

- Phishing awareness: Train employees to recognize and report phishing attempts, reinforced by real-world simulated phishing and individual risk scores.
- Secure password practices: Encourage the use of strong, unique passwords and the implementation of password managers.
- Data handling procedures: Ensure employees understand how to handle and store sensitive information securely.

4. Data encryption

Encryption protects data by making it unreadable to unauthorized users. Implement encryption for:

- Data at rest: Encrypt sensitive data stored on servers, databases, and other storage devices.
- Data in transit: Use encryption protocols (e.g., TLS/SSL) to protect data being transmitted over networks.

5. Regular security audits and assessments

Conduct regular security audits to identify and address potential weaknesses in your cybersecurity posture. This includes:

- Penetration testing: Simulate attacks to identify vulnerabilities.
- Compliance audits: Ensure adherence to relevant regulations and standards (e.g., GDPR, HIPAA).

6. Implement advanced threat detection and response

Utilize advanced technologies to detect and respond to threats in real-time. Modern approaches also apply behavioral analytics to how data actually moves — surfacing genuine exfiltration risk without the false-positive floods of legacy DLP. This includes:

- AI-powered email security: Defend against sophisticated email attacks — including BEC, phishing, malware, and impersonation — with Mimecast Advanced Email Security, since the overwhelming majority of attacks still begin with email.
- Behavioral data loss prevention: Monitor how sensitive data moves across endpoints, browsers, cloud, SaaS, and email with Mimecast Incydr, prioritizing real threats over noise.
- Unified human risk visibility: Aggregate behavior-based risk signals across your security ecosystem in the Human Risk Command Center to quantify risk and respond faster, aided by AI-powered investigation.
- Security Information and Event Management (SIEM): Collect and analyze security-related data from various sources to detect and respond to threats.

Emerging threats in data security

As technology continues to evolve, so do the tactics and techniques used by cybercriminals. Emerging threats in data security present new challenges for organizations aiming to protect their sensitive information. Staying informed about these evolving threats is crucial for maintaining a robust cybersecurity posture. Below are some of the emerging threats in data security of which organizations need to be aware:

Artificial intelligence and machine learning exploits

The increasing use of artificial intelligence (AI) and machine learning (ML) in cybersecurity is a double-edged sword. While these technologies enhance security defenses, they also introduce new challenges. The vast majority of organizations now use AI to defend against threats, yet most remain concerned about sensitive data exposure through generative AI tools, and many still lack a strategy to address AI-driven threats. Prompt injection attacks can cause generative AI applications to reveal sensitive information, and employees eager to benefit from these tools may enter confidential data into them, creating new pathways for data leakage, impersonation, and policy drift.

Deepfake and synthetic identity fraud

Deepfake technology, which uses AI to create realistic fake videos and audio, poses significant threats to data security and personal privacy. Similarly, synthetic identity fraud involves creating fictitious identities using a combination of real and fake information.

Quantum computing threats

Quantum computing, while still in its early stages, poses potential future threats to data security due to its capability to break traditional encryption methods.

Supply chain attacks

Supply chain attacks involve compromising an organization by targeting less secure elements within its supply chain, such as third-party vendors or software providers.

AI agent risk

As organizations deploy a rapidly growing number of AI agents, these autonomous tools introduce new attack surfaces. Securing how employees and AI tools interact in real time — with adaptive controls and open ecosystem integrations — is becoming essential to preventing data leakage and impersonation.

FAQs

What steps should you take if you've had a data breach?

If you experience a breach, quickly contain and assess the damage by identifying affected systems and data. Notify relevant authorities and affected individuals, and work with cybersecurity professionals to remediate vulnerabilities and prevent future incidents.

How can you protect data after a breach?

After a breach, prevent the attacker from regaining access and monitor your accounts for unusual activity. Review lessons learned and identify opportunities to strengthen security measures and improve your incident response process.

How can you ensure your organization is prepared for a potential data breach?

Prepare for a potential breach by developing a comprehensive incident response plan that includes regular security audits, employee training, and robust access controls. Regularly update and test your security measures to adapt to evolving threats and ensure a swift, effective response.

The bottom line

Data breaches are common enough in today's online world, however, if we are unable to identify, mitigate, and stop these kinds of attacks then the way our data is used and stored will become unsustainable. The good news is that, through a multi-faceted approach that combines technological measures, policy development, and a focus on human risk, your organization can take action to significantly reduce the associated risk and impacts.