Published on *The National Law Review* https://natlawreview.com

Data Privacy Insights Part 2: The Most Common Types of Data Breaches Businesses Face

Article By:

Angela P. Doughty

As part of Data Privacy Awareness Week, Ward and Smith is spotlighting the most common types of data breaches that businesses encounter.

In Part 1, we explored the industries most vulnerable to cyberattacks, highlighting the specific sectors frequently targeted by cybercriminals. In Part 2, we dive into the most common types of data breaches businesses face and offer actionable strategies to safeguard your organization. By understanding these threats, businesses can take the first step toward mitigating risks and protecting themselves from the costly and damaging consequences of cybersecurity incidents.

Human Error

Human error is at the core of many cybersecurity incidents. According to Infosec, 74% of breaches involve some sort of human element, making education and preventative measures critical.

Phishing Attacks

One of the most common manifestations of human error is phishing. Cybercriminals exploit trust and naivety through deceptive emails that mimic legitimate communications. These emails often trick employees into revealing sensitive information like login credentials or financial data. Businesses can reduce this risk by prioritizing comprehensive employee training to recognize and report phishing attempts.

Stolen Credentials

Closely linked to phishing is the issue of stolen credentials. Weak or reused passwords create openings for hackers to exploit. When an employee's credentials are compromised, unauthorized access to company systems becomes a reality. Implementing strong password policies and multi-factor authentication (MFA) can significantly reduce this threat.

Ransomware

Ransomware represents an escalation of credential theft and phishing. These attacks encrypt vital business data and demand payment for its release, often causing operational paralysis. They frequently begin with malicious links or attachments. To combat this, businesses should invest in regular data backups and advanced endpoint protection tools.

Insider Threats

While external threats dominate headlines, insider threats—whether intentional or accidental—remain a critical concern. Employees can inadvertently leak data or intentionally sabotage systems. Mitigating this risk requires strong access controls, continuous monitoring, and fostering a culture of accountability.

Misconfigured Systems

Beyond human actions, misconfigured systems represent a technical vulnerability often stemming from human oversight. Improper security settings or cloud storage configurations can expose sensitive data to unauthorized users. Regular audits and vulnerability assessments are essential to identify and fix these issues.

Social Engineering

Building further on human vulnerabilities, social engineering attacks involve manipulation tactics such as impersonation of IT staff or executives. These tactics are designed to extract confidential information or gain unauthorized access to secure systems. Consistent training helps employees detect and resist these threats.

Physical Security Breaches

Cybersecurity measures are incomplete without addressing physical security. The theft or loss of devices like laptops, smartphones, or external drives can lead to unauthorized data access. Encrypting devices and enabling remote wipe capabilities can minimize the impact of such incidents.

Data Loss from Third-Party Vendors

Even with strong internal controls, businesses often depend on third-party vendors, which can introduce additional risks. Ensuring that vendors adhere to stringent data protection standards and conducting thorough due diligence are key steps to minimizing these v

How Businesses Can Protect Themselves

To combat these threats, businesses should adopt a proactive approach to data security:

- **Employee Training:** Regular training sessions ensure employees can identify and respond to potential threats effectively.
- **Robust Policies:** Develop and enforce data protection policies tailored to your organization’s needs.
- **Incident Response Plans:** Have a comprehensive plan in place to respond to breaches swiftly and minimize damage.
- **Legal Guidance:** Work with legal experts to ensure compliance with data privacy regulations

and to create enforceable contracts with third-party vendors.

Data breaches can have devastating consequences, but with the right measures, your organization can stay ahead of these threats.

National Law Review, Volume XV, Number 31