ProvePrivacy

QUICK GUIDE

Understanding Potential Data Protection Risk

With data the lifeblood of the majority of organisations, protection of it is critical. Whether it be customer information, financial records, or proprietary intellectual property there is a risk of breaches, leaks, and mishandling.

What is a Data Protection Risk?

A **data risk** refers to any potential threat or vulnerability that can result in unauthorised access, exposure, modification, or destruction of data. These risks can arise from both external and internal factors and encompass a wide range of issues, including cyberattacks, human error, system failures, or weak data security policies. A **data protection risk** relates much more to how these data risks could go on to impact a data subject. When these materialises they can lead to data breaches, loss of trust, significant disruptions to business operations and potential regulatory penalties.

It is clear then that data protection professionals must consider all data risk to understand the impact on their role.

What are the potential Data Protection Risks?

1. Cybersecurity Threats

- Hacking and Malware: External actors attempting to infiltrate corporate networks to steal or corrupt data. Malware, such as viruses, worms, and ransomware, can disrupt business operations, while hacking can lead to data theft or breaches.
- Phishing Attacks: A form of social engineering where attackers deceive employees into revealing sensitive information like passwords or financial data. Phishing often targets businesses via fraudulent emails that appear legitimate.
- Denial-of-Service (DoS) Attacks: These attacks aim to overwhelm and disable a business's digital infrastructure, preventing access to data or services and potentially causing long-term damage if sensitive information is affected.
- If this is not your responsibility, build good relationships with the stakeholders responsible for Information Security, document these risks and make sure that you are comfortable that appropriate safeguards are in place.

2. Cloud and Remote Work Vulnerabilities

- Cloud Security Risks: Many B2B companies store vast amounts of data in the cloud, but cloud environments can introduce new vulnerabilities if not configured correctly. Misconfigurations, weak encryption, and improper access management can expose sensitive data to hackers.
- Remote Work and BYOD Risks: With the rise of remote work and Bring Your Own Device (BYOD) policies, businesses face increased data protection risks. Employees accessing corporate data from unsecured personal devices or networks can lead to unauthorised access and potential breaches.
- Similar to cybersecurity threats, understanding these risks rely on good relationships with the stakeholders responsible for Information Security. Again, document these risks and make sure that you are comfortable that appropriate safeguards are in place.

3. Internal Threats

- Employee Negligence: Human error is one of the most common causes of data breaches. Mistakenly sending sensitive files to the wrong recipient, misconfiguring systems, or losing devices with unencrypted data can expose a company to significant risks.
- Insider Threats: Disgruntled employees or contractors with access to sensitive data may intentionally leak or misuse it. B2B firms often work with multiple stakeholders and vendors, increasing the likelihood of internal actors compromising data.
- Weak Access Controls: Failing to implement proper access control mechanisms means that unauthorised individuals within the organisation can access sensitive data. Weak password policies and shared login credentials can exacerbate this risk.
- You can have a real impact in this area, provide ongoing education to all stakeholders, learn from incidents and communicate what you have learned so that others become more aware.

4. Data Loss and System Failures

- Hardware or Software Failures: Hardware crashes, software bugs, or unexpected system downtime can result in data loss or inaccessibility. Without proper backup strategies, companies can face severe disruptions and potentially irreversible loss of sensitive data.
- Data Corruption: Errors during data storage, transmission, or processing can lead to corrupted files, making them unreadable or inaccurate. This can result in operational delays, and, in worse cases, total data loss.
- We often find that these types of incidents are managed by technical teams, but they can still be a source of personal data breaches. If you believe they are, make sure they are recorded on your data breach log and managed accordingly, appropriate to the harm to data subjects.

5. Third-Party and Supply Chain Risks

- Vendor Vulnerabilities: B2B businesses rely on network of third-party vendors and partners to deliver services. If on of these partners suffers a data breach or has weak security protocols, your sensitive data can be exposed.
- Supply Chain Attacks: Attackers target a company's suppliers or vendors, looking for security gaps to exploit. Once the supplier is compromised, cybercriminals can move laterally to access your company's data.
- Make sure that you are involved in the procurement process, this is very important where personal data is being shared, make sure that data processors have adequate contracts and be clear on responsibilities with Joint Controllers.

6. Regulatory and Compliance Risks

- Non-compliance with Data Protection Laws: Businesses face data protection risks if they do not comply with regulations such as Data Protection Act (2018), GDPR or PECR. Failure to comply could result in fines, other sanctions, and damage to the company's reputation.
- Inadequate Data Handling Policies: If your business lacks clear data protection policies—covering data retention, encryption, or disposal—your organisation is at risk of mishandling data and facing regulatory action.

7. Data Breaches and Leaks

- Accidental Data Exposure: Data can be inadvertently exposed to the public or unauthorised users due to misconfigured servers, unintentional sharing, or improper disposal of data storage devices.
- Targeted Data Breaches: Cybercriminals may specifically target a business to gain access to its intellectual property, financial records, or customer information, often selling this data on the black market or using it for fraudulent activities.

These last two categories of risks are very much your concern, your colleagues will need your guidance so make sure that you document these. Understand how your organisation's activities process personal data and look for the risks within these processes. Keep logs of breaches and look for the risks whilst undertaking your response, not all reaches are serious but all can give you insights into where risks reside.

Whilst the list of risks is long it highlights the importance of taking proactive steps to manage, monitor and where possible mitigate risk.

Investing in robust cybersecurity measures, developing strict data governance policies, educating employees, and regularly auditing systems for vulnerabilities are essential strategies to safeguard sensitive information. Additionally, compliance with relevant data protection regulations and maintaining a comprehensive incident response plan can significantly reduce the impact of potential breaches.

The ProvePrivacy platform helps you capture risks at source. Our Record of Processing Activities (ROPA) highlights risks automatically and our Breach and Data Subject Rights modules allow risks to be identified and recorded so that they can then be managed and mitigated. To find out more visit, www.proveprivacy.co.uk.