GDPR Challenges in Small and Medium Size Businesses

Introduction

SMBs generally are facing many challenges in their operations even without the risks that are opening with GDPR. Cutting costs, improving on outdated IT systems and staying current with the global competition are the main topics of conversation.

Unfortunately, data protection isn't always taken into consideration until it's too late. Our guide will help pinpoint and explain the security and privacy issues companies like yours face and help you undertake proper measures to secure and protect private data to be compliant and avoid hefty fines.

Security issues & concerns

Miadria Group has been working with clients for over 7 years and we noticed the **10 most common issues and vulnerabilities** SMB's face in their IT systems and business processes:

1. A large proportion (often as high as 80%!) of employees completely excluded from digital business processes - these workers are often left with paper and phone or private email addresses as their only ways of communicating and exchanging information.
2. Using consumer communication, sharing and storage services which exposes corporate data and causes loss of control of the data.
3. User access management is still largely only password based, passwords policies are lax and passwords are frequently shared between users, preventing reliable user authentication and authorization.
4. Critical business data is residing unencrypted on on-premise systems or hosting environments, frequently in unsupported and/or unpatched software. Data in transit is also unencrypted.
5. Network security is primarily based on firewall and VPN. However once inside corporate network, attacker or malware is free to roam, compromise devices and steal data.
6. Endpoints (PCs and mobile devices) are unmanaged and unpatched.
7. Unawareness of outside data breaches and inside data theft.
8. Backuping and recovering data.
9. Finding information across systems for business, reporting and compliance.
10. Insufficient security procedures and/or audits.

More and more of these vulnerabilities get exploited and cause serious breaches and data leaks.

Main causes of data leaks

Malicious attacks by hackers

One of the main causes of data breaches. A 2015 report by Risk Based Security found that **hacking accounted for over half of all reported data breaches** during the year. These breaches may occur due to a targeted hacking attack; inadvertent installation of malware, which can steal user passwords and gain backdoor access to sensitive information; and ransomware, which is software that encrypts file until the victim agrees to pay a large sum of money to the attacker.

Negligent Employees or Insufficient Security Training

More than half of corporate data breaches can be traced back to an employee. In some cases this may be a malicious leak of data by a disgruntled employee, but in the majority of cases this breach is inadvertent and caused by poor security procedures. According to the same study mentioned above, many organizations provide only brief security training and do not sufficiently educate staff on the causes of data breaches. Insecure passwords, using the same passwords on several accounts and for long periods of time, working over an insecure network and even sending a document to the wrong person can all be ways in which an employee can accidentally cause a data breach.

Phishing and Social Engineering Attacks

Phishing scams, in which hackers set up fake websites and applications in order to steal passwords can allow access to sensitive information within minutes. The unknowing employee will usually click on a link from within an email that seems to come from an official source and be redirected to the fake website. Despite awareness of phishing emails increasing over recent years, most people still find it difficult to tell genuine and fake emails apart. According to the 2016 Verizon Data Breach Investigations Report, **13% of those tested clicked on the attachment of a phishing email.** Another type of scam involves calling or emailing the target, posing as an official or co-worker and asking questions to extract information, which could include confidential company data or passwords. It is also possible for hackers to guess passwords using the information they can find about employees via public records and social media – many people use the names of their children as part of their password, for example.

Loss or Theft of Physical Hardware

Laptops, tablets, and mobile phones are at a high risk for being stolen as they are small and easy to take and are commonly used outside the workplace in public areas such as cafes and

airports. There were 9,701 cases of corporate hardware theft or loss in 2015 and 56 of those led to confirmed data breaches. Losing an unlocked mobile phone that is logged into company accounts poses a much bigger potential loss than the cost of the hardware itself. With access to these accounts, an outsider can easily gain access to sensitive company information.

Insecure Mobile Devices

Many companies now give their employees mobile devices or have a BYOD (bring your own device) policy but this must be carefully managed if it is not to compromise the security of corporate data. As noted above, stolen mobile devices can be a huge security risk but even hardware that never leaves the sight of your employees poses a threat to company data security. If employees are allowed to bring their own devices to work, the company has less control over passwords, applications, and who has access to the device. Any insecurities on these mobile devices increases the risk of a data leak significantly.

Third Party Software and Services

Many companies now rely on the convenience and expertise of using an external company to manage some aspect of their data. This including accounting and team management software and cloud backup services. Any third party is equally at risk of being attacked by hackers or having data breached in another way, so it is vital that you choose companies to work with that have stringent security procedures and make keeping client data safe their top priority.

Repercussions of breaches and data leaks

We've seen it, maybe you've already experienced it and almost everyone heard in the media about the damage breaches and data leaks caused companies, regardless of the size. Large companies seem to recover more easily, but for SMB's it can be devastating, usually including some or all repercussions like:

- **Loss of customers**
- **Ransomware payments**
- **Productivity losses**
- **Business downtime**

GDPR comes into play

However, starting 25th May 2018, **data leaks containing private data of European Union residents will also result with fines up to 20 Million Euro or 4% of annual earnings, whichever is bigger.** Due to these, achieving GDPR compliance for SMB's on their own and without seeking help from experienced consultants is going to be next to impossible.

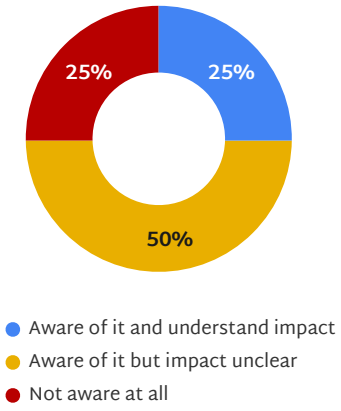
Research shows SMB's are not ready for GDPR:

- Only around 20% of SMB's are aware of the GDPR
- 50% know about it but are unclear on impact on their organization
- 25% are completely unaware

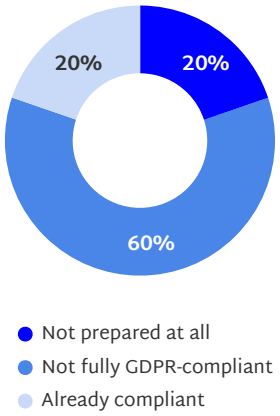
Of those 25% who are aware and understand the impact:

- 20% are not prepared at all
- 60% are not fully GDPR-compliant
- Only 20% are already compliant

GDPR UNDERSTANDING



GDPR COMPLIANCE



How can Miadria help SMB's with GDPR compliance?

Achieving compliance with old (on premise or hosted) software and systems will be next to impossible so Miadria's competences and experience working with leading cloud technologies, will help you achieve compliance by:

- Conducting risk assessment
- Implementing cloud services and solutions to locate and catalog the personal data in your systems, build a more secure environment, simplify your management and monitoring of personal data, and give you the tools and resources you need to meet the GDPR reporting and assessment requirements.
- Consulting on new business processes: identifying and secure the personal data in your systems, Accommodating new transparency requirements, Detecting and reporting personal data breaches
- Training privacy personnel and employees

Contact us to talk about your compliance!