SMBs AND THE NEW InfoGov ENVIRONMENT

Author: Pat DAWSON - Editor: Catherine TALL
EVERTEAM, EFCSE member
18/10/2019
The once under-appreciated discipline of information governance has in recent years gotten a good deal of press, particularly since the enactment of GDPR and the public disclosure of high-profile data breaches by large corporations and social media behemoths.

The specter of GDPR compliance and the need to mitigate the risk of data breaches are just two prominent use cases that underscore the broader, emerging need for organizations of all sizes to do a better job of safeguarding their information assets.

Most people understand the importance of information governance for large corporations, public sector agencies, and social media giants. However, small-to-medium-sized businesses (SMBs) underestimate the relevance of good information governance to their day-to-day operations.

Typically, SMBs view information governance or data protection as something that only big organizations need to worry about. However, a recent study by Verizon highlights the fact that a whopping 43% of all data breaches involve SMBs*. The number of undetected incidents remains unknown. As frequent targets of data breaches, SMBs inadvertently disclose sensitive information, endangering their customers and their business.

In today’s fast-moving technology and information environment, SMBs should prioritize information governance.

Consider the following:

- **Data Breaches Cause Considerable Damage for SMBs**: While fines and litigation can be costly and hurt the bottom line for large companies, they are potentially devastating for SMBs. Studies by consulting firm Switchfast Technologies concluded that at least 60% of SMBs are forced to discontinue operations within 6 months of a data breach.¹ Large organizations typically have the financial resources to survive and recover following a major incident like a data breach. With fewer organizational, technical, and marketing / PR investments needed to overcome such a loss of trust, SMB revenue diminishes as customers take flight.

According to Cisco, the typical cyberattack results in financial damages of more than $500,000 USD.² For SMBs, this high failure cost compels proper information governance. It is no longer a luxury, but a necessary investment in business continuity.

Small Organizations Often Lack IT Resources: Easily procured cloud and mobile application services have lowered the perceived need for IT support within many SMB organizations. Imbued with a “do it yourself” culture, SMBs often have little or no trained IT staff to help protect their information infrastructure. Security services provider Underscore surveyed 300 SMBs and found that 29% of them spend less than $1,000 USD per year on IT security. The same study found that 52% of those same SMBs distributed IT responsibilities across employees with other roles in the organization. Lack of trained IT personnel and under-developed information governance programs leaves SMBs vulnerable to lapses in information governance due diligence, putting their customer’s data and their business continuity at risk.

3 https://www5.untangle.com/smbitsecurityreport2019
4 https://www5.untangle.com/smbitsecurityreport2019
Small Organizations Often Commingle Personal and Professional Lives:
Small business owners and their staff often use the same laptops, mobile devices, and storage infrastructure not only to manage their businesses but their personal lives as well. Usually unhindered by policies prohibiting the use of business devices or applications for personal use, small organizations present a potentially more impactful target to cybercriminals thanks to their wealth of both personal and corporate information. This means that breaches endanger both the business and the individuals running it for many SMBs.

Responsible information lifecycle management can mitigate these compelling risks.

Below are some basic tools and processes aimed at empowering SMBs to develop a greater literacy and capacity for information governance.

> **Perform an Information Inventory**: To identify gaps in your organization’s current information lifecycle management/information governance strategy, perform a thorough review of your information. The review should encompass all information with which the organization interacts. Particularly sensitive information includes:

<table>
<thead>
<tr>
<th>Personally Identifiable Information (PII) present in transaction systems such as scheduling, invoicing, or other systems used for day-to-day operations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information governed by industry-specific regulations -- medical information (PHI) or financial data (PCI), for instance.</td>
</tr>
<tr>
<td>Proprietary information. Trade secrets, designs, formulas, or other intellectual property. Stolen trade secrets can be used to blackmail the company or undermine an organization’s competitive position.</td>
</tr>
<tr>
<td>Customer and Prospect information. Of particular interest the degree to which contacts in your organization’s marketing database have consented via double opt-in to receive email communications from your firm.</td>
</tr>
</tbody>
</table>
> **Perform an Application Review:** SMBs understandably choose the software used to run their business on pragmatic factors like price, functionality, and ease of use. What’s often neglected in the selection process is the trustworthiness of the software publisher and the resilience of their software to the threat posed by cybercriminals. Some criteria for performing this review include:

- **Use of Encryption:** Does the software used include the use of encryption for things like email encoding, file storage, or secure website access? If not, the software is probably not a good choice for hosting sensitive or proprietary information, and alternatives should be sought.

- **Compliance with any key regulations and standards:** For instance, if the application manages payments via credit cards, does it comply with the PCI DSS standard? If the application deals with personal information, do they have a statement of compliance with regulations like GDPR?

- **Are There Robust Security Protections?** Does the software, app, or website have good controls for password and permission systems, including the ability to define role and group-based access permissions, regular refresh of passwords based on defined criteria, password complexity requirements, use of Captcha, and other measures aimed at preventing unauthorized access to information?

- **Software Publisher Policies for Data Breach Events:** Transparency is important. Do software publishers with whom your organization works have proactive breach prevention and breach reporting policies in place? If data protection policies are inadequate or lacking, consider an alternate application provider.
Review Your Digital Marketing Practices and Assets: One of the biggest sources of personally identifiable information comes in the form of marketing data, used historically to generate demand via email, telephone, or direct mail outreach. When examining your organization’s marketing information, pay special attention to:

**Website Forms:** Ensure lead capture forms are GDPR compliant. More specifically, do they incorporate a “double opt-in” which explicitly indicates a willingness to accept future marketing correspondence from your organization?

**Contact Lists:** Confirm subscription with double opt-in, for existing contacts and future prospects. Secure double opt-in via an email campaign for non-compliant marketing assets with interest to do so. Purge any information from non-interested contacts from all digital marketing systems. This process often entails significant loss of email list assets. However, this is the only way to GDPR compliance and protect your organization from privacy infractions that can carry significant fines, litigation, or worse.

**Sales and Marketing Service Suppliers:** Many SMBs rely on partners to help generate new business through digital marketing or inside sales (i.e. “cold calling”) services. As you seek to grow your organization’s data protection and compliance maturity, work to ensure that each of these partners operates in a manner consistent with GDPR and local regulations.
Develop and Execute on an ILM (Information Lifecycle Management) Strategy: The results of a Data Inventory and an Application Review addresses identified deficiencies and corrects known problems only at a specific moment in time. This effort remains temporary until an ILM strategy employs and implements the following tools and processes in a sustained manner:

- **Appoint a Data Protection Officer:** A Data Protection Officer (DPO) is an individual within the organization who has accountability for the human, system, and process aspects of information governance within the organization. The DPO responsibility is typically not a full-time job—it is a role assumed by a leader within the organization who understands the importance of data protection to the organization’s wellbeing, and who can act in a role of empowered oversight on these matters.

- **Allocate Appropriate Budget:** Business challenges important to the continuity of operations require a budget. Information governance allowances need not be exorbitant— but they should be realistic. Budgets can be used to procure software to facilitate data privacy protection and regulatory compliance. Budgets can also be allocated in time—time needed by internal resources to perform regular data and application audits.

- **Consider Tools to Make the Work Easier:** Implement tools and processes to address issues and support information management moving forward, including:
  - Routine discovery of sensitive data
  - Define and implement retention policies
  - Remote Redundant Obsolete, or Trivial (RoT)
  - Define and implement processes for managing subject access requests (SARs)
  - Implement processes for reporting a data breach if it occurs
> **Routine discovery of sensitive data** in places where it shouldn't be stored, such as file servers, groupware systems, unencrypted email local storage on laptops or mobile devices, etc. Federated search products are available for SMBs that connect to enterprise applications like email, groupware, file services, and ERP / CRM applications. These products can provide a complete inventory of sensitive data and its location.

> **Define and implement retention policies** across the information lifecycle. Ensure that information is appropriately managed from creation to disposition. Smaller organizations may choose to track this process using something as simple as a spreadsheet, but commercially-available products can automate this process, significantly reducing error and time.

> **Remove Redundant, Obsolete, or Trivial (RoT) data.** ROT information can provide outdated information to members of your team and increases your organization's exposure to a data breach or similar event. Regularly prune your information systems and remove out-of-date or irrelevant information, either manually or as part of a retention policy managed by a commercially available software product.

> **Define and implement processes for managing subject access requests (SARs).** While SARs are more often submitted to large organizations, every data subject has the right to ask how their personal information is being used. SMBs need to have procedures in place to acknowledge, respond to, and fulfill SARs as needed in ways that are compliant with GDPR-defined service level thresholds.

> **Implement processes for reporting a data breach if it occurs.** Just as your organization vets suppliers for their transparency in handling data breach issues, so too your customers expect a high level of transparency from your organization. Make data privacy protection a key component of your brand. Promote the mechanisms you use to ensure data privacy, communicate policies, and proactively engage with customers if an issue occurs. Inc. magazine noted that 73% of consumers indicate that transparency is more important than price\(^5\) in selecting the organizations they do business with.

---

5 [https://www.inc.com/rhett-power/trust-is-as-important-as-price-for-todays-consumer.html](https://www.inc.com/rhett-power/trust-is-as-important-as-price-for-todays-consumer.html)
Data privacy and protection can be complex hurdles for SMBs unfamiliar with information governance. As this short overview demonstrates, SMBs willing to take on these challenges can avoid fines, preserve customer trust, and help to ensure their business’s viability. Diligent information governance need not require massive capital investments or dramatic, disruptive change; it can be implemented as a series of incremental steps aimed at identifying, categorizing, and proactively managing your information assets.

And once implemented, good information governance can only be sustained through concerted effort as part of new hire training, recurring refresher courses, and internal marketing to promote the visibility of good information lifecycle management practices.

By effecting the changes outlined in this paper, your organization can make improvements that will not only protect your operations, but that will increase customer loyalty and the value of your brand.

With these and other benefits in mind, we encourage you to begin the journey.
On transition and digital transformation context, Information Governance is a major topic, EFCSE has dedicated one of its Working Groups to this theme.

Contact us on efcse.eu