# What You Don’t Have Can’t Hurt You – Reducing Cyber Risk Through Proper Data Management

As organizations continue to create more data and the threat of cyber risk continues to grow and evolve, businesses are trying to keep up with advancing technologies, find new ways to prepare for cyber-attacks, and mitigate the associated risks. While some of these actions typically occur in response to an attack (e.g. fixing exploited flaws and vulnerabilities, and upgrading technology to better monitor future threats), proper data management is critical to reducing the risks to an organization before an attack ever takes place. Key to this proactive approach is ensuring your organization has a framework in place for the defensible disposition of records, information and data; i.e. “what you don’t have can’t hurt you” in the context of a cyber-attack.

**Cyber Incidents**

Cyber threats can come in many different forms (malware, phishing, zero-day exploit, denial of service attacks, etc.), and be perpetrated by various threat actors from bored teenagers to nation-state sponsored groups, as well as by internal actors, whether unintentionally or intentionally with malice. These incidents can lead not only to disruptions in services, but also to the disclosure of records including those containing sensitive, confidential and personal information. The cause of a cyber incident can be complex, or as simple as a single employee downloading malware by clicking a malicious link in a phishing email or inserting an infected USB key into a computer within an organization’s network. It is important to be prepared for a variety of scenarios.

There have been a growing number of high profile cyber incidents in recent years, having a profound impact on individuals and business around the globe. Examples include the following representative cases:

- Attackers took advantage of a known vulnerability in software used by an organization and infiltrated enterprise systems and data, operating undetected for an extended period of time. This resulted in the information of nearly 150 million individuals being exposed. Although the organization had a retention policy in place, there was no process for deleting information in compliance with this policy, and information was retained beyond the established retention periods.

- An organization was targeted and hacked by threat actors seeking to damage the business, leading to the exposure of the information of some 30 million individuals whose customer profile data was being retained by the organization indefinitely.
- A malicious employee exfiltrated the information of nearly 10 million individuals over a period of roughly 2 years. Confidential information had been copied from a secure location by individuals with authorized access onto a shared drive from which an employee with malicious intent was able to obtain access. At the time of the breach, the organization had been retaining millions of files that had been inactive for decades.

There is a common theme across these cases. When looking at the breach investigation reports of the regulatory authorities for these and other incidents, a key issue frequently highlighted is that information had been retained longer than necessary. This sometimes happened in contravention of an organization's existing retention and disposition policies, while in other instances information had, in practice, been kept indefinitely. These organizations would have significantly reduced the risk and impact of these cyber incidents if they had avoided retaining large amounts of information longer than necessary.

**Balancing and Assessing Risk**

As part of an organization's general risk assessment, it is increasingly important to consider the appropriate measures to take for cybersecurity purposes. This requires conducting a risk analysis and balancing the identified risks in order to come up with an approach that fits an organization's needs depending on the quantity and types of data held and the available resources.

Cost Risk Analysis

While implementing and keeping cybersecurity systems and policies up-to-date may seem like a daunting and expensive endeavour, cyber incidents themselves come at a significant cost. Not only can they result in significant reputational damage and loss of public or consumer trust, but they can also bring hefty regulatory fines and orders to spend large sums upgrading cybersecurity systems. Additionally, organizations may be required to provide certain services to individuals impacted by the breach such as credit monitoring and identity theft protection, or to engage the services of expert consultants and/or auditing firms to ensure compliance with obligations moving forward. Organizations can also find themselves facing class action lawsuits, resulting in additional legal fees and potential monetary awards or settlements.

The proactive and systematic disposition of information can reduce the number of individuals affected by a breach, decreasing the overall costs of a cybersecurity incident. Retaining unnecessary information in the first place can also result in significant cost to organizations. Storage can be expensive, and the more data organizations hold the greater these costs will be. Organizations are responsible for all information they collect and hold, including information found in legacy systems and backups. The risk associated with maintaining information longer than necessary suggests it is best practice for organizations to ensure disposition is properly addressed in retention policies and protocols, and information is not over-retained.

If there is a requirement to retain certain information for regulatory purposes, but there is no need to maintain it "live", consider moving the information to "cold storage" with increased access and other controls for the required period of time before disposition. This will allow organizations to meet their

retention obligations while reducing the risk of a breach. When there is a desire to retain certain information for a longer period of time for business purposes, the organization will need to consider whether there truly is a need to retain it from a business perspective, whether the need is reasonable, and whether the expressed need can only be met through the retention of the specific information in question. If so, organizations need to consider whether they have the available resources to cover the cost of implementing additional security measures and whether the risk associated with extended retention is acceptable in the event of a cyber incident.

Legal Risk Exposure Analysis

Another important issue is the legal risk exposure associated with the potential for premature deletion of information subject to legal retention requirements or potentially relevant to dispute resolution, balanced against the risk of over-retaining certain information in the event of a cyber incident. To help understand and mitigate these risks, organizations need to invest in developing a proper data management framework.

*Development and Implementation of Retention Policies*

It is critical for organizations to develop and implement retention policies and procedures as part of their overall data management framework. This requires an understanding of all the different types of information an organization creates, collects and retains, its purpose, and where it is kept. It is important for organizations to classify this information and tag it appropriately. Tagging records and information with the correct metadata will help in associating them with the proper retention rules, as well as establishing access controls, preventing unauthorized use, and protecting integrity.

When considering the most appropriate period of time to keep certain records and information, there is often a perceived tension between privacy and retention, especially for records that attract regulatory retention requirements but also may include personal information (e.g. receipts, sales invoices, etc.). Organizations will need to consider whether there are any legal requirements obligating them to keep the record for a certain period of time, and if not, the most appropriate timeframe based on the purpose of the record, and the business need to retain it. Guidance is available from regulatory authorities to assist in making these determinations (e.g. Personal Information Retention and Disposal: Principles and Best Practices (Canada OPC), Principle (e): Storage limitation (UK ICO), etc.). A common practice in establishing a period of retention when there is no explicit legal requirement, is to rely on limitation periods. While this is generally acceptable, organizations need to carefully consider this approach when personal information is implicated (see Applying Limitation Periods in Information Governance Programs).

Further, it is not enough to simply have retention policies developed, they must be implemented to be effective. As demonstrated in the first case example above, having a retention policy in place that is not followed will not establish credible due diligence in the event of a cyber incident; the damage will have been done. Putting retention policies into practice requires adequate employee awareness and training. This includes clear instruction on who is responsible for implementation of the retention and disposition policies for any particular records and data.

*Managing Third Party Relationships*

Another potential risk factor for organizations to consider is whether they have any third party relationships that may result in the transfer of information. This includes circumstances where one organization has contracted another for the provision of services, or where the organization has itself

been engaged to provide services. In either case, it is important to ensure there is a formal written agreement which specifically includes reference to retention obligations relating to the information transferred. These obligations may differ from an organization's own retention rules for the same types of information. To help address this issue, organizations should consider segregating their information to assist in proper disposition and reduce the potential impact in the event of a cyber incident.

**Conclusion**

Demonstrating that sufficient effort has been made to mitigate risk prior to a data breach can help reduce potential fines, penalties and reputational damage when faced with a cyber incident and potential investigation. Establishing a proper data management framework is one way to help achieve this objective. If an organization proactively takes steps to avoid retaining information longer than necessary, the risk and impact of exposure is significantly reduced. The proper training of employees on the organization's relevant polices is an important line of defence in protecting against the occurrence of cyber incidents, and in reducing risk in the event of an incident occurring. Finally, organizations should have a structured program in place to monitor compliance with cybersecurity and data management policies and procedures.