

# SECURING THE FUTURE

## In this Issue

- Awareness is the first step in information security
- Regular staff training is crucial for protecting confidential data
- Businesses should not underestimate the impact of a breach
- Consider data stored on all pieces of technology
- Would legislation impact adherence?
- Survey findings and suggestions for improving data security
- Your free security consultation



## Big Business vs. Small Business – Who is More on Top of Information Security?

*In this issue, we will discuss how effectively Canadian businesses are protecting confidential information and what businesses of all sizes can do to improve their security practices and protocols.*

When it comes to information security, businesses may not be doing as well as they think in protecting their and their clients' confidential information.

Earlier this year, Shred-it commissioned a survey called the *Information Security Tracker* to find out if Canadian businesses are doing enough to protect their own confidential information as well as the their client's information. The survey asked large and small businesses to share their attitudes, protocols and practices towards information security. The results of the survey demonstrated that there are businesses of all sizes that are not making information security a priority. The question is: *who is doing more to protect client and business data – large or small businesses?* Or, is business size not a factor in proper information security procedures?

In order to gain an understanding of who is more on top of document security, we will look at how big and small businesses responded to relevant questions from the 2012 Information Security Tracker.



# SECURING THE FUTURE

## Awareness is the first step in information security

When asked *if they were aware of the legal requirements of storing, keeping or disposing of confidential data in their industry*, 95 per cent of large businesses admitted to being at least somewhat aware of the requirements, while only 76 per cent of small businesses could say the same. This brings a question to mind – if a business is not at least somewhat aware of what is legally required of them, how can they ensure they are taking the proper precautions?

While it's essential that businesses know what is compulsory from a legal perspective, an information security policy is not effective unless it is shared with all staff. The survey asked respondents if *their company had a known and understood protocol for storing and disposing of confidential data*. Again, large businesses demonstrated that they understand the significance of awareness as it relates to information security – 92 per cent said they had a protocol, while only 55 per cent of small businesses said they had a protocol in place.

## Regular staff training is crucial for protecting confidential data

For employees working at any given company, having knowledge of their organization's data security policies is vital. At the same time, it's possible that an employee may be trained on these procedures when hired but then never given subsequent training. The *Information Security Tracker* sought to find out more about how often companies are training employees on relevant security procedures. Only 21 per cent of large businesses and six per cent of small businesses train their staff twice a year, while a fair number train on an annual basis (40 per cent of large businesses compared to 10 per cent of small businesses). Many companies opt to only train on an ad hoc or as-needed basis (24 per cent of large businesses compared to 47 per cent of small businesses); however, a number of organizations provide training only once during their staff's employment (15 per cent of large businesses compared to 6 per cent of small businesses). One step that can help an organization ensure that these policies are communicated to staff is to appoint an employee to be directly responsible for managing data security issues. Most large businesses surveyed (93 per cent) have an individual filling this role, while just over half of small businesses (52 per cent) have designated an employee to fill this position.



# SECURING THE FUTURE

## Businesses should not underestimate the impact of a breach

Data breaches have the potential to cause serious implications for businesses of any size, including a loss of money, reputation, clients and more. In an effort to learn more about how seriously businesses consider breaches, the survey asked: *in the event that data from your company was lost or stolen, how would this impact your business?* Large businesses seemed to understand the complications that could arise as a result of a breach, as only 15 per cent of large businesses indicated a data breach would not seriously affect their business. Small businesses were less likely to recognize the severity of a breach with 61 per cent answering the same.

## Consider data stored on all pieces of technology

As technology continues to advance, organizations need to be aware that there are increasingly more items containing sensitive data. In the survey, businesses were asked *how they dispose of aging or obsolete computers (or other data-storing electronics such as smartphones or photocopiers) that are no longer used.* A relatively equal number of large and small businesses answered that they simply recycle these items (18 per cent of large businesses compared to 19 per cent of small businesses) along with erasing, wiping or degaussing contents then recycling (54 per cent of large businesses compared to 55 per cent of small businesses). With both of these methods, sensitive information could potentially be retrieved – the best way to ensure data is not recovered is to have the hardware fully destroyed—something that only 22 per cent of large businesses and 15 per cent of small businesses are doing.

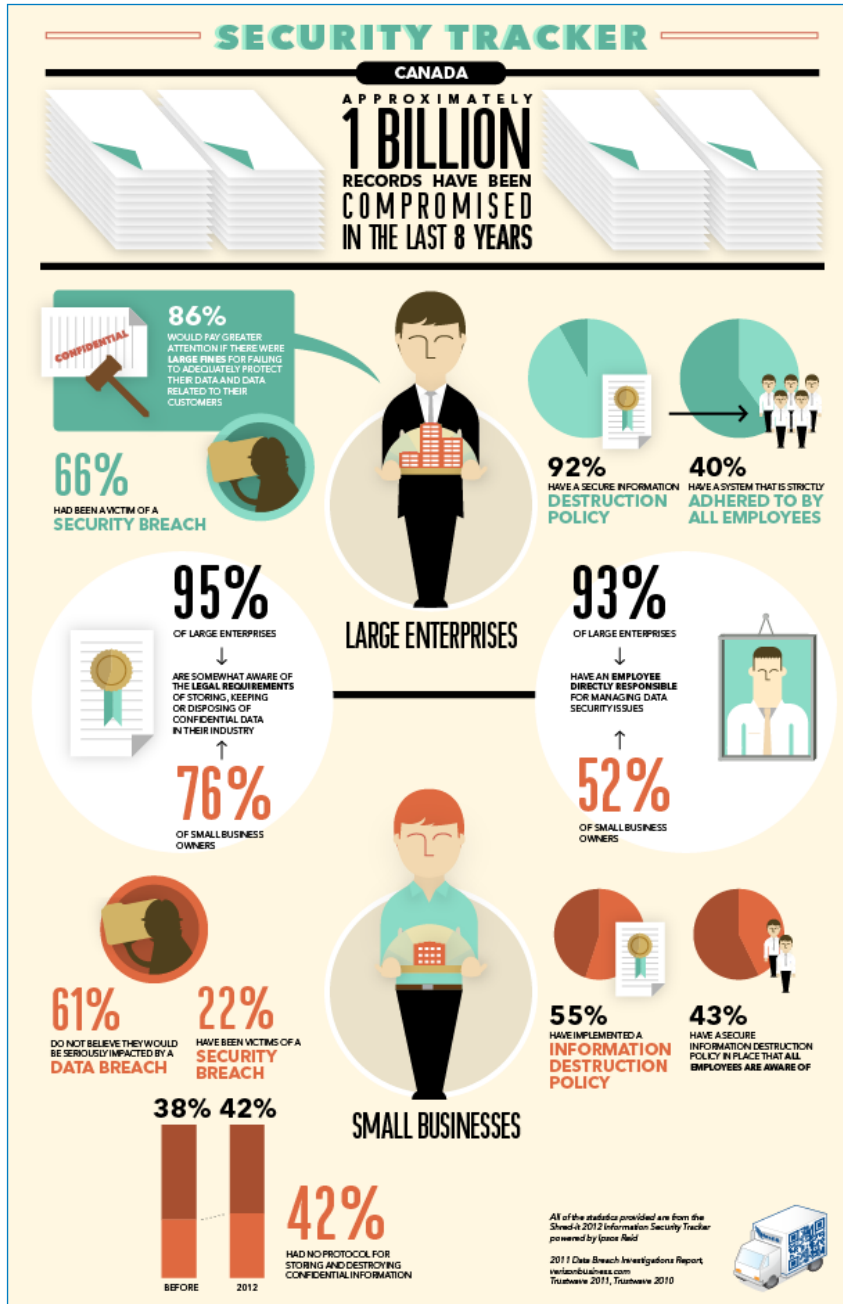
## Would legislation impact adherence?

Data breaches may seem like they are not a source of concern for businesses that have not been affected by one. However, the survey asked businesses *if they would pay greater attention to safeguarding data if the Privacy Commissioner were to introduce large fines for organizations that failed to adequately protect their own or their customer's data.* In response, large businesses were more likely to answer yes (86 per cent), though under half of small businesses had the same response (48 per cent).



# SECURING THE FUTURE

## Survey findings and suggestions for improving data security:



The *Information Security Tracker* revealed that large businesses overall seem to be more on top of their procedures; however, it also showed that there are organizations of all sizes that have gaps in their policies and there are areas for improvement. It is crucial to be vigilant when seeking ways to safeguard data. In order to strengthen their data security measures, businesses should consider the following tips:

- Consider holding regular training sessions for all employees on proper information security procedures
- Appoint an individual or committee responsible for managing data security procedures
- Conduct an annual information security audit and risk assessment to identify potential sources of data loss
- Establish a shred-all policy that is communicated to all employees
- Ensure that all pieces of obsolete technology are fully destroyed or crushed so that information cannot be recovered

Information Security Tracker Graphic Summary



# SECURING THE FUTURE

## Your FREE Security Consultation

Shred-it has developed an online survey to help businesses better understand security gaps. Conduct your own [security self-assessment](#).

Learn more about [Shred-it services](#) or book your [FREE security assessment](#).

Read more about the [2012 Shred-it Information Security Tracker](#).

You can also visit Shred-it on [Facebook](#) and [LinkedIn](#) or follow us on Twitter at @Shredit.



## About Shred-it

Shred-it is a world-leading information security company providing document destruction services that ensure the security and integrity of our customers' private information. The company operates 140 branches in 16 countries worldwide, servicing over 150,000 global, national and local businesses, including the world's top intelligence and security agencies, more than 500 police forces, 1,500 hospitals, 8,500 bank branches and 1,200 universities and colleges.

