Risky business: the hidden costs & impact of data breaches
Small businesses, big targets

58% of data breach victims are small businesses\(^1\). Why? First, they typically don’t have the IT defenses to prevent or detect a breach, and second, they have less employee oversight and fewer processes to help prevent data leaks.

Although data breaches can happen rapidly, it’s reported that 68 percent of these security incidents in 2017 took “months or longer” to identify\(^2\). This delay in discovery provides hackers with more time to not only steal personal and confidential data, but to put measures in place for long-term data exposure and compromise. Ultimately, costs can accumulate to the point where many small businesses aren’t able to recover.

What is a data breach and how does it happen?

A data breach is an incident where information is stolen or lost, often without the knowledge or authorization of the owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, employee data, trade secrets, or even matters of national security.
Most data breaches are attributed to hacking or malware attacks.

Hacking is when a criminal gains unauthorized access to data in a system or computer. Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

There are also other ways in which data may become breached. Other frequently observed breach methods include the following:

- **Insider leak**: A trusted individual or person of authority with access privileges steals data.
- **Payment card fraud**: Payment card data is stolen using physical skimming devices.
- **Loss or theft**: Portable drives, laptops, office computers, files, and other physical properties are lost or stolen.
- **Unintended disclosure**: Through mistakes or negligence, sensitive data is exposed.

Fraudsters are primarily after your business Information, as well as your employee or client data.

**For business information**: Your name, officer names, officer home addresses, emails, phone numbers, social security numbers, EIN, bank account numbers, logins and passwords, credit card numbers, mortgage or lease documents, computer passwords, and more.

**For employee and client data**: Name, home address, email address, phone number, social security number, credit card information, bank account information.

**Risky Business**: The Hidden Costs & Impact of Business Data Breaches

Source: Trend Micro, Data Breach
The most common conclusion is that data breaches can lead to the loss of bank account funds, but the impact could be much larger than that. The number of individuals affected, the type(s) of information compromised, and how the event was handled by the breached organization will all contribute to the total incident cost.

For example, the average cost of a data breach to a small business was between 38,000-$120,000 (Kaspersky Lab 2016-18).

**Costs come in many forms. For example:**

**Direct costs:** These costs are incurred to investigate and mitigate damages that could be attributed to the breach, including public relations expenses, and costs incurred to notify affected parties of the breach and provide them with credit monitoring services.

**Cross-claims:** These are lawsuits that may be filed against the breached company by employees or customers, for exposing their data.

**Legal costs:** Legal defense costs could be substantial—attorneys who specialize in this work charge as much as $1,000 an hour.

**Compliance costs:** Breached businesses may be subject to penalties for violations of federal statutes and regulations. About 50 federal statutes and regulations govern privacy and security.

**Reputational costs:** A privacy breach, actual or perceived, may result in a loss of consumer trust significant damage to the public perception of the small business.

91% of hacking attacks start as phishing emails.
How you can protect your business

Here are some recommendations to help protect your business from data breaches:

**Secure common cyber attack touch points.** Make sure you use anti-malware software on your computers so they detect an attack. Engage an IT professional.

**Get up to speed on phishing scams.** Educate yourself and any employees or contractors to recognize common phishing scams so that you and they don’t give out sensitive business data, such as bank account and routing numbers.

**Prepare for a breach before it happens.** If a data breach does occur, make sure you have a response and notification plan in place. Being able to quickly take action could significantly reduce the cost of recovery.

**Develop a document handling policy.** Develop rules about leaving computers unattended and for discarding documents with sensitive information (bank statements, employee W2s, etc.).

**More tips to help avoid a breach.** Change passwords often. Check bank statements and other financial accounts regularly. Never respond to suspect emails. Arm your business with identity protection tools, like QuickBooks Detect & Defend, powered by EZShield.
Risky Business:  
The Hidden Costs & Impact of Business Data Breaches

$38,000-120,000
Estimated cost of a small business data breach

Source: Kaspersky Lab, 2016-2018

How QuickBooks Detect & Defend can help with data breaches

Given the frequency of data breaches and the potential downside of having one, it pays to be prepared.

With QuickBooks Detect & Defend powered by EZShield, if a breach happens, you can call a U.S.-based Resolution Specialist any time. This Specialist is highly trained to know what to do, and will help guide you through the situation.

Learn more about QuickBooks Detect & Defend or ask one of our representatives how you can be better prepared to fight fraud by calling (800) 749-6400.
When it comes to small business identity theft, we’ve got your back

QuickBooks Detect & Defend

- Detect
- Alert
- Resolve

*Free trial offer is valid for new Detect & Defend customers only. First thirty (30) days of subscription to QuickBooks Detect & Defend, starting from the date of enrollment, is free. Customers will be asked to present a valid credit card account for authorization when they subscribe. After the first 30 days, your account will automatically be charged monthly, at the current rate for the service, until you cancel. You may cancel the service at anytime by calling (800) 749-6400 or accessing your Intuit account and clicking on “cancel now”. First charge on your account will align with your current bill date for other active Intuit offerings. Limit of one subscription per customer. Offer expires August 31, 2019. Terms, conditions, pricing, service and support options are subject to change without notice. Detect & Defend not available to customers located in NY.

1, 2 Verizon data breach investigative report 2018
3 Businessidentitytheft.org
5 Kaspersky Lab 2015