Shoplifting Goes Futuristic

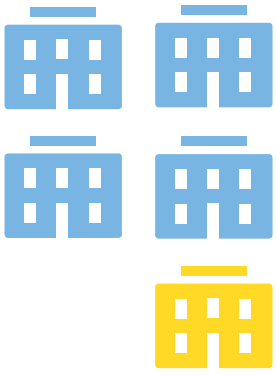
Data Breaches and Online Hackers Are Taking Business Owners to the Cleaners

MYDIGITALSHIELD

Table of Contents

(Click to jump to section.)

Welcome to the Age of Cyber-Attacks & Digital Security Issues That Threaten Your Business



1 in 5

small businesses falls victim to cybercrime each year, and of those, some 60% go out of business within 6 months

Imagine this: you're a retail store manager and you see a group of highly suspicious 'customers' enter your store and immediately head towards the back, away from the registers and other employees. While they may avoid direct eye contact, they continually look up and check to see if anyone is watching or heading in their direction.

If you're like most retail managers, you recognize the telltale signs of a potential shoplifter and are always keeping an eye on store visitors like this. Similarly, like all retail managers, you've also anticipated this threat from the beginning, **and have implemented a variety of loss-prevention policies to protect yourself and your store** from both external and internal threats.

Your store might use security tags, alarms at the doors, greeters posted at the exits, and loss-prevention teams.

In short, you're confident in your ability to protect your store and merchandise because you have prepared for this type of scenario and have well-tested strategies in place to deal with these types of unwelcome store visitors.

However, times have changed, and now the retail store owner and store managers need to keep a lookout for digital thieves coming into their stores to steal. As more and more business services move online and people increasingly choose to pay for purchases with credit cards, the risk of "digital shoplifters" (or "hackers") pose a massive risk to your company's livelihood.

Most small business owners are unaware of these threats, as 77% say their company is safe from cyber-attacks

And while it's a relatively instinctual ability that allows the diligent store keeper to identify suspicious behavior amongst visitors in a physical setting at a store, the threats posed by digital thieves are much more difficult to identify and yet, increasingly more frequent.

Small businesses are getting hit left and right with identity thieves gunning for customer credit card numbers, hackers attempting to sabotage networks and gain access to sensitive data, and employees looking to make a quick buck.

According to the National Cyber Security Alliance, 1 in 5 small businesses falls victim to cybercrime each year, and of those, some 60% go out of business within 6 months as a result of the accompanying financial damages.

Antithetically, most small business owners are unaware of these threats, as 77% say their company is safe from cyber-attacks, yet 83% have no formal cybersecurity plan to speak of.

Nowadays, it's not just merchandise that's being swiped off the shelves, it's also your company's reputation, customers' credit card information, and other forms of sensitive data that are up for grabs.

Choosing to protect your store from physical threats while leaving your business vulnerable to cyber-crime is paramount to leaving your store's door unlocked and your cash register open.

> **Visa Inc. reports small businesses represent more than 90% of the payment data breaches reported to the company.**

Whether it's widely acknowledged or not, loss prevention in the digital age extends to cyber security now. You wouldn't leave your storefront open to any unnecessary risk of theft, so why leave yourself unprotected against shoplifters' digital counterparts?

The Invisible Thief: 4 Ways Business Owners are Losing Out to Digital Shoplifters

Protecting your business and customers from cyber-crime and online threats is no longer a secondary priority for small business owners. In the past, only large companies needed to concern themselves with the illicit activity of hackers and online criminals.

But today, increases in enterprise-grade network security and implementation of tough-to-crack cyber defenses have redirected these threats and hackers' efforts to smaller stores that often present as an easy target due to lax digital security policies.

Obscurity is no longer a viable strategy for online protection and IT security, and with the prevalence of these cyber-attacks, coupled with the devastating financial consequences that accompany them, every business owner needs to take a serious look at how their business may be vulnerable to cyber-attack in the digital age.

4 Ways Business Owners are Losing Out to Digital Shoplifters

Inadequate Firewall Protection

Incomplete Cyber-Security Strategy

Unsecured Wireless Connection

Data Leakage Prevention (DLP)

1. Inadequate Firewall Protection

Cyber threats are evolving all the time and without state-of-the-art firewall protection, your network will be unable to identify and kick out possible threats to your system, allowing hackers access to your sensitive financial information and private company information.

2. Unsecured Wireless Connection

Without a secure wireless connection, you open your business up to a variety of vulnerabilities that even novice hackers can take advantage of, which can result in increased bandwidth usage and cost, slower internet connection, virus infections, and unauthorized access to company tax and financial records.

3. Incomplete Cyber-Security Strategy

A chain is only as strong as its weakest link. Likewise, a network protection system is only as effective as its greatest vulnerability. Protect your company's and your clients' sensitive information from even the most advanced of cyber-threats with Advanced Threat Protection similar to what large enterprises use to protect theirs.

4. Data Leakage Prevention (DLP)

Would you let a shoplifter walk right out of your store without some sort of attempted prevention? Then why would you let someone take sensitive, valuable information from your network uncontested? DLP prevents your data from being taken and alerts you when an unauthorized data transfer is attempted.

Of course, not every small business is equally likely to fall prey to cybercrime. Hackers usually don't discriminate by company type, valuation, or any other characteristic of the business itself, rather, they look for those businesses that are vulnerable due to lax digital security.

And unlike conventional thieves or shoplifters, hackers are experts at exploiting system vulnerabilities while remaining hidden, making them all the more difficult to stop.

The Cost of Having Inadequate Firewall Protection

In the perpetual arms race between hackers and internet security systems, traditional cyber security strategies have become obsolete. As newer and more sophisticated types of attacks and viruses are developed, internet security systems have had to evolve in order to face these new threats.

One such common system that has undergone a transformation in order to rise to the challenge is the traditional firewall.

To put it simply, a firewall works as a barrier, or wall, between cyber space and your company's private network. It is your business's first line of defense against cyber threats, much like greeters or a loss prevention team are to potential shoplifters and thieves.

110 million

As many as 110 million people had their personal or payment info stolen in the now infamous 2013 data breach at Target.

The widespread theft of Target's customers' data had a significant impact on the company's profit, which fell more than 40 % from the same period a year earlier.

Net earnings dropped from $961 million to $520 million after the breach.

Whenever any aspect of your business is connected to the internet, it is constantly sending and receiving information and data in small groups, commonly referred to as 'packets.'

Among these packets of information there is genuine, safe business traffic coupled with the occasional malicious grouping seeking to exploit a weakness or vulnerability in your system.

A firewall filters these packets to see if they meet a certain criteria, set by a series of rules based on known threats and tactics, and allows or blocks these packets accordingly.

However, as hackers and methods of cyber-attacks have become more complex, so to has the type of firewall protection needed to protect your business from these developing threats.

While the majority of internet services already provide basic firewall protection, many business owners are unaware that the vast majority of standard firewalls only monitor incoming traffic by default. This can give business owners a false sense of security and enable 'hackers,' and other cyber criminals, to view outgoing traffic that may contain credit card information, customer transactions, and other types of financial communications.

If, and when, information like this gets into the wrong hands, it can cost your business hundreds of thousands of dollars in both remediation and legal costs, as well as the drop in sales that accompanies a loss in reputation and perceived security.

Nationwide retailer, Target, learned this the hard way last year after its now infamous data breach.

Additionally, almost all tech-savvy folks know exactly what traditional firewalls protect users from, and how they do it, which allows hackers to design viruses and other forms of infectious programs in a way that disguises them from most firewall filters.

While clever, this hacking strategy is easily thwarted if your firewall has up-to-date information and diagnostics on the most current strategies and sources of these types of attacks, which unfortunately, most standard firewalls do not.

With these types of vulnerabilities, your sensitive business information, bank account numbers, and customer transaction details are essentially available to the public after a bit of tinkering and patience on the part of cyber criminals.

So What Can You Do? Fortunately, with the development of the cloud-based Next Generation Firewall (NGFW), these vulnerabilities are all but eliminated, and the risks associated, mitigated.

> **NGFWs are the latest development in firewall protection for your business network, and are used by all national and international businesses to deter hackers and other forms of cyber-criminals.**

In essence, NGFWs go beyond the common protections provided by traditional firewalls by widening the filtering criteria to include intended application, user identity, and source reputation of all incoming traffic.

Additionally, when NGFWs are cloud-based they're able to be routinely updated on the most current list of known malicious applications and hacking techniques used by cyber criminals, allowing an ever-evolving standard of protection for your business's sensitive data.

Traditional Firewall

"5-tuple"

- Source of the IP address
- Destination of the IP address
- Source of the port
- Destination ports of 80 and 443
- Destination of the specific protocol

Next Generation Firewall

Includes all the standard features of traditional firewall in addition to:

- An Integrated network intrusion prevention system (IPS) with deep packet scanning
- Web filtering to prevent access to 'high-risk' websites
- Gateway anti-virus to scan incoming data for malicious content
- Application Control Abilities

NGFWs are the latest development in firewall protection for your business network, and are used by all national and international businesses to deter hackers and other forms of cyber-criminals.

However, not all NGFWs are the same — or rather, not all firewalls named NGFWs actually offer next generation protection. In order to get the protection you need, your NGFW should include:

- **All the standard features of a traditional firewall**

  Includes packet filtering, network address translation, and VPN capabilities

- **An integrated network intrusion prevention system (IPS) with deep packet scanning**

  While Intrusion Detection Systems (IDS) have been one of the most common security solutions on the market for some time, such systems continue to evolve and respond to the ever-changing threats of the modern cyber world.

  One such evolution brought on by the NGFW is the change from a basic Intrusion Detection System to a Signature-based Intrusion Prevention System, which incorporates all the pre-emptive detection abilities of a traditional IDS with the ability to then tag and prevent potential threats from entering a network or organization.

  Similar to an IDS, a Signature-based IPS monitors and scans traffic flowing into the network for malware and suspicious activity. Where it differentiates, is in its ability to respond to known, as well as suspicious, malicious signatures.

  Additionally, with the adoption of cloud computing, the effectiveness of Signature-based IPSs has skyrocketed, as it grants signature-based IPSs access to an online database of thousands of new and unique signatures, as well as real-time updates and data on new developing threats and reputation-based detection technology.

- **Web filtering to prevent access to 'high-risk' websites**

  Unknowingly going to 'bad' websites, or downloading 'infected' content, is one of the most common ways a computer or network gets infected. With web filtering, a NGFW goes beyond traditional firewall protection by 'following' the user out onto the web, and preventing them from accessing questionable sources and thereby accidentally putting your network at risk.

  With cloud-based web filtering provided by Fortinet, users can select category-based filtering depending on the needs and concerns of their specific business model and industry.

  Additionally, as some threats only occur occasionally, cloud-based web filtering also allows for temporary blocks, or in some cases bypasses, on certain web content, giving more control and customization to the user.

> **Gateway Anti-Virus catches zipped files, polymorphic viruses, and other more advanced threats that the average anti-virus is unable to protect against.**

- **Gateway anti-virus to scan incoming data for malicious content**

  Gateway Anti-Virus allows applications across the enterprise to check files and other types of incoming data for potential threats to the system through a full proxy mode scan, which catches zipped files, polymorphic viruses, and other more advance threats that the average anti-virus is unable to protect against.

- **Application Control Abilities**

  Application control (also known as "application awareness") is capable of identifying applications and applying controls at the application layer (such as allowing regular Skype calls but blocking users from being able to transfer files over the service.)

These application control services are an added security feature with the NGFW, to help monitor and block the input, output, and system services calls when they do not meet the configured policy of the NGFW.

However, while implementing a NGFW is a major step toward securing your internet connection from malicious attacks, it is only the first step.

A NGFW will provide sufficient protection from internet-based attacks, but it is incapable from stopping people within range of your wireless signal from accessing your network and wreaking havoc from within — and with the latest technology, your Wi-Fi signal may be reached by someone operating from all the way down the block.

3 Ways an Unsecured Wireless Connection Can Cost You Big Time

Many businesses nowadays use wireless (Wi-Fi) networks to enable their laptops and other business-specific hardware to connect to the internet and do on-the-spot transactions and business processes.

Unlike a traditional wired network, which requires a "rat-nest" of wires to connect all one's devices to the internet, Wi-Fi networks are much more convenient and practical, as they allow for easy internet access and scalability for the number of connected devices your small business may need at any point in time.

However, these benefits are not without their shortcomings and unlike traditional wired networks, which are extremely difficult for someone to hack into and require a physical presence to do so, an unsecured Wi-Fi network exposes the business or network owner to unnecessary risk from outside intrusion.

Wi-Fi networks generally include a modem that is attached to both the cable or telephone network, and a wireless router which provides broadband internet service via a Wi-Fi signal.

The big problem with these wireless signals is that, if unsecured, they often give indiscriminate internet access to any device in range, which allows unauthorized users to access your network and use your bandwidth without your knowledge. This unauthorized access presents three major, yet unnecessary, risks that can raise your business costs:

- **An increase in your monthly Internet bill especially when paying per byte of data transfer.**
- **A decrease in Internet speed since you are now sharing the same internet connection with other users.**
- **Create security hazards as others may hack your computers and access personal files or download malware or illegal files through your wireless network, leaving you responsible for damages.**

If your small business, like so many others, is already running on tight margins, these three added risks can lead to data breaches, catastrophic losses, and, ultimately, business failure if left unchecked.

So What Can You Do? Securing your wireless connection is one of the most basic strategies for protecting your business and ensuring the integrity of both your wireless network and all the devices connected to it.

Luckily, it also happens to be a very simple and easy-to-implement solution for even the most tech adverse of us. A simple Google search will turn up tons of results and how-to-videos you can watch that will guide you each step of the way. But for convenience sake, here's our 5-step process for securing your wireless network:

1. Set a password for your wireless network

Since most default, factory-setting passwords are publically known, it is necessary for you to come up with your own password for your wireless network. Choose something long, and preferably avoid words or street names, or things that are connected to any aspect of your business.

2. Change your network's SSID name to something unique

This makes it harder for malicious users to find your Wi-Fi network and attempt to gain access by impersonating you. Everyone uses 'Admin' or 'Linksys' and hackers know that.

3. Check to make sure your router's firmware is up-to-date

You can find the existing firmware version of your router by typing 192.168.1.1 into your internet browser.

4. Disable remote login

This is often the first strategy of a brute force attack by a router worm or virus attempting to gain access to your network, and can be done under your router's settings.

5. Disable wireless administrating

Change the setting that allows administrating the router through a wireless connection to 'off' (meaning that you need to connect with a LAN cable for administration.) This disables any wireless hacking into the router.

In essence, having a (really) complex passphrase, a unique network name, MAC Address filtering, and an up-to-date software should provide sufficient security for your wireless network against most common attacks. Not only will it be harder to find, but it will take more time and energy for an unauthorized user to gain access to your network.

However, while this may stop your average mal-doer, there is no guarantee that it will stop a dedicated hacker with the right tools and patience. Often, this type of attacker will not waste time on the common network, but **if your network is hiding something of value, like credit card information or sensitive data, they may be drawn to it like blood in the water.** If this is the case, more security may be warranted.

No Half Measures: Without Advanced Threat Protection (ATP) Your Cyber-Security Strategy is Incomplete, Giving Criminals Opportunities to Exploit

On today's internet, threats to your small business's network security can come from anywhere, with threat levels ranging from 'novice hacker' to 'hardened cyber-criminal.'

Luckily, the former is rather easy to deal with, but while more advanced firewalls and strategies to secure your wireless signal may protect yourself from your run-of-the-mill cyber-threat, small businesses like yours are increasingly becoming victims of more targeted, and hard hitting, cyber attacks that are not so easily dissuaded.

To put it simply, as **more and more 'professional hackers' are discovering the unmined potential of relatively unprotected small business networks,** the average cyber threat these businesses face is becoming more intelligent, and more difficult to prevent, **requiring business owners to implement enterprise-like levels of protection to face enterprise-like levels of attack.**

Unfortunately, the sophisticated level of protection that large-scale enterprises use to keep their networks secure often comes with a large-scale price tag, making them unaffordable for small businesses owners to implement.

As a result, many vendors have begun suggesting a strategy known as 'sandboxing' — in which suspicious code or programs are tested/operated in a contained, virtual environment that separates them from your network - as an alternative for small businesses to mitigate some of the increased risk inherent to being online today.

However, while strategies like these certainly have their benefits, they are only one part of an overall cyber security protection apparatus that large enterprises rely on to protect their cyber assets.

Without the whole package, small businesses are only protecting themselves from a very small and specific source of common cyber threats, giving themselves a false sense of security and leaving their networks vulnerable to a majority of the more commonly advanced methods of network intrusion and data breaches.

To give a parallel example, **relying on a small spectrum of advanced IT protection is similar to implementing security tags,** cone locks, or alarming ink tags **on only a small portion of your merchandise,** allowing most shoplifters a free ride home once they've managed to stuff their bags with unpaid goods.

So What Can You Do? Fortunately, due to the adoption of cloud-computing, small businesses no longer need to sacrifice quality, overall protection for affordability.

With cloud-based Advanced Threat Protection (ATP) systems, small enterprises now have access to a comparable professional enterprise-like protection apparatus, which focuses on the five most fundamental areas of advanced protection, at a fraction of the cost.

The 5 areas that make up the framework for large-scale enterprise protection are:

Framework for Large-Scale Enterprise Protection

1. **Access Control:** By limiting access to the network through certain, predetermined authorized ports available to authorized users only, this feature of an ATP system reduces the overall risk of a network breach or data leak by minimizing the vulnerability of the network at large to only a few access points.
2. **Threat Prevention:** Similar to an intrusion prevention system, threat prevention monitors and inspects all incoming code, packets of data, visited websites, and program/command applications for suspicious and known methods of intrusion.
3. **Threat Detection:** In addition to threat prevention, this feature of an ATP system continues to monitor the network for indicators of intrusion or compromise that may have gotten past the first few layers of protection.
4. **Incident Response:** The new feature of an ATP system identifies and contains suspicious activity when either of the previous prevention and detection systems identifies a threat in your system.
5. **Continuous Monitoring:** Continuous monitoring, the baseline for ATP, assesses and improves your current security measures against the newest known threats and methods of attacks.

In today's online world, threats to network security are evolving constantly and without access to live updates or a large database of known and developing threats, traditional firewalls, anti-virus, and even sandboxing, cannot prevent infections they have not encountered and documented before.

As new cyber threats become more automated and intelligent, more flexible and in-depth measures of protection are warranted. **Without a cloud-based ATP system in place, your business's network security will be playing a game of perpetual catchup**, where the stakes are higher than they have ever been before.

What Is Data Leakage Prevention (DLP) and Why Do You Need It?

Even with all the right tools and systems in place, data breaches still happen. Just like how shoplifting is, at some point, unavoidable despite your best efforts and strategies, hackers will occasionally gain access to your system either through an explicit attack or, most often, by being "invited" in after masquerading themselves as something much more benign.

However, just because they managed to weasel themselves into your system, doesn't mean you have to just let them waltz right out with valuable information in their hands.

Would you give up on trying to stop a shoplifter just because they managed to slip merchandise in their bag without anyone noticing?

Unfortunately, many small business owners are unaware of the threat these cyber thefts pose to their businesses and are woefully unprepared to stop them.

According to a recent poll by the U.S. Small Business Administration, **86% of small business owners say they are satisfied with the amount of security they provide to protect customer or employee data**.

Visa Inc. reports small businesses represent more than 90% of the payment data breaches reported to the company.

Something's not adding up.

The reason for this discrepancy is that many small business owners misunderstand the threats they face in the digital age, causing them to misallocate precious resources when looking to beef up their online security.

When properly utilized, intrusion prevention programs like NGFWs and network encryption have protected data from explicit forms of 'hacking' sufficiently enough, that it has caused a number of would-be hackers to redesign malware, or viruses, to become concealable among other seemingly useful programs or links.

Due to this, most security breaches now a days actually come from malware "invited" into the system by unsuspecting users opening or downloading a bad link from an email or website, making it much more difficult for most prevention programs to stop.

Somewhere around 98% of business data breaches happen this way. Once this type of malware takes root in a victim's computer or device, it waits for the user to visit a banking or financial site and then automatically captures log-in information and sends it back to the cyber criminal, who can then use those credentials to wipe out an account.

By constructing your digital security to rely heavily on 'gate-keeper' like software and other forms of outward protection, you leave your network practically unprotected for when an unauthorized user eventually manages to gain access inside.

So What Can You Do? With a proper data leakage prevention (DLP) program in place, the risk posed by these masquerading malware programs that manage to get into your system becomes null.

Since DLP programs prevent your company's sensitive data (such as account numbers, passwords, and client credit card information) from being accessed or transferred out of your system, you can rest assured that even if a 'hacker' gets by the perimeter defensives, there is still another line of defense between them and the prize.

A Data Leakage Prevention (DLP) system is essentially the loss prevention team, security tags, and exit-alarm system of the digital age.

By classifying your business's data and files based on their sensitivity, which you can control or automate, a DLP system prevents important information from leaving your system unauthorized by monitoring the data while in use, in-motion, and in storage to ensure that the data is being handled in the proper way by the proper people.

Similar to how physical loss-prevention tools and protocols prevent shoplifters from exiting your store with unpaid merchandise, DLP programs protect your business from sensitive-data breaches, and the financial risk and costs that accompanies them.

Protecting Your Business in the Digital Age

The world is far more connected now than it has ever been before, providing a multitude of opportunities for business advancement and increasing sales, while also introducing a variety of accompanying new risks, like cyber theft, electronic shoplifting, and new-and-improved point of sale scams that go after you and your customer's financial data.

With the increasing frequency of data breaches and cyber-attacks suffered by small businesses today, you can't afford to leave your business or clients unprotected against these threats.

These risks presented by the digital age will always be there to threaten your business, and short of closing off your business from the online world, entirely — there's only so much we can do to protect ourselves from them and mitigate the chances of disaster.

However, acknowledging this is not a white flag, nor an admittance of defeat, but rather, a more complete understanding of the new challenges and decisions faced by businesses today.

Thanks to recent developments in the field of IT security and cloud-computing, adding the four previously discussed types of security features to your business's network has become an affordable option.

There is a new plug-and-play solution designed specifically for non-tech savvy individuals that simply requires is a small, router-like device that plugs in to your internet connection and sits between any data collection device at your store, like a point-of-sale computer, desktop PC, or credit card terminal, **and provides small businesses with Fortune 500 levels of protection.**

While no system is completely secure, and getting anywhere close to near perfect protection would be prohibitively expensive, the availability and relative low cost of cloud-based IT security solutions currently on the market promises to make the business world of tomorrow a much safer place for small businesses — at least for those taking the right precautions today.