

Cybersecurity Guide



April 2024

Introduction

This eBook focuses on cybersecurity threats that businesses and organizations of all sizes can expect to see and actionable steps leaders can take today to safeguard their business and protect against cyber attacks.

CHAPTER ONE

Cybersecurity is everyone's business



Cyber-attacks are not only against giant targets like the State Department, T-Mobile, and TopGolf, but hackers are also targeting smaller businesses (SMBs)

Staggering Statistics

Human behavior is the biggest risk to cyber security, with eighty-two percent (82%) of breaches caused by human error according to Verizon's Data Breach Investigations Report.

Negligent employees represent a significant portion of insider threat incidents, with fifty-six percent (56%) of reported insider threat incidents caused by negligent insiders.

Malicious or criminal insiders, including employees, contractors, and third-party vendors, were behind 1 in 4 (25%) insider threat incidents.

Small and Medium Sized Businesses are At Risk

Accenture's 2023 Cybercrime Study found that almost forty-three percent (43%) of cyber-attacks are on small and medium-sized (SMBs). Midmarket companies were not immune.

Eighty-eight percent (88%) of larger midmarket firms had cyber-attacks. However, only thirty two percent (32%) of employees in these larger midmarket firms understand phishing, a common attack vector.

Ninety-five percent (95%) of cybersecurity incidents at SMBs cost between \$826 and \$653,587.

Reputation Damage, Business Closures

Not including damage to reputation. According to CopSys research, eighty three percent (83%) of consumers in the U.S. said they will stop spending at a business for several months immediately after a security breach, and twenty one percent (21%) said they will never return to that business. And, sixty percent (60%) of small businesses close within six months of being hacked.

Why It Matters Today

Only seventeen percent (17%) of small businesses implement data encryption as a security measure, and many rely on free consumer-grade cybersecurity solutions rather than enterprise-level protections. This lack of robust cybersecurity leaves small businesses highly vulnerable to attacks that can cripple their operations.

While businesses are adopting more sophisticated software and hardware solutions, technology alone is not enough. Frequently, it is a good-intentioned employee who makes a mistake, falls victim to an email, or skirts safe IT practices because they are rushed for time or were not even aware of the safe practice in the first place.



It all Starts with Someone

Your employees need to aware of their role in preventing cyber-attacks. Training should include:

- What phishing and other malicious emails look like and taught not to click on them
- How to set strong passwords or use passphrases
- And, the importance of keeping operating systems and browsers up-to-date.

Phishing Emails

We all have seen phishing emails trying to trick you into doing something. Here are some common examples:

The fake FedEx message claims the recipient's package is stuck in customs and needs to be paid for with Bitcoin. This phishing tactic tries to get the victim to send money or provide sensitive information.

An email from the IRS asking for overdue taxes is another classic phishing scam.

An email from another company sometimes impersonates an employee or someone the recipient knows. The email asks the recipient to change bank accounts, send a payment, provide payment details, or do a variety of other things.

The email impersonates an authority at the company and asks the recipient to send sensitive information to a third party to gain access to confidential data.

The key to spotting these phishing emails is to look for suspicious email addresses, generic greetings, urgent requests, and links or attachments that could download malware.

Verifying the source directly with the company is the best way to avoid falling victim to these scams.

Passwords/Passphrases

Ideas on setting strong passwords. Passwords should be at least eight characters long and a minimum of eight letters, numbers, and symbols. The longer and more complex the password, the harder it is to guess. Avoid using sequential numbers or letters, personal information, or common words that can be easily guessed.

Password

Weak

Password

Medium

Password

Strong

Consider using a passphrase - a sequence of 4-7 unrelated words. Passphrases are highly secure and easier to remember than random character strings.

Passwords - What to Avoid

Reusing the same password across multiple accounts. This is risky because if one account is breached, all other accounts are compromised.

Sharing or exposing your passwords to others, intentionally or unintentionally, such as writing them down or entering them on public/unsecured devices.

Not changing your passwords regularly and only updating them when prompted or forced to do so can allow compromised passwords to remain in use over time.

Setting up a Passphrase

To set up a passphrase, choose a memorable phrase or sentence least 12 characters long with uppercase and lowercase letters, symbols and numbers. Avoid using personal information or common phrases.

For example: "bO()K451BR^Dbury" or "ywAM100%ot\$tyN+"
Enable the passphrase feature on your hardware wallet or password manager. This will create a new, separate wallet or account that is protected by the passphrase.

When accessing this wallet or account, you must enter the full passphrase and your regular PIN or password. The passphrase is case-sensitive, so enter it exactly as you created it.

The key benefits of using a passphrase are:

- Passphrases provide an extra layer of security over a PIN or password, an attacker would need to know both the passphrase and the PIN/password to access your accounts.
- The passphrase is not stored on the device, so even if your device is compromised, the attacker cannot access your accounts without the passphrase.

By setting up multiple passphrases, you gain more control over your security, which empowers you to protect different accounts and provides more granular control over your security.

Keep Operating Systems and Browsers Up-to-Date

Operating systems require updates with critical security patches to fix vulnerabilities and protect against the latest cyber threats. Running outdated software leaves you exposed to hackers and malware.

Google Chrome

Chrome is the most popular browser in the world, with 3.46 billion users worldwide as of December 2023.

In 2024, Google Chrome is expected to receive security updates weekly, or two to three times a month. This training cannot be a once and done but needs to be refreshed consistently.

What's Your Cyber Security Policy?

As a business owner, you need to protect your business with a well thought out cybersecurity policy. Start by asking yourself questions like:

- Does my business have a policy that restricts access to specific data to employees with the right or need to know?
- When it comes to cardholder data, how is that data recorded and stored? Who has access to it, and why?
- What about disgruntled employees what systems and data might they access?
- When hire seasonal staff what safeguards can be put in place to prevent their access to cardholder and sensitive data?

A basic security template you can follow is [here](#).



PCI Compliance

If you currently or want to accept credit cards for payment, you have signed or will be required to sign a merchant agreement. Your merchant agreement requires you to follow PCI DSS security requirements and practices to be compliant and to continue to accept credit and debit cards for payment. You can find an overview of PCI standards [here](#).

PCI security standards state the business must “implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.”

- **Comprehensive training:** The security awareness training should cover a variety of topics, including phishing, physical security, mobile device security, acceptable use of end-user technologies, and the organization’s security policies and procedures.
- **Tailored delivery:** The training should be customized by employee role and level of access to cardholder data, rather than a one-size-fits-all approach.
- **Ongoing reinforcement:** Security awareness training should be ongoing process with regular refreshers.
- **Measurement and improvement:** Business owners need to the effectiveness of the security awareness program. Regular reviews of staff activity and compliance with policy can be used to continuously improve the program and conduct refresher training.

For those new to PCI compliance, an excellent beginning point and a resource for building an employee training program can be found [here](#).

The Consequences of Non-Compliance with PCI DSS

- **Fines and Penalties:** PCI fines are not like a traffic ticket, but rather penalties in a merchant contract with payment processors and card brands.

The financial burden of non-compliance with PCI DSS can be staggering. Businesses, depending on their size and transaction volume, fines range from \$5,000 to \$100,000 per month.

In the event of a data breach, the fines can be even higher, up to \$500,000 or more, as the card brands (Visa, MasterCard) may impose additional penalties.

- **Legal Risk:** Businesses could face lawsuits from affected customers, leading to substantial legal costs and damages. This could also result in the business being held liable for the costs associated with a data breach, such as card replacement, credit monitoring for affected customers, and forensic investigations.
- **Reputational Damage and Revenue Loss:** The fallout from a data breach due to PCI non-compliance can be devastating. It can severely damage a business's reputation, erode customer trust, and lead to a loss in revenue and customer loyalty.
This is a risk you can't afford to take
- **Increased Transaction Fees or Risk of Termination:** Out of compliance merchants can face increased interchange and others fees and continued non-compliance could put the merchant's relationship with credit card brands at risk.
- **Operational Disruptions:** A data breach can cause significant operational disruptions, including downtime, investigation, and remediation efforts.

Operational disruptions impact the ability to serve its customers and remain a viable business.



PCI Summary

In summary, the consequences of PCI DSS non-compliance can be severe, including substantial fines, legal liabilities, reputational damage, and operational disruptions, which can threaten a business's viability.

PCI compliance is critical for merchants to protect their customers, avoid financial penalties, preserve payment processing capabilities, and mitigate the risks of data breaches and evolving security requirements.

The financial burden of non-compliance with PCI DSS can be staggering. Businesses, depending on their size and transaction volume, fines range from \$5,000 to \$100,000 per month.

Your network is the backbone of your business - everything depends on it. Yet, its security and maintenance can be easily overlooked and exploited.

CHAPTER TWO

What's Connected?



What is Connected to Your Network?

The number of devices connected to WIFI continues to multiply. As convenient and useful as these devices are, they are exploited by hackers.

Thermostats, printers, scanners, security systems, and other devices are often left untouched for extended periods. Manufacturers might have issued a security patch, but unless the firmware is updated, these devices can pose a risk.

Here are some specific recommendations on How to Protect your Business from the Internet by the PCI Security Standards Council:

- Isolate Usage:** Don't use the device or system you take payments with for anything else. For example, don't surf the web or check emails or social media from the same device or computer that you use for payment transactions. When necessary for business (for example, updating your business's social media page), use another computer and not your payment device for these updates.
- Protect Your virtual Terminal:** if you enter customer payments via a virtual terminal (a web page you access with a computer or a tablet), minimize your risk – don't attach an external card reader to it.
- Protect Wifi:** If you offer free Wi-Fi for your customers, make sure you use another network for your payment system (this is called "network segmentation"). Ask your network installer for help with safely configuring Wi-Fi.
- Use a Firewall:** A properly configured firewall acts as a buffer to keep hackers and malicious software from getting access to your payment systems, your e-commerce website, and/or your card data. Check with your payment terminal vendor or service provider to make sure you have one and ask them for help configuring it correctly.
- Use Personal Firewall Software or Equivalent:** When payment systems are not protected by your business firewall (for example, when connected to public Wi-Fi).

Outdated Equipment

Finally, one additional risk is outdated terminals. Not only can these terminals become a security threat due to old firmware, just using this data equipment can open your business up to other liability risks.

With the advent of EMV, in October 2017, the liability for lost card or fraudulent card transactions shifts to the merchant if their POS equipment is not EMV compliant.

There is Help

The online resources of the Small Business Administration and other organizations make it easier to identify threats and train your employees.

Don't overlook your payment processing company; cutting edge payment processing platforms can help mitigate risk and help you remain PCI and card network rules compliant.

Why IntelliPay?

IntelliPay's all-in-one suite eliminates the need to work with other vendors, while detailed reporting simplifies payment management. Spend more time growing your business and less time with payments.

More Money Saving Options

No junk fees, transparent pricing, and customer fee options like surcharging to reduce your cost of credit card processing.

Integrations Save Time

Seamless integrations with QuickBooks online, WooCommerce, etc., or through API, streamline accounting and eliminate manual processes.

Safe and Secure

All customer payment transactions over our customer facing solutions are on our PCI complaint Level 1 network.

Our proven technical and Google cloud infrastructure delivers exceptionally high levels of service availability demanded by our clients, many of whom operate in sensitive operating environments where speed and reliability are vital.

- Multi-layer security
- PCI DSS Level 1
- P2PE
- Tokenization
- Cryptographic signatures
- Isolation
- SAML

The IntelliPay platform exists within the Google Cloud Platform architecture where the environment allows for rapid deployment and high reliability.

As the entire architecture resides within the Google Cloud Platform, network segmentation is provided by the Google Cloud firewall, and the cardholder data environment is completely contained within the Google environment.