Guide to Cybersecurity for Small and Medium Businesses

PART I: UNDERSTANDING CYBERSECURITY
ACKNOWLEDGEMENTS

The Guide to Cybersecurity for Small and Medium Businesses was developed with guidance from the U.S. Agency for International Development (USAID) Bureau for Development, Democracy, and Innovation’s (DDI) Center for Economics and Market Development (EMD) and principally authored by Daniel Vázquez under the Trade and Competitiveness Activity implemented by Resonance Global. Additional contributions and review were provided by Clare Sullivan of the Cyber SMART Research Center at Georgetown University, as well as Jeremy Ravenelle, Evan Legé, and Anne Szender McCarthy of the Trade and Competitiveness Activity.

This document was produced for review by the United States Agency for International Development. It was prepared by the Trade and Competitiveness Activity, contract number AID-OAA-C-17-00110. Its contents are the sole responsibility of the author and do not necessarily reflect the views of USAID or the U.S. Government.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Glossary of Terms</td>
<td>4</td>
</tr>
<tr>
<td>Acronyms List</td>
<td>5</td>
</tr>
<tr>
<td>Foreword: USAID Digital Strategy and Cybersecurity</td>
<td>7</td>
</tr>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Cybersecurity: A Critical Business Investment</td>
<td>11</td>
</tr>
<tr>
<td>Antivirus and Insurance</td>
<td>13</td>
</tr>
<tr>
<td>Origins of Cybersecurity Risk</td>
<td>14</td>
</tr>
<tr>
<td>Data</td>
<td>14</td>
</tr>
<tr>
<td>Access Vulnerabilities: Internet Connections and Physical IT Systems</td>
<td>17</td>
</tr>
<tr>
<td>Categories of Threats</td>
<td>18</td>
</tr>
<tr>
<td>1. Malware</td>
<td>19</td>
</tr>
<tr>
<td>2. Ransomware</td>
<td>19</td>
</tr>
<tr>
<td>3. Phishing</td>
<td>20</td>
</tr>
<tr>
<td>4. Man-in-the-Middle</td>
<td>21</td>
</tr>
<tr>
<td>5. Emerging Threats</td>
<td>23</td>
</tr>
<tr>
<td>a. Internet of Things</td>
<td>23</td>
</tr>
<tr>
<td>b. Fintech</td>
<td>24</td>
</tr>
<tr>
<td>c. Additive Manufacturing</td>
<td>24</td>
</tr>
<tr>
<td>d. Supply Chains</td>
<td>24</td>
</tr>
<tr>
<td>Conclusion</td>
<td>26</td>
</tr>
</tbody>
</table>
As digital connectivity and tools become increasingly important in business operations, micro, small, and medium enterprises (MSMEs) are also increasingly exposed to potential cybersecurity threats. This guide aims to help MSMEs better understand these potential threats and the importance of integrating cybersecurity into core business operations. It also provides information on simple, low-cost tools and approaches that MSMEs can use to increase their resilience to typical cybersecurity threats.

Cyber attacks can be crippling for a business, shutting down equipment, eliminating access to data and communication systems, and potentially putting sensitive client or other business information at risk. The increasing integration between business, customers, and suppliers means that a business’s liability from an attack can also extend to all other partners whose information it manages or transacts with. Although purchasing antivirus software or an insurance plan may provide some basic protection, MSMEs need to invest in cybersecurity as a core business function to truly mitigate the risk of a cyber attack.

To appropriately manage their cyber risk, businesses must first understand their potential vulnerabilities and the range of cyber threats. The core target of cyber attacks is data, whether it’s business information, customer information, or other personally identifiable information (PII). Businesses need to map and track the data they have to understand and address potentially vulnerable points of access. Similarly, businesses need to be aware of their points of access vulnerabilities—whether that is physical access to equipment that retains company data or Internet and other network connections.

To better manage these potential vulnerabilities, businesses must also understand the types of attacks that they may be subject to. The growing range of threats includes malware, ransomware, phishing, man-in-the-middle (MitM) attacks, and other emerging risks linked to fintech, Internet of Things (IoT), and supply chain integration. Simple tactics, such as developing standard policies and procedures that segregate and limit access to data, educating employees on potential threats, and ensuring that IT equipment is updated and maintained, can have a significant impact on mitigating cyber threats.
GLOSSARY OF TERMS

**Antivirus software:** A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents, sometimes by removing or neutralizing the malicious code.¹

**Cryptocurrency:** A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography rather than by a centralized authority.² Examples include Bitcoin, Ethereum, Monero, etc.

**Cyber attack:** An attack via cyberspace that targets an organization’s use of cyberspace, for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure or to destroy the integrity of the data or to steal controlled information.³

**Cybersecurity:** The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.⁴

**Distributed denial-of-service (DDoS):** A form of cyber attack in which the attacker renders the target machine, website, or network unavailable to its users by flooding the target with requests in an attempt to overload the system.

**Fintech:** Digital technologies used to deliver financial and payment services.

**Internet of Things (IoT):** Everyday objects (such as security systems, lights, refrigerators, industrial equipment, etc.) with the capability to connect to the Internet and to send and receive data.

**Internet Protocol (IP) address:** A unique string of characters that identifies each computer using the IP to communicate over a network.⁵

**Malware:** Software that compromises the operation of a system by performing an unauthorized function or process.⁶

**Man-in-the-middle (MitM):** A type of cyber attack that unlawfully interrupts or modifies data as they are transmitted between two legitimate parties, frequently via unsecured Wi-Fi or other network infrastructure.

**Personally identifiable information (PII):** When customer information is linked or linkable to the identity of a person, those data are considered PII or personal data. Technical standards or laws define and protect these data.

**Phishing:** Fraudulent messages that appear real and seem to be from a legitimate source to trick employees into providing information like credit card numbers, bank account details, and login credentials. They can also trick users into carrying out actions, such as financial transactions.

**Ransomware:** A type of malware that prevents or limits users from accessing their system, either by locking the system’s screen or by locking the users’ files, until a ransom is paid.⁷

**Sensitive personal information (SPI):** When compromised, this type of PII has the increased risk of causing financial, reputational, or personal harm to a person.

**Virtual private network (VPN):** A method employing encryption to provide secure access to a remote computer over the Internet.⁸
# ACRONYMS LIST

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CFO</td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MitM</td>
<td>Man-in-the-Middle</td>
</tr>
<tr>
<td>MSME</td>
<td>Micro, Small, and Medium Enterprise</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>SPI</td>
<td>Sensitive Personal Information</td>
</tr>
<tr>
<td>USAID</td>
<td>United States Agency for International Development</td>
</tr>
<tr>
<td>USD</td>
<td>United States Dollar</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>

---

1. [https://niccs.cisa.gov/about-niccs/cybersecurity-glossary](https://niccs.cisa.gov/about-niccs/cybersecurity-glossary)
2. [https://www.oed.com/](https://www.oed.com/)
5. [https://www.oed.com/](https://www.oed.com/)
8. [https://www.oed.com/](https://www.oed.com/)
FOREWORD: USAID DIGITAL STRATEGY AND CYBERSECURITY

The Guide to Cybersecurity for Small and Medium Businesses follows the guiding principles and objectives laid out in the Digital Strategy of the United States Agency for International Development (USAID). USAID has a long history of stewarding development-driven digital goals and promoting digital tools to address development challenges. USAID co-drafted the Principles for Digital Development and became the first of more than 200 organizations to officially endorse them in 2015.

Building on this leadership, USAID launched its first Digital Strategy (2020–24) in 2020. The Strategy offers the Agency’s vision on incorporating digital technology in its development and humanitarian work, based on the principles of open, secure, and inclusive digital ecosystems that contribute to increased self-reliance of emerging market countries and broad-based growth.

The Strategy recognizes that digital technologies have the potential to bring informal merchants, women entrepreneurs, smallholder farmers, and other small and medium businesses access to markets, information, and finance. Although the emergence and adoption of digital technology leads to multiple benefits, it also exposes adopters to the risks of the digital space. In this context, USAID’s role in strengthening cybersecurity is to support the development of resilient local digital ecosystems by:

- Helping with the adoption of policies that promote global cybersecurity best practices;
- Facilitating the protection of Internet freedom;
- Promoting the principles of the free flow of data and the protection of intellectual property; and
- Prioritizing the development of a cyber-ready workforce in the countries in which USAID works.

Recognizing the economic and social benefits that result from public-private partnerships in the digital space, the Strategy also calls for joint work with the private sector to improve local capacity and preserve trust in digitally enabled services and to counter cyber-related threats to economic growth.

---

9 https://digitalprinciples.org/
INTRODUCTION

Significant improvements in access to information technology (IT) and Internet connectivity have dramatically increased opportunity for businesses around the world. However, the increased connectivity also creates new risks. As businesses rely more on digital tools, these tools create potential vulnerabilities to ever-evolving cyber threats.

This guide aims to help micro, small, and medium enterprises (MSMEs) build basic digital resilience by focusing on cybersecurity. It explains foundational concepts of cybersecurity and suggests basic, low-cost actions that MSMEs can implement and later integrate with more sophisticated strategies as the organization matures in its understanding of cyber risks. It also encourages business owners to view cybersecurity as another operational risk. Cybersecurity is a complex problem that affects a variety of business operations—without a one-size-fits-all solution. This guide presents a range of actions available to MSMEs to help mitigate the specific risks most pertinent to their business operations.
PART I: UNDERSTANDING CYBERSECURITY

CYBERSECURITY: A CRITICAL BUSINESS INVESTMENT

Business operations are increasingly reliant on information and communications technology (ICT) to manage inventories, conduct sales, and communicate with suppliers and clients. Disruptions to these fundamental business systems can be devastating for MSMEs. If a cyber attack suddenly shuts down all computer-based operations and communications, eliminating access to all data, email, or other electronic information, business would grind to a halt. For MSMEs, these are increasingly real risks and they must consider whether they’re prepared to weather such a crisis and, if data are permanently lost, how employees, clients, suppliers, and partners would be affected.

Payment records, sensitive business plans and strategies, and business information are increasingly kept only in digital format. However, convenient access to information and ease of communication are often prioritized over cybersecurity. Without adequate measures in place, an attack can severely damage a business, endanger its position in the market, and, in the worst cases, be a legal liability.

Amid the COVID-19 pandemic, the trend to adopt digital tools has accelerated to keep operations open. Businesses have rushed to adopt new technologies that enable remote work and make up for lost revenue, often without dedicated IT support. Managers and business owners tend to assume that an IT product is safe because it is available in the market, but that is not always true. Leadership often does not pay attention to cybersecurity until vulnerabilities of software (like Zoom¹² or Slack¹³) are publicly exposed or their security improvements are announced.

The consequences of a cybersecurity incident are not only internal. These incidents can quickly expand to customers or suppliers and can tarnish a business’s reputation. They can even lead to legal liabilities. For example, a cyber attack targeting a health clinic could expose patient clinical records or hold these records hostage and inaccessible. Similarly, the data breach of a bank or financial institution could expose sensitive personally identifiable information (PII), allowing hackers to steal individuals’ identities—impacting their credit ratings or worse. Therefore businesses must consider not just the potential impacts on their own operations but also the impacts on all other partners whose information they manage or who they transact with.

A.P. MØLLER-MAERSK CYBER ATTACK

In June 2017, A.P. Møller-Maersk, a multinational conglomerate that owns one of the world’s largest shipping companies, faced a crippling cyber attack. A malicious program (malware) attacked phone, email, and other systems, stopping corporate functions in a matter of hours. It took weeks and an army of hundreds of people to rebuild IT operations. This breach cost the business an astounding $300 million U.S. dollars (USD).¹¹ Maersk’s case should be a cautionary tale to businesses, regardless of size, of the real implications of cybersecurity.

¹² During the first months of the COVID-19 pandemic, the number of Zoom users drastically increased from 10 million to 200 million. https://www.cnbc.com/2020/04/03/how-zoom-rose-to-the-top-during-the-coronavirus-pandemic.html
DATA PRIVACY VERSUS CYBERSECURITY

The intersection of privacy and cybersecurity can be confusing. “Security” refers to data being protected, while “privacy” refers to safeguarding the identity of the person associated with the data. Privacy applies to information that is saved in any format—not just digitally. A classic example is that of medical records in a doctor’s office. There are privacy concerns, regardless of whether a patient’s health file is kept in printed or digital format. If the information is stored digitally, the law can require the doctor to implement additional measures to prevent unauthorized electronic access to those records.

Businesses should be aware of local privacy and cybersecurity legal frameworks that must be observed. Most nations have made—or are in the process of making—these laws. (About 80 percent have privacy laws, and 85 percent have cybersecurity laws.) International regulations may also create legal requirements that go beyond national borders if a business has access to, or works with, data of citizens of another country.

Beyond pointing out this intersection and the possible broader implications, this guide does not explore the issues of privacy in detail. Businesses that handle data of any foreign national, do business in another country, or even have a website that may be used internationally should obtain legal guidance on the national and international privacy laws that can apply. Specific legal advice that takes into account local requirements and individual businesses is beyond the scope of this guide, but every business should keep in mind their legal situation and should fully understand their legal obligations based on their location and the data they are collecting, handling, and storing. The compliance requirements can be complex, so it may be necessary for a business to obtain specific guidance from the regulator and/or a legal professional. As a routine part of running a business, owners should take all the steps necessary to comply with those legal obligations.
Antivirus and Insurance

Quality antivirus programs are widely available and provide valuable services but are insufficient to fully protect a business from cyber attacks. Similarly, insurance may mitigate the financial impact of a cybersecurity incident but cannot guarantee the recovery of data or reputation. Cybersecurity should not be viewed as an isolated line item in the budget or a “check in the box” to be managed by a single employee. It is an integral component of a successful business.

All cybersecurity incidents involve unauthorized access from inside or outside the business, and most involve removal, copying, or holding data hostage for payment. The rapid evolution of criminal activities in the black market, along with increased access to often inexpensive IT tools at the retail level, can reduce the reliability of an antivirus program, especially if it is not regularly updated to address emerging threats. Antivirus programs are still a very important line of defense but should not be regarded as infallible and should be part of a more comprehensive approach to building a business’s digital resilience.

Similarly, a standard business insurance policy likely would not cover all the costs associated with a cybersecurity incident. Some costs, such as employee theft, may be covered, but many others, like lost productivity or the need to replace IT equipment, might not. Some insurers offer specialized cybersecurity coverage (see “Cyber insurance,” in Part II of this guide) but still cannot repair damage to a company’s reputation or productivity.

COLONIAL PIPELINE RANSOMWARE ATTACK

In early 2021, a ransomware attack on the Colonial oil pipeline in the United States led to gasoline shortages in several regions and was a national news story for over a week, eventually resulting in a $4.4 million USD ransom payment in bitcoin (a portion of which was later recovered). Although not all businesses will be the target of an attack of that type or magnitude, the insurance business Beazley Breach Response Services found in 2019, after reviewing 3,300 incidents, that businesses are prime targets of ransomware, accounting for 71 percent of attacks, with an average financial demand of $116,324 USD.

14 https://unctad.org/page/cybercrime-legislation-worldwide
Because of their ever-evolving nature, it is impossible to comprehensively catalog all types of cyber threats. Security software company McAfee estimated that in the second quarter of 2020, there were over 1.2 billion different malicious software programs (known as “malware”). The complexity of this malware wave is compounded as new technologies arrive and hackers learn how to exploit their vulnerabilities. However, most cybersecurity incidents have several common elements: when data, connectivity/access, and a vulnerability are put together, a company is at risk.

**Data**

Behind nearly every attack is a criminal mind looking for electronic information (data) that has some value, either for the targeted business or for the attacker. An attacker can sell hacked information back to the breached business or to third parties in the black market or can use it to engineer other attacks. Typical examples of sought-after data are:

- **Customer information.** Examples are phone numbers, addresses, demographics, buying patterns, or general interests, even when the identity of the person is not known. Artificial intelligence (AI) tools can be used to analyze digital behavior, through customer information gathered by a business.

- **Personally identifiable information (PII or personal data).** When customer information is linked or linkable to the identity of a person, those data are “PII” or “personal data.” Technical standards or laws define and protect this data. Privacy laws, like the European Union’s (EU’s) General Data Protection Regulation (GDPR), which also forms the basis of many other countries’ laws, regulate personal data and set guidelines for collecting, using, keeping, disseminating, and disposing or de-identifying it.

- **Sensitive personal information (SPI or sensitive personal data).** This type of PII has the increased risk of causing financial, reputational, or personal harm to a person when compromised. Because of this higher risk, regulations impose stricter rules on this information to protect it. In many jurisdictions, this type of information is specifically defined and the required protections are prescribed. As a practical matter, credit card and financial information, personal identification numbers (PINs), tax identification numbers, health data, and biometrics should be considered sensitive and protected accordingly.

- **Business information.** This includes client and pricing lists, intellectual property, website logins, expenses, contracts, financial reports, and information used for regulatory compliance filings. Anything relating to the operation of the business falls into this category.
Definitions about what constitutes each type of data and how they should be protected differ from country to country. Businesses, first and foremost, should comply with these applicable laws. Where there is no existing legal framework, or when a business would like to exceed the minimum legal requirements, it must first catalog the internal business processes and policies for data management and then examine them for weaknesses or flaws. This includes examining the processes involved in obtaining the data (i.e., who can obtain information, when, and how) especially if the data can be considered personal data or sensitive personal data. This also includes examining how the data are stored and processed and how it is eventually removed from the system.

Knowing the processes and addressing identified vulnerabilities can demonstrate a business’s commitment to cybersecurity, which can be useful to mitigate potential liability should a breach occur. If an organization does not have a policy for collecting and managing data, it should develop one. To mitigate risk, businesses should limit data retention to only the information that is necessary and should not collect or keep extraneous data on customers, transactions, or operational history.

**MITIGATING RISK:**
**MAPPING BUSINESS DATA**

The sensitivities and vulnerabilities of data vary by business, and not all information needs to be safeguarded in the same way. For these reasons, individual businesses should catalog their data, the responsibilities attached to that data, and which roles and positions need access to the data.

Create a data map by identifying all the information that the business collects, stores, generates (e.g., customer credit card numbers, contract information, sale lists, purchase orders/history, sourcing agreements, employee personal information, studies/publications, patient health history, client confidential information, etc.). A business could collect information by apps, websites, physical forms, phone calls, or text messages and could then enter it manually or automatically into the business’s database.

Categorize the information by type according to the risk it poses in case of loss, damage, tampering, public release without authorization, etc. For example, see the three-tier classification below:

- **(R) Restricted** (data with the fewest authorized users). This includes patient medical history, financial information, the business’s trade secrets, and any other information or data that by law, legal agreement, or contract should be safeguarded following special procedures. A breach or an incident involving this information needs to be reported to customers, law enforcement, or a government agency. The loss of, damage to, or tampering with this information can result in severe financial, reputational, or operational damage or legal liability to the business.

---

18 For more information on AI, see [https://www.ibm.com/cloud/learn/what-is-artificial-intelligence](https://www.ibm.com/cloud/learn/what-is-artificial-intelligence)
• **(C) Confidential** (data that select employees can access). Generally, this information is proprietary to the business and not publicly accessible but is less sensitive than restricted information. This could be client and price lists, business memoranda, reports for clients that are not public, and information not made public but shared with clients. Keep in mind that information shared by email, text messages, or messaging apps (e.g., WhatsApp) can also fall under this category and should be considered. The loss of, damage to, or tampering with this data can result in financial, reputational, or operational damage to the business, or may result in legal liability, but it won’t be as serious as with restricted information. Not all employees need to have access to all confidential business information. Businesses might be able to subcategorize information to decide who needs to know what and to grant access accordingly, with all that data falling within the confidential category.

• **(G) General** (data that all employees can access). Information that is made public by the business through its website, publications, partners’ websites, government records that are available to the public, etc. The loss of, damage to, or tampering with this data can have minimal or no effect on the business. In this category are released publications, public policies, public listings of clients, and knowledge shared through public forums, among other information.

Consider current policies for data access, sharing, and deletion, and whether they are appropriate to meet the company’s legal and contractual obligations and risk profile.

Determine who should be responsible for authorizing access to data, sharing restricted data, determining how information should be transferred outside and within the business (e.g., restricted information only with password protected PDFs that can’t be modified), and deciding whether certain data should only be stored with encryption.

Define a policy for data retention and deletion. Companies do not need to maintain all data in perpetuity. There are several tools available that can securely erase information, and these tools comply with one or more technical standards, like DoD 5220.22-M, VSITR, Schneier, Gutmann, or RCMP DSX. These programs remove the data from a hard drive in a way that cannot be recovered by the specialized software used by hackers.

Update, review, and keep updating. As a business evolves and adds operations that generate or store data (software, vendor service, apps, etc.), the new information needs to be added to the data map. Businesses should update their data map at least once a year.
**Access Vulnerabilities: Internet Connections and Physical IT Systems**

Cyber attacks can originate from both outside and inside a business. To enter a business’s IT network and have access to data, outsiders can use a number of methods discussed below. However, insiders, such as employees, contractors, and even customers, can also pose a security threat to the business and create a cybersecurity incident.

If a business is connected to cyberspace, particularly through the Internet, it is exposed to potential attack from actors outside the business. To penetrate the network, attackers look for vulnerabilities and use them as access points. An “access point” can be anything that is connected to the business’s IT infrastructure, such as laptops, routers, Wi-Fi networks, servers, apps, smart phones, other connected devices (IoT),\(^{19}\) cloud storage, and even third-party vendors.

Alternatively, a “point of access” can be an insider, such as an employee or contractor, who has legitimate access to company data and systems. In small businesses, employees often have multiple roles and responsibilities, giving them access to many different types of data. This can increase the cybersecurity risk. A disgruntled employee can take or erase sensitive client information, or an inexperienced trainee or casual worker may inadvertently share sensitive or confidential business or customer information.

Physical access to IT infrastructure, such as being able to log in to someone’s computer, or plugging a cable into the office router, can also be an access point for an attack. A cybersecurity strategy should consider all access points and plan for security accordingly, knowing that cyber and physical access need to be addressed together.

---

\(^{19}\) For more information on IoT, see https://www.oracle.com/internet-of-things/what-is-iot/

CATEGORIES OF THREATS

1. Malware

Malware can infiltrate systems through different delivery methods, including through plugging an infected device into a laptop. The device can be a USB memory stick or peripherals, such as keyboards, charging cables, and printers or mobile phones that have been infected or tampered with—deliberately or inadvertently. Malware can also be downloaded and can infect a machine when a file or program is opened, an infected website is visited, or infected videos are played.

Malware can be used for different purposes, such as taking control of an entire system or parts of it, and for extracting or deleting useful data. Malware is becoming increasingly pernicious, with some types coded to make removal difficult or to avoid detection by antivirus programs. Some programs use stalling tactics that delay execution of specific actions detected by antivirus software. “Rootkits” are another type of malware that, to avoid detection, can hide in operating system code that is not normally monitored by antivirus.

As a first line of defense, companies should ask their employees not to visit suspicious or even popular websites for personal purposes when using business computers. This should include not downloading free content or using pirated or free software—even if it’s for business purposes. Although the initial cost savings may be tempting, the business can end up paying a high price. In the case of pirated software, for example, security processes might have been removed to eliminate licensing requirements, purposely creating vulnerabilities through embedded malware. Security patches are not available for this software because it is not recognized by the manufacturer.

Although not all files and Internet content are dangerous, many products can be, especially those targeted at consumers and offering free access or discounts if an email address is provided. The link and the email contact can be used as conduits for malware and for other unauthorized access to and use of business and personal data by illegal actors.

2. Ransomware

In 2020, it was estimated that ransomware was among the most rapidly growing cyber threats. Some estimates put its growth at over 300 percent in 2020, with ransom payments reaching nearly $350 million USD. This form of malware takes advantage of a person’s or a business’s fear of suffering harm because of the loss of data. The malware makes the data inaccessible to the business, or the business is threatened with a public data release, thereby exposing sensitive business and personal information, unless a ransom is paid.

https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021
Payment is typically requested in a cryptocurrency (e.g., Bitcoin, Monero, or Ethereum). The amount varies, probably taking into account the size of the business, its ability to pay, the sensitivity of the information, and risk of being caught. When a computer is infected, the ransomware typically issues a notification to the computer or device user stating the demand, asserting that the information has been encrypted, and declaring that the attacker is the only one holding the decryption key. The business must then decide whether to pay the ransom. The usual recommendation is not to pay, which is likely to be an easier option if the business has the appropriate backups and processes in place to restore operations.

MITIGATING RISK: RESPONDING TO A RANSOMWARE ATTACK

In the event that a company computer has been targeted by ransomware, the business can follow three simple steps:

• **Step 1: Contain.** Disconnect the machine from the business’s network and the Internet. Keeping it disconnected decreases the risk of the virus spreading to other devices in the network.

• **Step 2: Clean.** The malware needs to be removed from the machine and, if necessary, files need to be restored. At this point, it is strongly advisable that the company obtain professional IT support to perform the system clean and restore tasks. An IT professional should be able to accomplish this without endangering the business’s network. In some cases, the IT professional may use specialized programs to complete these tasks.

• **Step 3: Restore.** If it is not possible to recover the information from the computer or system that was attacked, the company should use backup files to recover the most recent versions. Windows and Apple operating systems have built-in functionalities that allow users to create backups and to restore files from those backups. However, to be useful, these tools must have been activated before the ransomware encrypted the data.

3. Phishing

“Phishing” schemes use fraudulent messages that appear real and seem to be from a legitimate source to trick employees into providing information like credit card numbers, bank account details, and login credentials. These schemes can also trick employees into carrying out actions, including financial transactions. They may also be combined with other attacks and programs, such as installing ransomware on the system, which further increases the threat to a business. Phishing may be done using phone calls, voice mails, emails, instant messages, social media, and chat boxes in collaborative business tools like Microsoft Teams or Zoom. As new communication methods appear and gain popularity, it should be expected that these attacks will evolve, adapt, and continue.
Phishing is one of the most common forms of attacks, with some cybersecurity companies estimating that it affects 90 percent of businesses. In recent years, sophisticated and targeted phishing attacks, known as “spear phishing,” have flourished. In these attacks, hackers use previously gathered information about the target business or an associated person and then pose as a trustworthy source, such as a supplier, customer, or employee, making the request appear credible.

**MITIGATING RISK: PREVENTING PHISHING ATTACKS**

To avoid damaging phishing attacks, businesses should instruct employees not to click on any links or open any files if there is any doubt about the authenticity of a communication. Simple tactics to prevent phishing attacks include verifying that the message is legitimate or looking for inconsistencies (such as incorrect spelling of an email address, e.g., annazon.com instead of amazon.com). Strange link configuration and unusual wording in the message or unfamiliar details are also red flags. Similarly, messages promising a rich inheritance, a lost fortune, or rich compensation for simple tasks are typical phishing scams. Any messages requesting bank or identity information, and any requests to transfer funds, especially to new accounts, should be treated as suspected phishing attempts. Legitimate suppliers and customers usually understand if a business takes the extra step of verifying the authenticity of a communication and appreciate the need for extra security.

4. Man-in-the-Middle

Electronic communications between two or more people (like virtual meetings, emails, or computer-server connections) can be unlawfully intercepted by a third party to eavesdrop or to obtain or modify information. These types of attacks are known as “man-in-the-middle” (MitM) attacks because the attacker intercepts data as it transits between two legitimate parties.

MitM attacks have always been predominant among the mobile workforce, frequently occurring in places that offer free Wi-Fi connectivity with inadequate security, such as hotels, cafes, airports, short-term rentals, public libraries, and community centers.

---

22 Larger corporations have been asked for multimillion dollar payments. For example, attackers demanded a payment of 750 Bitcoins (at that time, $14 million USD) from chip manufacturer Advantech. [https://hotforsecurity.bitdefender.com/blog/conti-ransomware-attack-demands-14-million-from-industrial-iot-firm-advantech-24608.html](https://hotforsecurity.bitdefender.com/blog/conti-ransomware-attack-demands-14-million-from-industrial-iot-firm-advantech-24608.html)


The vulnerability of these Wi-Fi sites is significant because the hosts may not regularly upgrade the residential hardware provided by the Internet service provider (ISP), change the security credentials, or adequately patch IT devices, such as routers, switches, etc. An attacker can use these vulnerabilities to create a MitM attack in a few minutes—with significant consequences.\(^{29}\) It is far better to pay to use a secure mobile network than to risk the insecurity of a free or low-cost Wi-Fi location.

Vulnerable devices and apps also open the door to MitM attacks. All devices have a limited life span. When a manufacturer no longer supports old hardware, it stops receiving security patches, even if problems are known by the manufacturer.\(^{30}\) To ensure that IT equipment remains secure, business plans should include regular replacement and upgrading of hardware and software.

Mobile apps are now ubiquitous in the workplace. However, apps that have not been appropriately configured can be vulnerable to MitM attacks. Cybersecurity firms\(^{31}\) estimate that one in five Android apps and one in seven Apple apps use insecure or deficiently configured HTTP protocols, which do not properly encrypt data as it is transferred from the phone to the app’s servers. Hackers can exploit this weakness to download malware, such as an altered copy of an original app, onto a mobile device and gain access to the business’s network.

Many methods to secure connections and prevent MitM have been developed over the years, with some companies now offering affordable technology to businesses, such as virtual private networks (VPNs), which were previously only accessible to large corporations. VPNs route network use through their servers, often located around the world, so that anyone tracking Internet browsing (from ISPs, to search engines or hackers) cannot locate the user. A business’s network traffic is then associated with the VPN’s servers rather than its own Internet Protocol (IP) address.\(^{32}\)

**MITIGATING RISK: PREVENTING MitM ATTACKS**

When time and budgets are tight, businesses may be tempted to use convenient low-cost security solutions, but these “free” solutions can put sensitive business information at significant risk. To prevent MitM attacks, businesses should:

- **Ensure that secure connections** are established between business devices and email providers and other services, such as cloud computing services.

- **Hire reputable and experienced developers** to create business applications. If free applications are available through different channels, like trade associations or governmental programs, before using, ask for an independent security audit of the program, if it has not been independently audited and certified for security.

- **Use trustworthy service providers** (e.g., Google, Amazon, or Azure), for hosting websites, e-commerce stores, and cloud computing needs. These companies have
good cybersecurity and tend to be more transparent with customers about how they test products, and they share information about threats, etc.

- **Buy hardware from reputable manufacturers** that provide free software updates until the device’s end-of-support date.
- **Install updates** as soon as they are available.
- **Retire old devices that have reached their end-of-support date.** An old laptop given to an intern, if not properly maintained, can be the single most dangerous device in a business’s network.
- **Never assume that a device sold in the used market is safe.** Avoid buying from unrated online sellers or unknown sources.
- **Sanitize second-hand devices** by performing a hard reset or factory restore before using them. If planning to use sensitive business information on a used device, businesses should replace the internal hard drive with a new one, if possible.

5. **Emerging Threats**

With advances in technology and continued digitalization of business, new risks will continue to emerge. Businesses should not assume that all digital products or devices placed in the marketplace prioritize security. Reputable companies build devices and products responsibly and provide support to patch vulnerabilities throughout their useful life. However, less scrupulous companies will prioritize profit or foreign policy objectives of their country of origin over their customers’ security.

a. **Internet of Things**

Technology is entering new spaces, changing how people interact with all kinds of devices—even with buildings and other objects. IoT adoption will bring a new wave of cybersecurity challenges that companies need to balance against productivity, convenience, and increased competitiveness.

Smart door locks and smart energy solutions (like sensors in light bulbs) or production lines with connected devices that assist in the manufacturing process will become omnipresent in the home and the business environment. This accelerated pace of adoption has already seen the appearance of malware, with over 150,000 examples of attacks on IoT devices.²⁵

---

b. Fintech

The financial sector has been one of the fastest adopters of digital technologies, with the commercial benefits spreading throughout the whole ecosystem in the form of improved access to and delivery of financial and payment services. For businesses, this means easier payments (digital payments), transfer of funds with a cell phone (mobile money), obtaining better conditions for loans, easier exchange of financial information across different platforms (open banking), or accessing seed capital in ways not previously possible (crowdsourcing), but it also brings added risk.

The growth of fintech companies has made them prime targets for criminals. Fintech’s vulnerabilities include use of third-party solutions, in-house application development, incompatibilities with legacy systems, and attempts to abuse the system by money launderers. These threats can be compounded by classic vulnerabilities, such as employees falling prey to targeted phishing attacks.

Businesses that use fintech solutions should be aware of the higher risks associated with instant payments and transfers that cannot be canceled or rescinded, in addition to the risks from immediate access to financial information. When possible, businesses that use these solutions should impose controls to mitigate risk, such as limiting transfer amounts and access to banking apps.

c. Additive manufacturing

Malware in additive manufacturing, also known as “3D printing,” can be used to insert defects in printed parts, causing the final product to not meet specifications. The malware can even steal plans of objects to be printed. Additive manufacturing is increasingly used for prototyping. The consequences of a defective part or the loss of trade secrets in early development processes can be devastating for a business.

d. Supply chains

The rapid pace of digitalization of all sectors and the expanding levels of connectivity raise the cybersecurity risk that suppliers bring to supply chains. It can increase a business’s cybersecurity vulnerability because of the interconnections with other businesses. Modern, highly integrated supply chains require both upstream and downstream chains, and integrated communication on cybersecurity matters.
MITIGATING RISK: IDENTIFYING POTENTIAL CYBERSECURITY THREATS

For small organizations that don’t have dedicated IT support, one of the most difficult challenges is identifying the potential cybersecurity threats.

To adequately assess potential risks, businesses need to know what devices, services, and accounts they use, along with how the business uses data in its operations. Software manufacturers and cybersecurity companies routinely inform customers about vulnerabilities, and important trends are continuously reported in the general media. Many trade associations also provide useful cybersecurity alerts and incident reports, which can make membership worthwhile for smaller enterprises.

Basic vulnerabilities that smaller organizations should consider include using old computers with an outdated operating system that is no longer supported by the manufacturer, or not limiting the software that can be installed by employees.

More complex vulnerabilities relate to technical aspects of specific applications, operating systems, websites’ codes, devices, etc. If a business knows what apps, programs, services, etc., are being used, it can conduct basic online research to identify potential vulnerabilities. If a business encounters highly technical issues that cannot be solved internally, it may consider engaging an IT professional for expert support.

36 https://www.securityweek.com/thousands-3d-printers-exposed-remote-attacks
CONCLUSION

The growing digitalization of business and access to Internet connectivity has significant advantages for small businesses but also carries new operational risks. Small businesses lacking the resources for dedicated IT staff can be left particularly vulnerable. The information presented here provides the first steps to mitigating these risks and to increasing their resiliency to emerging cyber threats.

This guide is designed to raise awareness of the importance of cybersecurity for all businesses, particularly for small businesses with limited resources. This information is designed to help these small businesses take the first steps to building their cybersecurity strategy and to increasing their resilience to growing cybersecurity threats. As small business owners and managers become more informed, they will be better prepared to deal with cyber threats and incidents. We hope this guide makes cyber—and its advantages and dangers—more understandable and that it encourages businesses to look at cyber as an operational risk that must be managed.