Ho Chi Minh City University of Technology
Faculty of Computer Science and Engineering

Assignment
NETWORK SECURITY

Data Security for Small Business

Computer science

Instructor: TS. NGUYỄN ĐỨC THÁI

Authors: Nguyễn Quốc Phú (1914661)
Đinh Thanh Phong (2270243)
Trương Hoàng Phúc (1914720)
Trần Thọ Nhân (1910405)

Tp. Hồ Chí Minh, Nov/2023

Contents

1 Topic introduction

Few small businesses today can function without technology, and most of it involves the public internet. The internet is a great venue for business and offers many benefits; yet, it also presents challenges and dangers that are often difficult for many small business to understand and manage. This assignment was created to provide an overview of cyber security for small businesses and research how to secure business data.Cyber security intrusions are very real and are increasing daily. The number of small businesses becoming victims of cyber crimes is growing rapidly.

This assignment will research on how to implement data security for a small businesses, and we will focus on 4 question:

- What data do an enterprise need to stored?
- What security risks might occur?
- Ways to access business data?
- Data security cost?

This assignment bases on a guideline from University of Southern Maine "Small Business Cyber Security Guide" and combines with actual data on the internet in Vietnam.

We assume that we will implement a data security system for an online shop e.g. a flower shops or an retail shop, then we will set up hardware, software, tools and count the fee for the system.

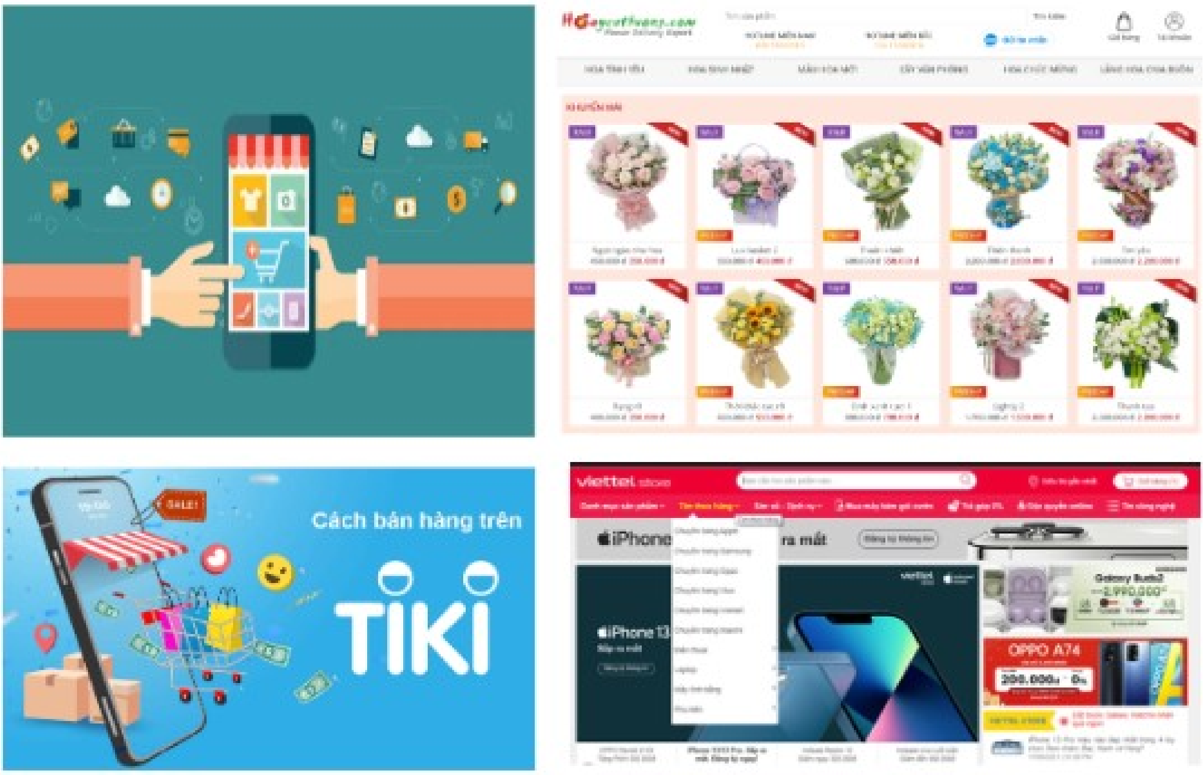


Figure 1: Data Security for Small Business

2 What data do an enterprise need to stored

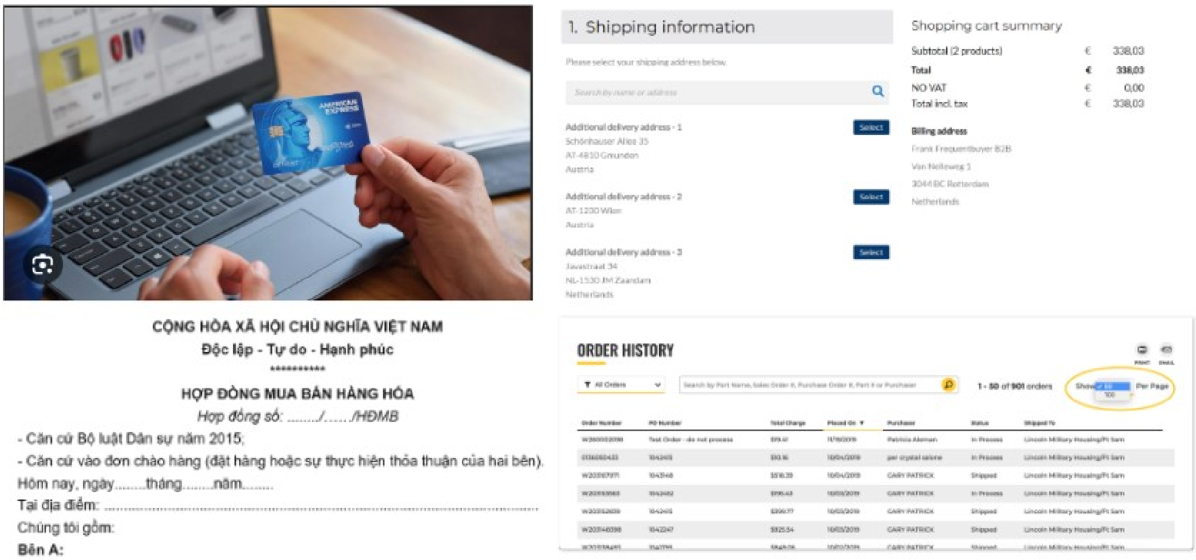
We separate business data into 3 parts, include:

- Business data
- Employee data
- Enterprise core data

2.1 Business data

Business data includes data that relative to transaction and information between our customers and our enterprise.

- Credit card or other financial account numbers.
- Customer information (address and phone number).
- Purchase Order history.
- Vendor and subcontractor agreements and schedules.



1. Shipping information

Please select your shipping address below.

Search by name or address

Additional delivery address - 1
Schönhauser Allee 35
AT-4810 Gmunden
Austria

Additional delivery address - 2
AT-1230 Wien
Austria

Additional delivery address - 3
Javastraat 34
NL-1530 JM Zaandam
Netherlands

Shopping cart summary

Subtotal (2 products)	€	338,03
Total	€	338,03
NO VAT	€	0,00
Total incl. tax	€	338,03

Billing address
Frank Frequentbuyer B2B
Van Nelleweg 1
3044 BC Rotterdam
Netherlands

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
****

HỢP ĐỒNG MUA BÁN HÀNG HÓA
Hợp đồng số: ..../....../HĐMB

- Căn cứ Bộ luật Dân sự năm 2015;
- Căn cứ vào đơn chào hàng (đặt hàng hoặc sự thực hiện thỏa thuận của hai bên).

Hôm nay, ngày........tháng........năm........
Tại địa điểm: ....
Chúng tôi gồm:
Bên A:

ORDER HISTORY

All Orders

Search by Part Name, Sales Order #, Purchase Order #, Part # or Purchaser

1 - 50 of 901 orders

Show 50 Per Page

Order Number	PO Number	Total Charge	Placed On	Purchaser	Status	Shipped To
[illegible]	Test Order - do not process	[illegible]	11/18/2019	Patricia Aleman	In Process	Lincoln Military Housing/Ft Sam
[illegible]	[illegible]	[illegible]	10/04/2019	per crystal salone	In Process	Lincoln Military Housing/Ft Sam
[illegible]	[illegible]	[illegible]	10/04/2019	GARY PATRICK	Shipped	Lincoln Military Housing/Ft Sam
[illegible]	[illegible]	[illegible]	10/03/2019	GARY PATRICK	In Process	Lincoln Military Housing/Ft Sam
[illegible]	[illegible]	[illegible]	10/03/2019	GARY PATRICK	Shipped	Lincoln Military Housing/Ft Sam
[illegible]	[illegible]	[illegible]	10/03/2019	GARY PATRICK	Shipped	Lincoln Military Housing/Ft Sam
[illegible]	[illegible]	[illegible]	[illegible]	GARY PATRICK	Shipped	Lincoln Military Housing/Ft Sam

Figure 2: Business data

2.2 Employee data

Employee data includes data that relative to employee private information.

- Social Security numbers (SSNs).
- Personally identifiable information pertaining to individuals (employees, applicants,parental/familial relatives).
- Employee schedules and vacation times.
- Medical and health data.

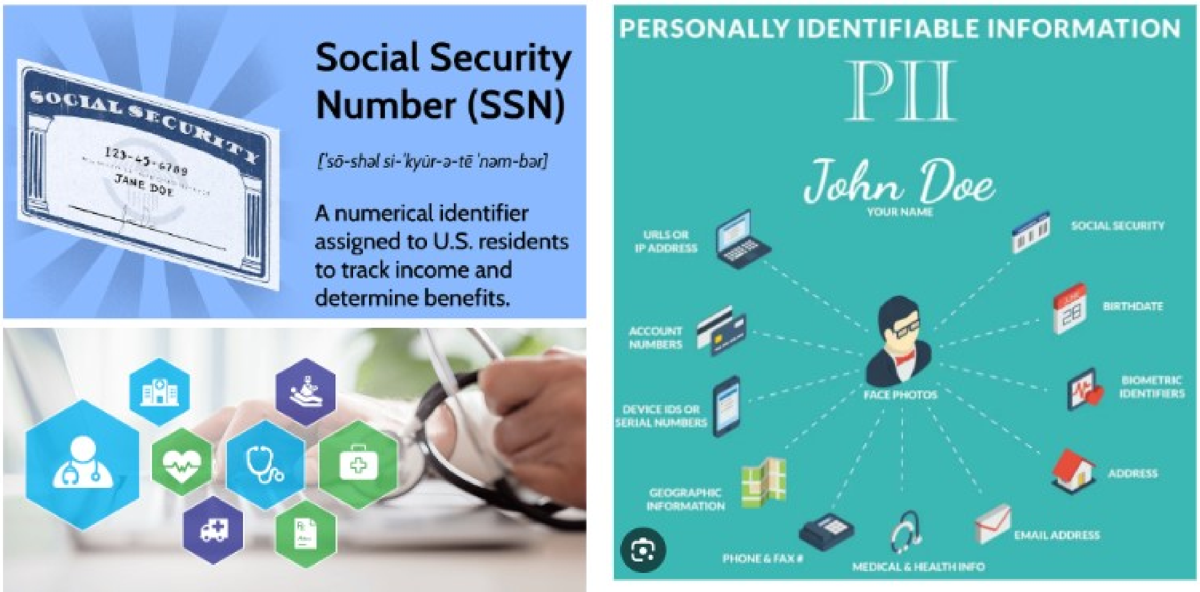


Figure 3: Employee data

2.3 Enterprise core data

Enterprise core data includes data that is very important and highly security and privacy to the enterprise.

- Proprietary and/or copyrighted data, such as research data and publications.
- Financial data.
- Confidential legal.
- Backup data.

Figure 4: Enterprise core data

2.4 Summary data needs to be secured

Summary data needs to be secured includes:

1. Credit card or other financial account numbers.
2. Customer information (address and phone number).
3. Purchase Order history.
4. Vendor and subcontractor agreements and schedules.
5. Social Security numbers (SSNs).
6. Personally identifiable information pertaining to individuals (employees, applicants,parental/familial relatives).
7. Employee schedules and vacation times.
8. Medical and health data.
9. Proprietary and/or copyrighted data, such as research data and publications.
10. Financial data.
11. Confidential legal.
12. Backup data.

3 What security risks might occur

Small businesses play a pivotal role in the global economy, contributing to economic growth and job creation. However, they are increasingly vulnerable to a wide range of security risks in the digital age. The evolving threat landscape demands a comprehensive understanding of these risks and proactive measures to mitigate them. This report aims to shed light on the security challenges small businesses face, their potential consequences, and strategies to address them.

3.1 Data Loss

Data is the lifeblood of any business, and small enterprises are no exception. Data loss can occur due to various reasons:

- **Hardware Failures:** Hard drives and storage devices can fail, leading to data loss.
- **Human Error:** Employees may accidentally delete or overwrite critical data.
- **Cyberattacks:** Ransomware and other malware can encrypt or destroy data.

Consequences of data loss may include:

- Financial Setbacks
- Reputation Damage
- Legal Repercussions

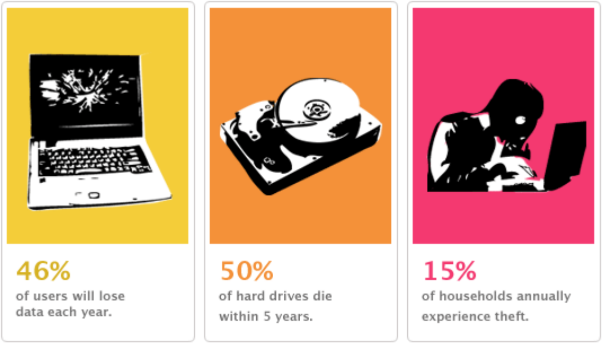

46%
of users will lose data each year.
50%
of hard drives die within 5 years.
15%
of households annually experience theft.

Figure 5: Data lost

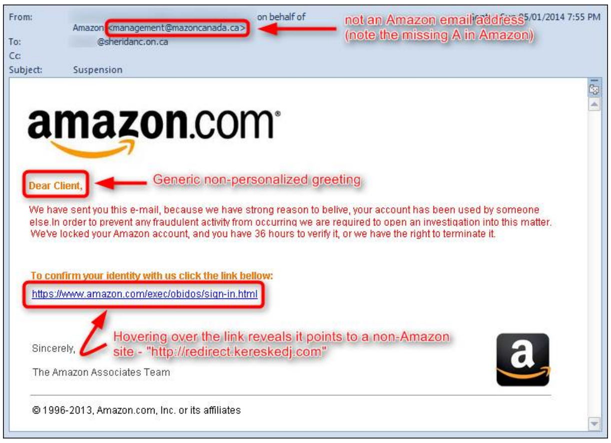
Small businesses can mitigate this risk by implementing:

- **Regular Data Backups:** Frequent and automated backups are crucial.
- **Data Recovery Solutions:** Implement data recovery software or services.
- **Security Best Practices:** Train employees on data protection and cybersecurity best practices.

3.2 Phishing Attacks

Phishing attacks are a prevalent form of cyber threat. Attackers use deceptive emails, websites, or messages to trick employees into disclosing sensitive information, such as login credentials or financial data.
Potential consequences include:

- Data Breaches
- Financial Losses
- Compromised Reputation



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>
To: [redacted]@sheridanc.on.ca
Cc:
Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

05/01/2014 7:55 PM

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:
https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

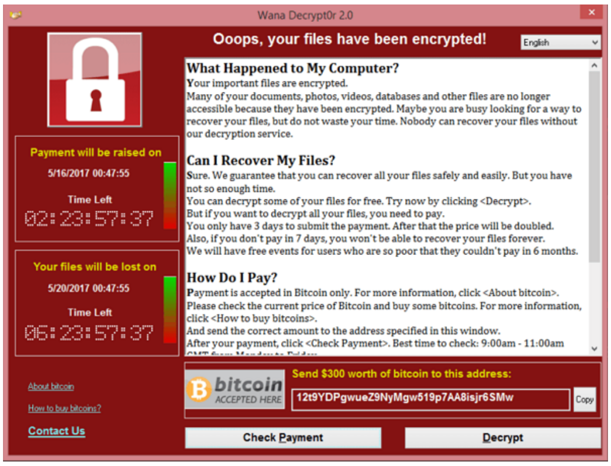
Figure 6: Phishing Email

To prevent phishing attacks, businesses should focus on:

- **Employee Education:** Regularly train employees to recognize and report phishing attempts
- **Email Filtering:** Implement robust email filtering and antivirus solutions.
- **Multi-Factor Authentication (MFA):** Require MFA for accessing critical systems and accounts.

3.3 Ransomware

Ransomware is a type of malware that encrypts a business's data and demands a ransom for its release. Falling victim to ransomware can disrupt operations, lead to financial losses, and potentially result in data exposure.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Figure 7: Ransomware

To prevent ransomware attacks, consider:

- **Regular Software Updates:** Keep operating systems and software up to date.
- **Cybersecurity Measures:** Invest in firewalls, intrusion detection systems, and endpoint protection.
- **Employee Training:** Educate employees on recognizing and responding to suspicious activities.

3.4 Information Disclosure

Information disclosure occurs when sensitive business data is unintentionally exposed, whether through misconfigured security settings, inadequate data protection, or employee errors.
Potential consequences include:

- Breaches of Customer Trust
- Legal Consequences
- Financial Repercussions

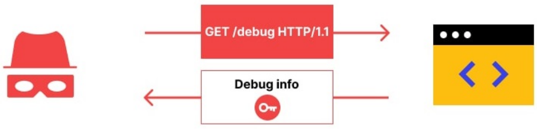


Figure 8: Disclosure Server debug data

To mitigate information disclosure, businesses should consider:

- **Data Access Controls:** Restrict access to sensitive data on a need-to-know basis.
- **Data Encryption:** Encrypt sensitive data to protect it from unauthorized access.
- **Employee Training:** Educate employees on data handling best practices.

3.5 Unsecured Wi-Fi Networks

Small businesses often rely on Wi-Fi networks, but using unsecured connections can put them at risk. Attackers can intercept data transmissions and gain unauthorized access to sensitive information.

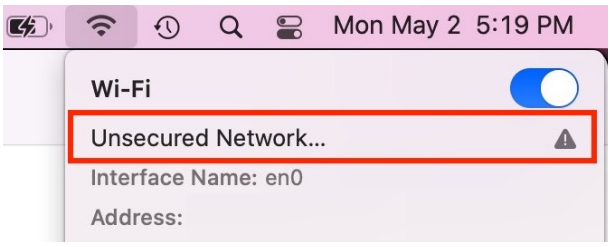


Figure 9: Unsecured Wi-Fi Networks

To secure Wi-Fi networks, businesses should:

- **Use Strong Encryption:** Implement WPA3 or WPA2 encryption protocols.
- **Enforce Secure Passwords:** Use complex, unique passwords for Wi-Fi access.
- **Regular Network Monitoring:** Monitor network traffic for suspicious activities.

3.6 Employee Negligence

Employees can inadvertently introduce security risks through careless actions, such as leaving sensitive documents unattended or sharing login credentials.

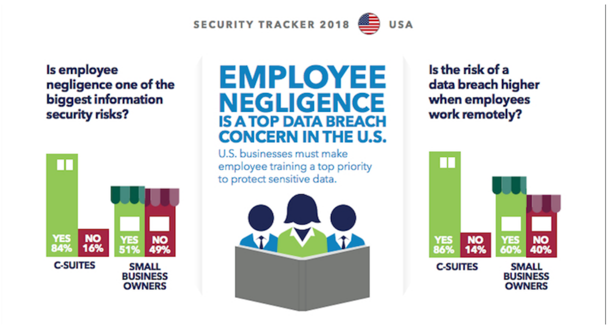


Figure 10: Employee Negligence

To minimize the impact of employee negligence:

- **Training and Awareness:** Provide cybersecurity training to educate employees about best practices.
- **Security Policies:** Establish and enforce security policies that clearly define acceptable behaviors.
- **Monitoring Employee Behavior:** Use technology and monitoring tools to track and address risky behavior.

3.7 Insider Threats

Insider threats involve malicious actions by employees, contractors, or business partners with access to an organization's systems and data. These threats can lead to data breaches, fraud, and significant damage to a company's reputation.

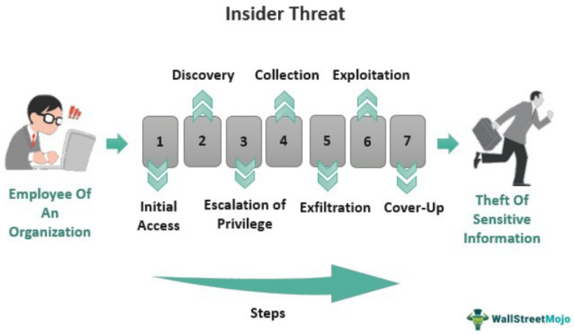


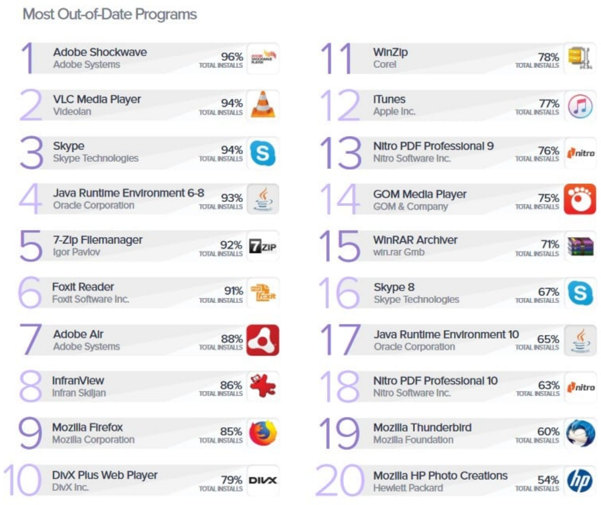
Figure 11: Insider Threats

To address insider threats:

- **Access Controls:** Implement role-based access controls to restrict access to sensitive data.
- **Monitoring User Activities:** Regularly review logs and monitor employee activities.
- **Incident Response Protocols:** Develop clear incident response protocols to address insider threats promptly.

3.8 Outdated Software

Using outdated software and hardware increases vulnerabilities to known security threats. Small businesses must regularly update and patch their software and hardware to protect against exploits.



Most Out-of-Date Programs

1	Adobe Shockwave Adobe Systems	96% TOTAL INSTALLS
2	VLC Media Player Videolan	94% TOTAL INSTALLS
3	Skype Skype Technologies	94% TOTAL INSTALLS
4	Java Runtime Environment 6-8 Oracle Corporation	93% TOTAL INSTALLS
5	7-Zip Filemanager Igor Pavlov	92% TOTAL INSTALLS
6	Foxit Reader Foxit Software Inc.	91% TOTAL INSTALLS
7	Adobe Air Adobe Systems	88% TOTAL INSTALLS
8	InfranView Infran Skiljan	86% TOTAL INSTALLS
9	Mozilla Firefox Mozilla Corporation	85% TOTAL INSTALLS
10	DivX Plus Web Player DivX Inc.	79% TOTAL INSTALLS
11	WinZip Corel	78% TOTAL INSTALLS
12	iTunes Apple Inc.	77% TOTAL INSTALLS
13	Nitro PDF Professional 9 Nitro Software Inc.	76% TOTAL INSTALLS
14	GOM Media Player GOM & Company	75% TOTAL INSTALLS
15	WinRAR Archiver win.rar Gmb	71% TOTAL INSTALLS
16	Skype 8 Skype Technologies	67% TOTAL INSTALLS
17	Java Runtime Environment 10 Oracle Corporation	65% TOTAL INSTALLS
18	Nitro PDF Professional 10 Nitro Software Inc.	63% TOTAL INSTALLS
19	Mozilla Thunderbird Mozilla Foundation	60% TOTAL INSTALLS
20	Mozilla HP Photo Creations Hewlett Packard	54% TOTAL INSTALLS

Figure 12: Most out-of-date programs

To prevent vulnerabilities from outdated software:

- **Comprehensive Software Management:** Develop a software management strategy that includes regular updates and patches.

- **Vulnerability Assessments:** Periodically conduct vulnerability assessments to identify and remediate weaknesses in software and hardware.

3.9 Vendor and Supply Chain Risks

Small businesses often rely on third-party vendors and supply chain partners. These relationships can introduce security risks if not adequately vetted.

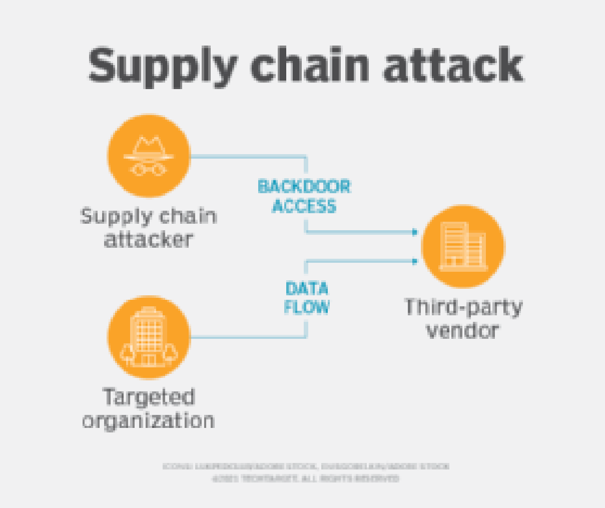


Figure 13: Supply Chain attack

To mitigate vendor and supply chain risks:

- **Vendor Security Assessment:** Assess the security practices of vendors and partners.

- **Contractual Agreements:** Include security requirements and provisions in contracts.

- **Communication Channels:** Establish communication channels to address security concerns and incidents promptly.

3.10 DDoS (Distributed Denial of Service) Attacks

DDoS attacks overwhelm a business's online services with traffic, causing them to become unavailable. This can lead to lost revenue and damage to a company's reputation.

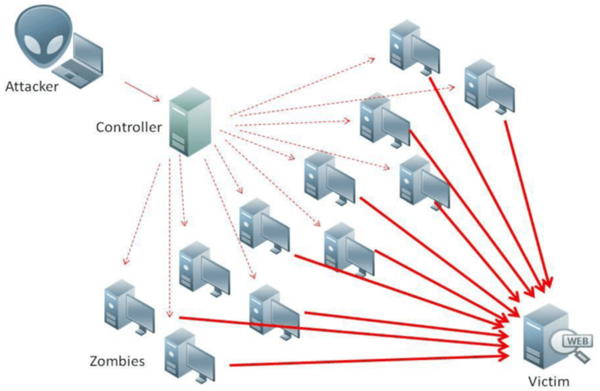


Figure 14: Distributed Denial of Service

To minimize the impact of DDoS attacks:

- **DDoS Mitigation Tools and Services:** Invest in DDoS mitigation solutions to filter malicious traffic.
- **Incident Response Plan:** Develop an incident response plan that outlines steps to take during a DDoS attack, including communication and recovery procedures.

Small businesses must be proactive in addressing security risks to ensure the continuity of their operations and protect sensitive data. By understanding the various security risks they face and implementing appropriate mitigation strategies, these enterprises can better safeguard their assets and thrive in the digital age.

4 Secure business data

4.1 Classify Data

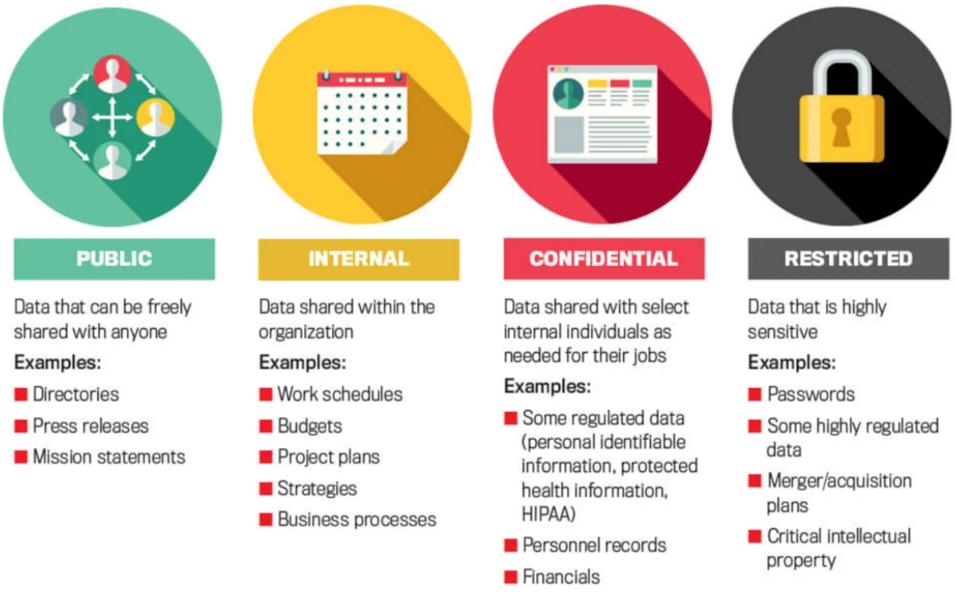
Depending on the sensitivity of the data held by an organization, there is a need for various levels of classification. These classifications determine several aspects, including who is granted access to the data and how long the data should be retained. Typically, there are four data classifications: public, internal-only, confidential, and restricted. Let's examine examples for each of these.

- Level 1 - Public data: This category of data is openly accessible to the public, which means it can be accessed by all employees and company personnel. It can be freely used, reused, and shared without any consequences. Examples of public data include first and last names, job descriptions, and press releases

- Level 2 - Internal-only data: This type of data is restricted to internal company personnel or employees with specific access permissions. It may encompass internal memos, business plans, and other internal communications.

- Level 3 - Confidential data: Access to confidential data necessitates specific authorization and/or clearance. Examples of confidential data include Social Security numbers, cardholder data, and more. Confidential data is typically protected by regulations such as HIPAA and the PCI DSS.

- Level 4 - Restricted data: Restricted data includes information that, if compromised or accessed without authorization, could result in criminal charges, substantial legal fines, or irreparable harm to the company. Examples of restricted data encompass proprietary information, research data, and data protected by state and federal regulations.



PUBLIC

Data that can be freely shared with anyone

Examples:

- Directories
- Press releases
- Mission statements

INTERNAL

Data shared within the organization

Examples:

- Work schedules
- Budgets
- Project plans
- Strategies
- Business processes

CONFIDENTIAL

Data shared with select internal individuals as needed for their jobs

Examples:

- Some regulated data (personal identifiable information, protected health information, HIPAA)
- Personnel records
- Financials

RESTRICTED

Data that is highly sensitive

Examples:

- Passwords
- Some highly regulated data
- Merger/acquisition plans
- Critical intellectual property

Figure 15: Classify Data

4.2 Secure Non-public data

Following the classification of data into four categories based on their security requirements, the next phase involves the establishment of protocols to ensure data security within each category. In this section, we will delve into the guidelines and measures necessary to safeguard data according to its classification, ensuring that sensitive information remains protected within storage infrastructure.

4.2.1 Level 2 - Internal-only data

1. **Log Retention:** All connections and actions to non-public data must be logged. This practice ensures the maintenance of a comprehensive audit trail for tracking and monitoring data access and operations.

2. **Malware Detection and Endpoint Detection and Response:** To enhance data security, all servers must be equipped with robust malware detection and endpoint detection and response software. These software solutions should operate with up-to-date signature files to effectively identify and counteract potential threats.

3. **Current Patches:** To maintain the robustness of our data storage systems, it is essential that both operating systems and application software receive regular updates and patches. These updates should be sourced from reputable vendors or Open Source projects and must be installed in a timely manner to mitigate vulnerabilities.

4. **Password Management:** Secure password management is fundamental to data security. Mechanisms for users to set or change passwords must be designed securely. Systems responsible for managing passwords should be configured securely. Furthermore, it is imperative that systems managing user passwords and other access credentials are designed to prevent unauthorized retrieval of these sensitive data elements.

5. **Appropriate User Access:** Granting access to servers and applications should be based on a well-defined and regularly reviewed business need. Users must only be permitted to access a server or application once their current business requirement for access has been explicitly established.

6. **Server Communication:** Securing communication between servers or applications and client machines is of paramount importance. Data in transit should be encrypted to safeguard it from potential eavesdropping and tampering, ensuring data confidentiality and integrity during transmission.

4.2.2 Level 3 - Confidential data

1. Satisfy all the requirements at previous levels

2. **Secure Disposal:** Information designated as level 3 and upper must be properly disposed of by securely overwriting the information or physically destroying the media when it is no longer needed.

3. **Reporting Breaches:** Server and application operators must promptly inform the appropriate escalation contacts of any possible breaches, ensuring swift response to potential security incidents.

4. **Reviewing Logs:** Periodic reviews of logs are necessary to identify anomalous behavior. Additionally, administrative functions on servers and applications must be logged to maintain accountability and transparency.

5. **Improper Access Protection:** Servers must be safeguarded from improper network-based access, minimizing the risk of unauthorized intrusion.

6. **Idle Sessions:** Implementing a mechanism to force re-authentication to user accounts after an idle period enhances security by reducing the risk of unauthorized access during idle sessions.

7. **Password Guessing Prevention:** Servers or applications must incorporate mechanisms that inhibit password-guessing attacks on user accounts if the server or application handles its own authentication. This precautionary measure helps protect against unauthorized access attempts.

4.2.3 Level 4 - Restricted data

1. Satisfy all the requirements at previous levels

2. **Encryption at Rest:** All Level 4 data must be encrypted to ensure the security of data at rest.

3. **Outbound Traffic:** Outbound traffic from servers must be limited to what is necessary for the proper operation of the service. This restriction reduces the exposure of servers to external threats.

4. **Server Vulnerability:** Server operators must regularly take reasonable actions to ensure that their systems are not vulnerable to attacks, fortifying the security of our infrastructure.

5. **Private Address Space:** Servers handling Level 4 information must be on a private address space to minimize exposure to external networks.

6. **External Access:** Servers must not be directly accessible from the Internet or from parts of the internal network where user computers are located. This control limits the attack surface and enhances security.

4.3 Handling Non-public data

In addition to establishing data storage standards, it is equally important to outline regulations for employees responsible for handling data.

4.3.1 General safeguards for all non-public data

- **Limit subjects, time, and location of data access:** Restrict access to sensitive data by specifying who can access it, when they can access it, and where they can access it. This control helps minimize the risk of unauthorized exposure.

- **Share only with those authorized to have access:** Ensure that sensitive data is shared only with individuals who have explicit authorization to access it. This practice prevents unauthorized personnel from viewing or using the data.

- **Use caution when discussing in public places:** When discussing sensitive data, exercise caution in public areas to prevent inadvertent exposure or eavesdropping. Confidential information should be handled discreetly.

- **Secure paper-based information in a locked desk/office/cabinet when not in use:** Physical documents containing sensitive data should be securely stored in a locked desk, office, or cabinet when they are not actively being used. This measure prevents unauthorized access to printed materials.

- **Report possible or actual loss immediately to your supervisor or Security Officer:** In case of a suspected or confirmed data loss or breach, employees should promptly report the incident to their supervisor or the designated Security Officer. Swift reporting is crucial for timely mitigation and response.

- **Never share passwords/PINs with anyone or carry them with the device they unlock:** Passwords or Personal Identification Numbers (PINs) must never be shared with others. Additionally, they should not be stored or carried together with the devices they are meant to secure. This practice helps prevent unauthorized access to devices and associated data.

4.3.2 Printing

- **L2:** Do not leave unattended on copiers/printers. When printing Level 2 data, ensure that the printed documents are not left unattended on copiers or printers. This practice prevents unauthorized access to the printed information.

- **L3:** Do not leave unattended on copiers/printers. Similarly, for Level 3 data, it is crucial not to leave printed documents unattended on copiers or printers. This precaution helps maintain the security of sensitive information.

- **L4:** Use badge retrieval for print jobs on an approved Level 4 printer. For Level 4 data, a higher level of security is required. Use a badge retrieval system to collect print jobs from an approved Level 4 printer. This additional measure ensures that only authorized personnel can access and retrieve printed materials, enhancing the protection of the most sensitive data.

4.3.3 Mailing Paper-Based Info

- **L2:** Put Level 2 information in a closed mailing envelope or box and send it via Interoffice mail. When dealing with Level 2 data, ensure that paper-based information is securely placed in a closed mailing envelope or box. Use the Interoffice mail system for the delivery.

- **L3:** Place Level 3 data in a sealed envelope or box and use Interoffice mail for sending. For Level 3 data, maintain security by using a sealed envelope or box and rely on the Interoffice mail system for distribution.

- **L4:** For Level 4 data, enhance security measures. Put the data in a sealed envelope or box and send it via FedEx, UPS, or USPS mail services, preferably with tracking and delivery confirmation when feasible. This added level of protection ensures the safe and traceable transit of highly sensitive information.

4.3.4 Storing Electronic Files on Work or Personal Computer

- **L2:** When storing Level 2 data on a computer, ensure that the computer meets security requirements, including a device password, anti-virus software, current patches, encryption, and remote wiping capabilities.

- **L3:** For Level 3 data, the computer should also meet security requirements, such as having a device password, anti-virus software, current patches, encryption, and remote wiping capabilities.

- **L4:** Never copy or store Level 4 data on your work or personal computer. This data should remain within the secure managed system or be stored on encrypted external storage media to maintain the highest level of security.

4.3.5 Storing Files on External Portable Storage Media

- **L2:** Storing files on external portable storage media is permitted for Level 2 data.
- **L3:** For Level 3 data, external storage media such as USB sticks, CDs/DVDs, backup tapes, etc., must be encrypted and password protected to enhance data security.
- **L4:** Similar to Level 3, Level 4 data on external storage media must also be encrypted and password protected to provide an additional layer of protection for the most sensitive information.

4.3.6 Sending Data/Files to Authorized Individuals

- **L2:** Sending data/files to authorized individuals is allowed for Level 2 data.
- **L3:** For Level 3 data, it's crucial to encrypt data when transmitting it, both internally and externally. Use a Secure File Transfer method such as OneDrive or Accellion. When using website forms, ensure the use of HTTPS for secure data transmission.
- **L4:** For Level 4 data, encryption is imperative when transmitting data, both internally and externally. Use a Secure File Transfer method like OneDrive or Accellion, and ensure the use of HTTPS for website forms. This provides an added layer of security to protect highly sensitive information.

4.3.7 Engaging Vendors to Store/Process Data

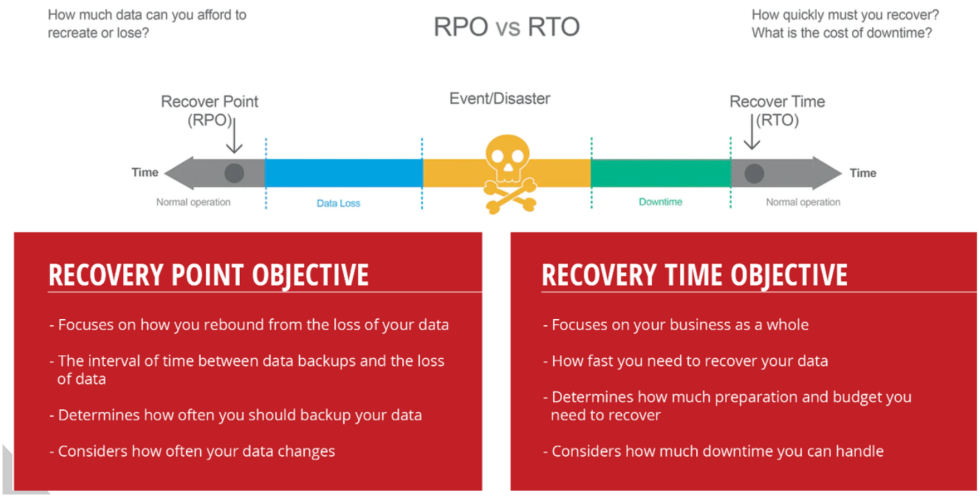
- **L2:** For vendors and other third parties handling non-sensitive, non-public university data, it is strongly recommended to have written contracts in place.
- **L3:** Ensure that vendor/hosting agreements include appropriate security requirements when dealing with Level 3 data. Security considerations are essential for maintaining the integrity and confidentiality of data.
- **L4:** For Level 4 data, engage the university's Information Security team for a vendor risk assessment. Additionally, include a Data Protection rider in the vendor/hosting agreement to ensure the highest level of data security.

4.3.8 Deleting Data

- **L2:** For Level 2 data, use the standard delete function and empty the trash bin to remove data.
- **L3:** Similarly, for Level 3 data, use the standard delete function and empty the trash bin to erase data securely.
- **L4:** When dealing with Level 4 data, use a secure overwrite or removal tool, such as Spirion or Identity Finder, to ensure data is irrecoverable, adding an extra layer of protection.

5 Backup business data

In addition to data storage protection, data backup is equally essential. Backup ensures that critical information remains safe from loss due to technical issues, user errors, or unexpected incidents. Maintaining backup copies is a crucial part of data protection and recovery strategy. The backup process needs to be established and executed regularly to ensure readiness and effective data recovery. It is through data backup that organizations can maintain operations without significant disruption in the event of an incident.



RECOVERY POINT OBJECTIVE

- Focuses on how you rebound from the loss of your data
- The interval of time between data backups and the loss of data
- Determines how often you should backup your data
- Considers how often your data changes

RECOVERY TIME OBJECTIVE

- Focuses on your business as a whole
- How fast you need to recover your data
- Determines how much preparation and budget you need to recover
- Considers how much downtime you can handle

Figure 16: RPO vs RTO

In the process of developing an effective data backup strategy, two crucial factors that demand attention are Recovery Point Objective (RPO) and Recovery Time Objective (RTO). These are two essential metrics that shape how data is backed up and restored to align with an organization's goals.
Recovery Point Objective (RPO):
RPO defines the point in time to which data must be backed up to ensure that, in the event of a disaster, the organization can restore data to that specific point without violating business requirements and compliance.
Recovery Point Objective (RPO):
RTO is a critical element in disaster recovery planning and backup strategies. It defines the maximum allowable downtime or the time needed to restore normal operations after a disaster or system failure. RTO is closely related to data backup as it measures the time required to recover data and systems from backups to resume business functions.

Based on the level of requirements for the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), we can choose from a range of strategies to build a suitable data backup and recovery system. Below are some commonly used strategies:

- **Backup and Restore:** This strategy involves regular data backups and restoring them as needed. Data is typically stored on backup media like hard drives or tapes.
  - **Advantages:**
    - Suitable for less critical data that doesn't require quick recovery.
    - Lower cost and easy to implement.
  - **Disadvantages:**
    - RPO and RTO may be relatively high for critical data.

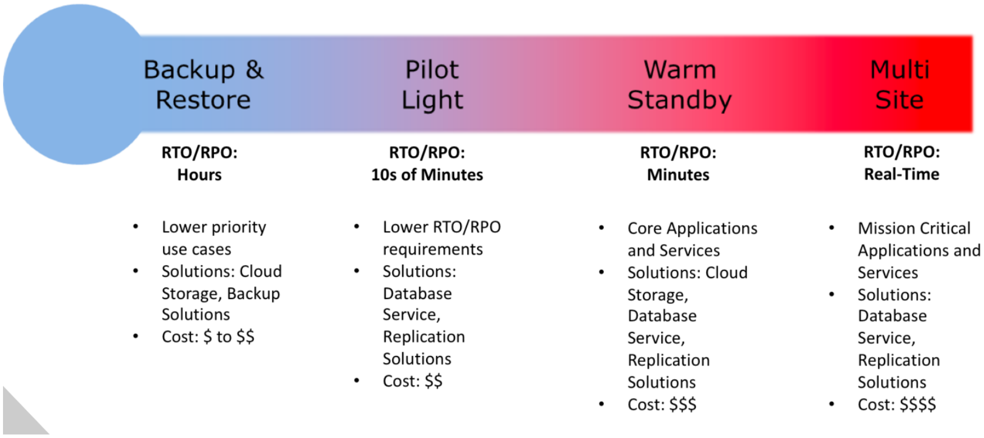

Backup & Restore
Pilot Light
Warm Standby
Multi Site
RTO/RPO: Hours
RTO/RPO: 10s of Minutes
RTO/RPO: Minutes
RTO/RPO: Real-Time
• Lower priority use cases
• Solutions: Cloud Storage, Backup Solutions
• Cost: $ to $$
• Lower RTO/RPO requirements
• Solutions: Database Service, Replication Solutions
• Cost: $$
• Core Applications and Services
• Solutions: Cloud Storage, Database Service, Replication Solutions
• Cost: $$$
• Mission Critical Applications and Services
• Solutions: Database Service, Replication Solutions
• Cost: $$$$

Figure 17: Backup strategy

        - Data may be lost if a failure occurs before the next backup.
    - **Suitable for:** Less critical data or backup purposes, such as non-critical documents.

- **Pilot Light:** The Pilot Light model maintains a near-operational recovery environment that can be activated when needed.
    - **Advantages:**
        - Low RTO, minimizing downtime.
        - Flexible and can scale quickly.
    - **Disadvantages:**
        - Significant resource and operational costs.
        - Requires continuous management and maintenance.
    - **Suitable for:** Critical data requiring fast recovery, such as online applications.

- **Warm Standby:** Warm Standby keeps a partially operational recovery environment ready but may require additional resource activation for full operation.
    - **Advantages:**
        - Low RPO, reducing data loss.
        - Lower RTO compared to Backup and Restore.
    - **Disadvantages:**
        - Significant resource and operational costs.
        - Requires continuous management and maintenance.
    - **Suitable for:** Critical data requiring fast recovery and readiness.

- **Multi-Site:** The Multi-Site model sets up multiple backup points at different physical locations to ensure data safety and readiness.
    - **Advantages:**
        - Almost zero data loss (near-zero RPO) due to distributed redundancy.
        - High reliability with automatic failover capabilities.
    - **Disadvantages:**
        - High costs for building and maintaining multi-site infrastructure.
        - Requires complex management and security.

- **Suitable for:** Highly critical data demanding absolute reliability and readiness, such as in banking or healthcare.

6 Data security cost

Business security system costs can be divided into two general categories: physical and cybersecurity.

6.1 Physical security

Hardware:

Business security hardware is usually the most expensive part of the solution, costing $1,000 to $2,500. However, these costs represent only one business location. If you open new locations or already have multiple locations, costs will be higher.

Installation and activation:

Your hardware will be installed and activated by fitters employed by your hardware supplier. You'll likely pay $300 to $500 for this service.

Business monitoring:

It costs between $40 and $120 per month to monitor individual security devices, like alarms and cameras. Landline monitoring prices are often around $10 less per month than cellular monitoring.

Access Control:

In the business environment, access control is smart lock functionality paired with monitoring capabilities. Businesses manage and monitor who comes through the door, providing individual-based access authority both internally within the building, as well as at the exterior entrance.
The components needed for this type of setup include mobile, passes, tags or fobs, wall or card readers, access control keypads, door lock hardware, and control panels. These are typically priced per system component needed, starting at a minimum of $1,500 for the hardware.

6.2 Cybersecurity

When it comes to cybersecurity costs, there is no one-size-fits-all. That's because there are so many different variables and factors involved when it comes to determining cybersecurity costs, including your industry, company size, compliance and regulatory requirements affecting your business, current IT tools, the complexity of your IT infrastructure, and the sensitivity of the data you collect, use and share.
On average, companies spend around 10% of their annual IT budget on cybersecurity and about $2,700 on average per full-time employee. So, if your business has an IT budget of $3 million, you'll likely spend $300,000 on cybersecurity costs. Ultimately, your cybersecurity costs will depend on the type of cybersecurity services and solutions you need.
Here are some of the most common cybersecurity services and how much they cost:

- **Endpoint detection and response (EDR):** Every endpoint—from laptops to mobile phones and tablets—in your organization represents a potential entry point for a hacker to infiltrate your systems. That's why endpoint management is a crucial part of cybersecurity. By monitoring your endpoints, EDR solutions can detect abnormal behavior, stop it and investigate whether something malicious (or accidental but dangerous) is happening.

Endpoint detection and response services typically cost \$5 – \$8 per user per month and \$9 – \$18 per server per month.

- **Vulnerability assessment:** A comprehensive vulnerability assessment helps to identify, quantify and address the security vulnerabilities that exist within your company's infrastructure, including on-premise and cloud networks. Remediation measures can then be applied accordingly. Identifying risks before hackers do will drastically improve the cyber security posture of your business. You can expect to pay \$1,500 – \$6,000 for a vulnerability assessment of a network with 1-3 servers and \$5,000 – \$10,000 for a network with 5-8 servers.

- **Firewall:** Firewalls act as the first line of defense between your network and the outside world. Without it, malicious traffic would be allowed directly into your network. Firewalls come in various sizes, so you will want to choose one that best fits your network's size and configuration. On average, you can expect to pay \$400 on the low end and up to \$6,000 on the high-end.

- **Two-Factor Authentication:** 2FA adds an extra layer of defense between your data and criminals. The strongest password is no match for a password that has been phished or stolen by a key logger, but with two-factor authentication, an attacker cannot log in without also having access to the additional authentication methods specified within the user's profile, such as push notification to their mobile device, text or phone call. The cost for two-factor authentication usually ranges between \$5 – \$10 per user per month.

- **Web application assessment:** As cyber-attacks increasingly focus on application-layer disruptions, the importance of application security has never been more vital. You can use web application assessment to test your web application to identify security vulnerabilities, understand how users and attackers could abuse or misuse your web application and verify whether required security controls are implemented. The cost of a web application assessment will depend on the time it takes an engineer to perform an assessment, but on average, you can expect to pay around \$4,000. If your web application has multiple roles to test and a significant number of unique pages/forms, that takes longer for an engineer to adequately test and might cost closer to \$8,000.

- **Email security:** More than 90% of targeted cyberattacks are initiated by email. Attackers often use deceptive messages to persuade victims to provide sensitive information, open attachments, or click links that allow them to install malware on their devices. Email security can prevent businesses from falling victim to ransomware, spyware, trojans, social engineering, and other malware threats. Email security costs will fluctuate depending on the number of employees and endpoints (computers) that need security. Generally, businesses should expect to pay between \$3 – \$6 per user per month for an email protection service with the necessary advanced features to protect you. For example, if your company has 250 employees, you should pay an average of \$1,125 per month for email protection services.

Besides, training employees on cybersecurity knowledge also costs a relatively large amount of money.

References

[1] Cyber Security Planning Guide https://www.fcc.gov/sites/default/files/cyberplanner.pdf

[2] Small Business Cyber Security Guide https://www1.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf