CSEC.603.01 - Enterprise Security

Organizational Cybersecurity Evaluation

Final Report

Shubham Verma(sv4168)

Table of Contents

Part 1- Large Enterprise Criteria Report

1.1 Executive Summary

Understanding the many business types that are available requires a thorough understanding of business classification. It enables us to comprehend business breadth, scale, and traits better across various categories. Businesses are categorized in this context based on their total assets, total income, and total staff count. For a more thorough explanation, read on:

Small businesses are those that have fewer than 50 employees, less than $10 million in annual revenue, and fewer than $5 million in total assets. Small firms typically serve local markets, which are frequently owned and run by people or families. They are also distinguished by a high degree of adaptability and flexibility, enabling them to react swiftly to market developments.

Medium-sized companies fall into this group if they have between 50 and 249 employees, a total annual revenue of between $10 million and $50 million, and total assets of under $20 million. Larger than small enterprises and with a more well-defined organizational hierarchy are medium-sized businesses. They could cover a larger geographic area or have several locations. Additionally, medium-sized businesses might have more specialized divisions and roles like marketing, finance, and operations.

Large Business: Companies in this category have more than 250 employees, more than $50 million in annual revenue, and more than $20 million in assets. Large enterprises, which have many levels of administration and a wide range of goods and services, are the biggest and most complex types of businesses. These businesses also operator in multiple geographical locations.

1.2 Introduction and Classification Factors

Small, medium, and large enterprises are usually categorized based on a variety of factors. Depending on the classification's business, location, and source, different specific factors might be employed. However, the following are some typical elements used to classify businesses:

Number Of Employees:

The number of employees is an element that is frequently used to classify businesses. Small businesses usually employ fewer than 50 people, medium-sized businesses employ between 50 and 250 people, and big businesses employ more than 250 people.

The sources I have used to classify using this factor are:

1. **European Union (EU)*[1]***: The EU categorizes businesses as either SMEs or large businesses based on the sum of their balance sheet total and yearly revenue. A microbusiness is defined by the EU as having fewer than 10, a small business as having between 10 and 49 workers, and a medium-sized business as having between 50 and 249 employees. And large businesses or large enterprise employee more than 249 employees.

2. **Organization for Economic Co-operation and Development (OECD)*[2]***: The OECD offers standards for classifying companies according to the amount of employees. A small business usually employs fewer than 50 people, while a medium-sized business employs between 50 and 249 people, according to the OECD. And for large enterprises this number is more than 249 for the number of employees.

3. **The International Finance Corporation (IFC)*[3]*:** The IFC is a part of the World Bank Group and concentrates on the growth of the private sector in developing nations. The IFC bases its definition of SMEs on a combination of yearly revenue and employee count. A medium-sized company has between 50 and 300 employees, while a small enterprise has

fewer than 50 employees, and large according to the IFC. Considering case of large enterprises, the number of employees will be greater than 300.

Thus, considering all the three sources we can see that they all agree upon on factor of number of employees for small or medium sized business, which is less than 50, for small or medium enterprise the value is between 50 to 250, and for large business the value is greater than 250.

Revenue of the company:

Because it gives a good sign of the company's size and financial strength, revenue is frequently taken into account when categorizing businesses into SMBs, SMEs, and large enterprises. Revenue is the entire sum of money that a business makes from the sale of its goods or services over a given time frame, typically a year. It is a crucial metric for assessing a company's financial success and is frequently used to classify businesses according to size.

I have used the following sources for the classification data used:

1. **Deloitte *[4]***:The fastest-growing technology firms in a particular nation or region are ranked annually in the Deloitte Fast 50 list. Rankings are determined by revenue increase over the previous four years. A small business, defined by Deloitte as having revenue of less than €10 million, a medium-sized business, defined as having revenue of between €10 million and €50 million, and a big business, defined as having revenue of more than €50 million.

2. **European Union (EU)*[5]*:** The EU offers recommendations for classifying companies according to income. A small business, according to the EU, is defined as having annual revenues of less than €10 million, a medium-sized business, as defined by the EU, as having annual revenues between €10 million and €50 million, and a large business, as defined by the EU, as having annual revenues of more than €50 million.

3. **International Finance Corporation (IFC)*[6]*:** The IFC is an organization that belongs to the World Bank Group and concentrates on the growth of the private sector in developing nations. The number of employees and annual revenue are combined to define SMEs by the IFC. A medium-sized company has annual revenue of up to $15 million, according to the IFC, while a small enterprise has fewer than 50 employees and annual revenue of up to $3 million. Considering large enterprises, they will have revenue greater than $15 million.

Here considering sources Deloitte Fast and European Union, we can see that they provide the same number for classifying small or medium sized business, small or medium enterprise and large enterprise. But for International Finance Corporation (IFC), the numbers change due to various factors, including various business contexts, various economic conditions, and various regulatory environments, each company may use different criteria. For instance, the IFC, a member of the World Bank Group, concentrates on developing nations and emerging markets, and these contexts are considered when determining how small, medium, and large enterprises should be classified.

Similar to this, the EU has its own classification standards for small and medium-sized businesses, which are based on the number of workers and the yearly turnover or balance sheet total of the business. In order to assist small and medium-sized businesses in the EU, these standards have been specifically developed.

On the other hand, Deloitte Fast offers a ranking of the fastest-growing technology firms based on their rate of revenue development over the previous four years. Thus, it aims to identify and rank high-growth businesses in the technology industry through its classification criteria.

Considering my criteria I will be agreeing and using the sources of Deloitte Fast and EU has their classification makes more sense to me personally. They focus on growing companies and considers wide range of data which gives a picture about future projections while International Finance Corporation (IFC) has its major importance on developing nations. Hence, I am going to consider my criteria where revenue less than 10 million euros will be for small or medium–sized business, 10 to 50 million euros for small or medium enterprise and greater than 50 million for large enterprises.

Total Assets of the Company:

Total assets are frequently used as a criterion for dividing businesses into small, medium, and large categories because they offer a gauge of an organization's total size and financial strength. All of a company's resources, including currency, investments, real estate, machinery, and inventory, are included in its total assets.

The classification component of total assets has several advantages. In the first place, it makes it possible to assess a company's size objectively and quantitatively, allowing for straightforward comparisons across markets and countries. The capacity of a company to finance expansion, acquire rival businesses, or weather economic downturns can also be determined by looking at total assets. Thirdly, compared to other factors, such as income, which can fluctuate, total assets may be a more stable classification factor.

1. **International Finance Corporation (IFC) :** based on total assets IFC categorizes total assets for small enterprise as less than 3 million dollars and for medium enterprise less than 15 million dollars. While for large it is greater than 15 million dollars.

2. **European Commission**: European commission categorizes small business with total assets upto or less than 4 million euros and medium size business between 4 million euros and 20 million euros. Large business have total assets more than 20 million euros.

3. **Small Business Administration (SBA):** For small businesses total assets should be upto 15 million dollars. For medium sized businesses total assets are from 15 million to 75 million dollars. While for large businesses it is more than 75 million dollars.

1.3 Classification table

	No.of employees	Total revenue	Total Asset
Small Business	Less than 50	Less than 10 million USD	Less than 5 million USD
Medium Business	50 to 249	Between 10 million USD to 50 million USD	Less than 20 million USD
Large Business	Greater than 250	Greater than 50 million USD	Greater than 20 million USD

Table 1: Business Classification Based on Employee Count, Total Revenue, and Total Asset

1.4 Small or medium Size business

Considering the factors discussed above for small sized businesses I have taken the company "SolarFi". A community of people focused on making a difference called SolarFi is developing a system for emergency response and hospitality that is more effective and sustainable. SolarFi aims to contribute to the global movement toward the use of solar energy for urban and commercial transformation by offering environmentally friendly options for emergency response and leisure services.

The total number of employees is 10 and the total revenue of around 5 million. SolarFi creates solar products for providing energy solutions.

The CEO of SolarFi is Antonio Dixon.

Security issues associated with SolarFi or small size business is :

a. Small companies mean less number of employees which means they have less resources to deploy on IT systems which could lead to faulty and misconfigured systems.

b. Another issue is that they don't have dedicated security team for securing data and IT systems.

c. These small companies like SolarFi also outsource or use third parties for their IT system management and configuration. Relying on a third party is an expansion of trust which may cause security issues.

d. Companies like SolarFi generally don't have enough budget to inform the employees regularly about security issues and attacks that could happen to them which makes employees unaware and uneducated about security risks.

1.5 Small or medium Enterprise

The company I have selected for small or medium enterprise is ITX corp. ITX corp has total revenue of approx. 50 million USD. While the number of employees in ITX corp is 250. With a passion for entrepreneurship, ITX solves challenging problems for clients across the country and around the world.

The related security issues are :

1.They are usually transitioning from small business models or may be planning to transition into a large organization, thus they need to implement certain security requirements to fulfill their transitioning.

2. They have to rely on third party services to implement security measures as they may not have enough resources or budget to implement these services by themself.

3. They may not have technologically advances employees and may even lack basic cybersecurity awareness which may make them prone to several attacks.

They are very easy target of phishing and ransomware attacks.

1.6 Large Enterprise

The large enterprise I have selected is Amgen. The corporate headquarters of the American multinational biopharmaceutical firm Amgen Inc. are in Thousand Oaks, California. George B. Rathmann and William K. Bowes Jr. established the business in 1980. One of the largest independent biotechnology companies in the world, it is renowned for creating ground-breaking treatments for debilitating diseases like cancer, kidney disease, and rheumatoid arthritis.

Amgen has around 23000 plus employees and annual revenue of around 27 billion dollars. The enterprise has total assets of around 63 billion dollars. The security risk a large enterprise like this can face are:

a. Large number of employees means more risk that any employee can be targeted for a social engineering attack. Since humans are the biggest factor in security breaches.

b. Large enterprise also means a large number of systems and a bigger network spread across multiple locations to protect.

c. Large enterprise like Amgen also have industry-leading techniques like for example, Amgen has industry-leading products in biotech which means they will be targeted the most by the attackers. Hence there is a constant need to be industry's best in security standards like using the best data encryption, best data backup, etc.

d. Another major security issue is that any small data breach can lead to loss of large amount of money and a bigger hit to the reputation of the company which will be very costly.

1.7 Security Issues Common for all size companies

Certain security issues cannot be characterized by enterprise size. These security issues common for all size companies are:

1. Human risk is the weakest point of any security system. Social engineering, and phishing attacks are increasing day by day and every enterprise's employees' are humans.

2. From Time to time education of employees related to security and strong password methods is also a security issue that is common for all-size businesses.

3. Remote work is offered by all-size companies and employees use their personal devices on the company network which is a big risk in any security system.

4. Not giving or assigning a proper budget to security teams or not ignorance towards system security is also a big security threat.

Part 2- List Of Vulnerabilities

2.1 Executive Summary

The report states and categorizes the vulnerabilities that could be found for a large enterprise like Amgen using Open Source Intelligence. The gathering, analysis, and dissemination of material from freely accessible open sources are known as open source intelligence (OSINT). Information that is freely accessible online, in public records, and in other publicly available places falls under this category.

Using this technique of Open Source Intelligence I was able to find infrastructure information, information regarding email address format, network security information, competitor information, and tools used within the large enterprise, Amgen. The vulnerabilities are then risk assessed using the Probability vs Impact matrix. The network/website vulnerabilities that were discovered are majorly commonly occurring vulnerabilities across enterprises. The vulnerabilities found are not difficult to mitigate and could be mitigated using different methods like updating CSP policy, hiding server information, etc. The major and high-risk vulnerability according to me is the email address format which could be used in a number of ways to perform phishing attacks. Phishing attacks are increasing year by year and remain one of the top threat to any enterprise.

2.2 Vulnerabilities

My chosen large enterprise, Amgen is committed to discovering, creating, and disseminating cutting-edge human therapeutics that will aid patients with terminal illnesses in completely realizing the potential of biology. Using tools like cutting-edge human genetics, this approach begins by unraveling the complexity of illness and comprehending the fundamental ideas of human biology.

The vulnerabilities that I could find include:

2.2.1 *Format of email id and email address of the CEO [1]:*

I was able to find the mail address of the CEO, Mr. Robert A. Bradway, mail address: rbradway@amgen.com. This could be used in whaling or spearhead phishing attacks. I was also able to find the mail addresses of top officials and also a general format in which mail addresses are assigned in Amgen. The two general formats used by the large enterprise are [first_initial][last_name]@amgen.com and [first_name]@amgen.com. For example, if the name is John Doe, the email address is most probably jdoe@amgen.com or john@amgen.com. I was able to verify this information as I got emails from the respective employees/recruiters of the company because I applied for a job position. All this information can be used in various targeted phishing attacks.

2.2.2 *Website Security Vulnerabilities [2]:*

- **X-Powered-By header exposed:**
  The header known as X-Powered-By can disclose details about the particular technology utilized on a server, which could be taken advantage of to target weaknesses. To prevent this, it's recommended to alter the server's setup and eliminate this header.

- **HttpOnly cookies not used:**

When HttpOnly cookies aren't used, the client can access the cookies, which makes some client-side hacks possible. HttpOnly cookies should be required, so the website configuration needs to be modified.

- **CSP allows insecure active sources:**
  The content security policy on the website should not allow insecure active content.

- **CSP implemented unsafely:**
  The Content Security Policy might not properly impose restrictions on sources or it might include "unsafe-inline" code that doesn't employ a nonce or checksum. This makes XSS assaults more likely.

- **HSTS header does not contain includeSubDomains:**
  The includeSubDomains command is absent from the HTTP Strict Transport Security (HSTS) header. This directive tells the browser to apply the HSTS rules to this domain's subdomains as well.

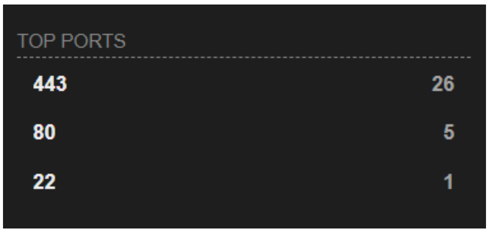
- **Domain was not found on the HSTS preload list:**
  The domain could not be located on the inventory of HSTS preloads. First-time visitors to the website will be at risk from MITM assaults. Hstspreload.org outlines the criteria for being added to the preload list.

- **CAA not enabled:**
  A valid Certification Authority Authorization (CAA) document is missing from the domain. The Certificate Authorities (CAs) that are permitted to issue certificates for a domain are listed in a CAA document.

- **DNSSEC not enabled:**
  Third parties are prevented from falsifying the records that confirm a domain's identification by DNSSEC records. For this name, DNSSEC configuration is required.

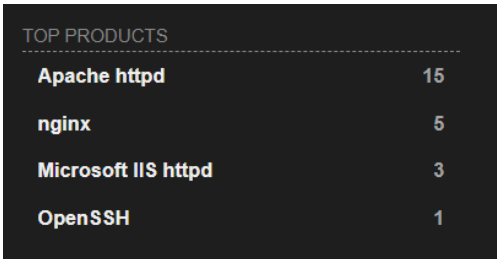
2.2.3 *Information about infrastructure found using (shodan.io search engine)[3]*:

- **Top Ports:**



TOP PORTS	
443	26
80	5
22	1

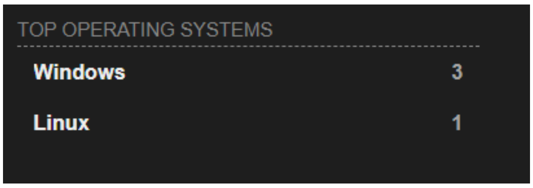
- **Top products used in the infrastructure:**



TOP PRODUCTS

Apache httpd	15
nginx	5
Microsoft IIS httpd	3
OpenSSH	1

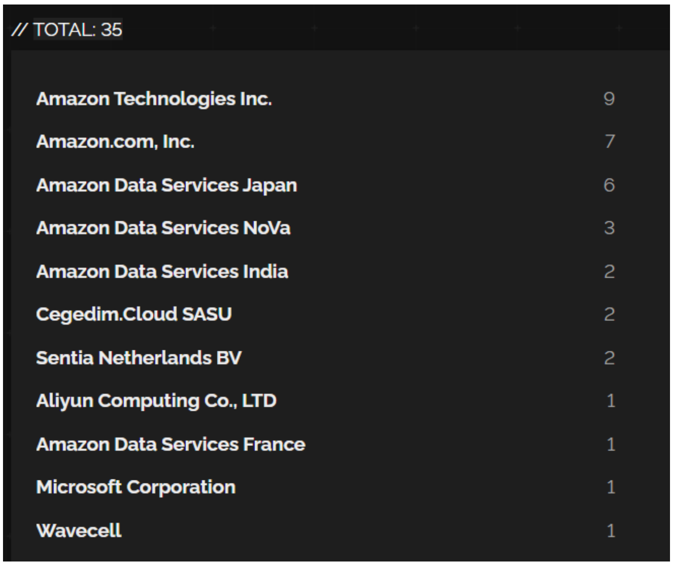
- **Operating System Used:**



TOP OPERATING SYSTEMS

Windows	3
Linux	1

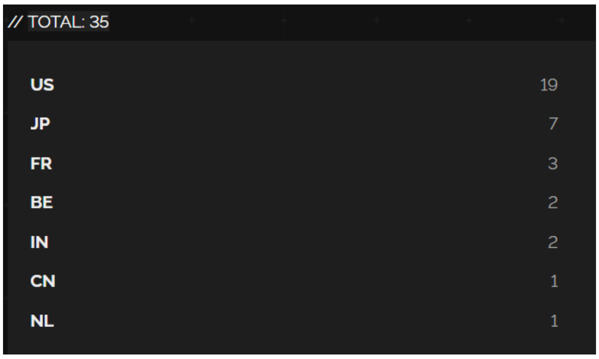
- **Third party organizations/services used**:



// TOTAL: 35

Amazon Technologies Inc.	9
Amazon.com, Inc.	7
Amazon Data Services Japan	6
Amazon Data Services NoVa	3
Amazon Data Services India	2
Cegedim.Cloud SASU	2
Sentia Netherlands BV	2
Aliyun Computing Co., LTD	1
Amazon Data Services France	1
Microsoft Corporation	1
Wavecell	1

- **Geographical Presence around the world**:



// TOTAL: 35

US	19
JP	7
FR	3
BE	2
IN	2
CN	1
NL	1

2.2.4 *Metadata from publicly released documents[4]*:

The large enterprise released documents on its website regarding environmental sustainability for public view. The metadata from the document revealed that the software used was “**Adobe InDesign 16.2 (Macintosh)**”, **“Adobe PDF Library 15.0”** and **“Adobe XMP Core 6.0-c006 79.164753”**.

2.2.5 *Competitors[5]*:

The top competitors of the large enterprise, Amgen include Merck, Genentech, MedImmune, Celgene, and Genzyme.

2.3 Probability versus Impact Matrix

IMPACT

PROBABILITY	LOW	MODERATE	HIGH
UNLIKELY	**LOW** **—**	**LOW** **–(3) Infrastructure vulnerability: Geographical presence–**	**MEDIUM** **—**
LIKELY	**LOW** **– (3) Infrastructure vulnerability: Third-party Services Used –**	**MEDIUM** **– (4) Metadata from publicly released documents –**	**HIGH** **– (3) Infrastructure information: ports, products, OS –**
VERY LIKELY	**MEDIUM** **– (5) Competitors information –**	**HIGH** **– (2) Website Security Vulnerabilities –**	**HIGH** **– (1) Format of email address –**

Table 2: Probability vs Impact Matrix

Part 3- Controls

3.1 Executive Summary

Controls are crucial for reducing vulnerabilities and hazards because they offer a methodical strategy for safeguarding the assets of an organization. By offering tools for identifying, preventing, detecting, and responding to threats, they assist in lowering the probability of a successful attack or data breach.

The list of controls I have suggested for the large enterprise Amgen concerning the vulnerabilities found in my assessment majorly lies in the preventative control category (around 77%). Around 12% are in detective controls and the rest are in audit and forensic controls categories. The goal of preventative measures is to stop attacks before they ever start. These include features like content security regulations, access controls, and encryption. Detective controls are used to find already-committed security flaws. Log monitoring and intrusion detection systems are two examples. After a security incident has happened, forensic controls aid in the investigation and analysis of the occurrence. This covers techniques like incident response strategy and digital forensics. By putting these procedures into place, you can lessen the risks posed by security events. For instance, keeping web servers updated and patched can stop attackers from taking advantage of known vulnerabilities. Multi-factor authentication can be put into place to assist prevent unwanted access to sensitive data. Regular vulnerability analyses can aid in identifying security flaws and offer suggestions for fixing them.

3.2 Controls

Ranking: Prioritizing security measures based on their relative efficacy and the level of risk they address might be useful when you have several security controls in place to reduce hazards. Utilizing a framework for risk assessment to assess each control's capacity to lessen the likelihood and impact of potential threats is one way to achieve this. This entails identifying potential threats, evaluating the likelihood and impact of each threat, identifying the security controls in place to address each potential threat, assessing the efficacy of each control, and ranking the controls according to how well they work and how much risk they reduce. Using this method, you can create a prioritized list of security controls that will assist you in managing the risks facing the organization. Here I have provided a ranked list of controls that should be employed by organizations (including Amgen) if they have vulnerabilities similar to what I have discovered in my Vulnerability/risk analysis.

3.2.1 *Email filtering*:

[TECHNICAL CONTROL]

Before emails arrive in a user's inbox, they are analyzed using specialist software to spot suspicious communications. This process is known as email filtering. An entry can greatly lower the danger of phishing attempts by putting email filtering into place. Because harmful attachments, phishing links, and other forms of malware may be identified and blocked by email filtering software, suspicious emails that contain them are less likely to be opened. In order to deploy email filtering, a company must select the right email filtering software and set up email filtering policies that specify which emails are permitted to reach users' inboxes. Additionally, email users should receive training on how to spot questionable communications and report them to IT or security staff.

3.2.2 *Multi-factor Authentication [1]*:

[TECHNICAL CONTROL]

Users must enter two or more different forms of authentication credentials in order to access a system or application when using the security mechanism known as multi-factor authentication (MFA). Even if an attacker has gained a user's password through a phishing assault, MFA's requirement for multiple forms of authentication can help prevent unauthorized access to a system or application. By devaluing passwords, diminishing the potency of phishing links, and enhancing the safeguarding of sensitive data, MFA can assist defend against phishing assaults. An organization must select a program or service that supports MFA, set the system up to demand MFA from specific individuals or groups, and then enroll people in the MFA system and let them select the types of authentication they like to utilize. MFA can help prevent phishing attempts since it requires users to give multiple forms of authentication each time they visit the system or application.

3.2.3 Employee training & Awareness:

[NON-TECHNICAL CONTROL]

A control that can be utilized to defend against phishing assaults is employee training and awareness. This entails teaching staff members about phishing attempts, checking the legitimacy of emails and links, and alerting the IT or security team when they notice anything odd. Training on phishing email identification is one way to do this. Employee education and awareness campaigns can heighten awareness of phishing scams, raise watchfulness, and lessen vulnerability to them. An organization can implement this control by holding simulated phishing exams, offering training sessions or online courses to staff, and reinforcing training with frequent updates and reminders. In general, increasing staff security knowledge and training is a good way to lower the likelihood of successful phishing attempts and strengthen an organization's security posture.

3.2.4 Regularly Updating & Patching web server:

[TECHNICAL CONTROL]

Regularly updating web server software and fixes is one of the most important procedures for mitigating website vulnerabilities. This security measure is crucial because known flaws in web server software are routinely used by attackers to access systems without authorization or harm them. Organizations can fix known vulnerabilities and make sure the web server is secure, dependable, and up to date by maintaining web server software.

3.2.5 Implement Content Security Policy (CSP) [2]:

[TECHNICAL CONTROL]

Cross-site scripting (XSS) attacks and other forms of code injection attacks can be thwarted by implementing CSP, a security feature, on web servers. In order for JavaScript, CSS, and other forms of material to be executed on a website, CSP enables companies to define which sources are permitted to do so. Organizations can lower their risk of threats by deploying CSP since it limits the sources that are permitted to execute content and helps stop attackers from injecting malicious code.

3.2.6 Enabling CAA & Http Cookies Only:

[TECHNICAL CONTROL]

Client-side scripting languages like JavaScript cannot access cookies that are HttpOnly in nature. Organizations can stop cross-site scripting (XSS) attacks that take advantage of cookie vulnerabilities by enabling HttpOnly cookies. For web servers that handle sensitive data or have a high risk profile, this control is crucial. Organizations can define which certificate authorities (CAs) are permitted to issue SSL/TLS certificates for their domain by using the CAA DNS entry. Organizations can lessen the danger of man-in-the-middle (MITM) attacks by enabling CAA, which prevents unauthorized CAs from issuing certificates for their domain.

3.2.7 *Regular Vulnerability Assessments*:

[TECHNICAL CONTROL]

The company can detect vulnerabilities and prioritize remediation activities by conducting regular vulnerability assessments. Network scans, application scans, and penetration testing are a few examples of these evaluations. Early vulnerability detection allows the company to take corrective action before attackers can use them against it. Not only should vulnerability assessments be performed when a security issue is suspected or confirmed, but also on a regular basis.

3.2.8 *Enable Certificate Authority Authorization (CAA) [3]*:

[TECHNICAL CONTROL]

Organizations can define which certificate authorities (CAs) are permitted to issue SSL/TLS certificates for their domain using the CAA DNS record. Organizations can lessen the danger of man-in-the-middle (MITM) attacks by turning on CAA, which prevents unauthorized CAs from issuing certificates for their domain.

3.2.9 *Network Segmentation [4]*:

[TECHNICAL CONTROL]

The process of segmenting a network entails breaking it up into smaller subnetworks or segments, each of which has its own set of security measures. This can lessen the chance that important assets will be exposed to attackers and stop lateral movement in the event of a breach. The business can implement various security controls by segmenting the network according to the importance of the infrastructure or data in each segment. This can lessen the chance that an attacker will move laterally over the network and get access to crucial infrastructure or data.

3.2.10 *Access Controls [5]*:

[NON-TECHNICAL CONTROL]

Access controls are laws and practices put in place to restrict access to private information and infrastructure. Policies like least privilege, multi-factor authentication, and role-based access control are examples of access controls. The least privilege concept states that users or devices should only be given the minimal access necessary to carry out their tasks. By requesting more than simply a password from the user, multi-factor authentication offers an additional layer of security. By allocating permissions based on the role or function of the user, role-based access management can help guarantee that users only have access to the data and infrastructure they need to carry out their assigned tasks.

3.2.11 *Using Encryption*:

[TECHNICAL CONTROL]

An organization can use encryption as a control to lessen the risk of vulnerabilities brought on by infrastructure information breaches. Information is encoded using encryption so that only those with the proper access can read it. An organization can use encryption at rest and encryption in transit. These are the two basic types of encryption. Data that is stored on devices is encrypted during encryption at rest, but data that is transmitted over networks is encrypted during encryption in transit. When implementing encryption, it's crucial to take into account the kinds of data and infrastructure that need to be secured, employ robust algorithms and long key lengths, and make sure that the encryption keys are safely stored and can only be accessed by authorized individuals.

3.2.12 Metadata Removal Tools:

[TECHNICAL CONTROL]

Software programs called metadata removal tools can be used to remove metadata from documents before they are made available to the public. These techniques are able to identify and eliminate metadata, including document attributes, author names, comments, and other data that can possibly reveal sensitive information. Organizations may make sure that papers made available to the public don't contain any information that threat actors could use against them by employing metadata removal technologies. There are many programs for removing metadata from documents, such as Doc Scrubber, the Metadata Anonymization Toolkit (MAT), and Adobe Acrobat Pro DC. With the use of these technologies, documents may be scanned for metadata and any sensitive material removed or redacted, making them suitable for publication to the public.

3.2.13 Document Classification and handling policies:

[NON-TECHNICAL CONTROL]

Organizations can use a set of rules called document categorization and handling policies to categorize documents according to how sensitive they are. Organizations can prevent the unintentional disclosure of sensitive information through metadata by adopting policies that specify how documents should be classified, who has access to them, and how they should be handled. Depending on the sort of information they contain, an organization could categorize papers as internal, public, confidential, or very confidential. Highly confidential documents can only be read by a select group of authorized individuals, in contrast to public documents, which might not include any sensitive information and are available for free distribution.

3.2.14 Intellectual Property Protection [6]:

[NON-TECHNICAL CONTROL]

For firms that largely rely on their technology, brand awareness, and other distinctive assets, protecting intellectual property is essential. The term "intellectual property" (IP) refers to mental works that are subject to legal protection, including inventions, literary and creative productions, symbols, names, and images. Businesses can use a variety of tools to protect their intellectual property, including patents, trademarks, copyrights, and trade secrets. For a specific amount of time, patents grant the owner the sole right to produce, use, and sell the invention. Trademarks, copyrights, trademarked works of authorship, and trade secrets all protect brands, logos, and other distinguishing markings. Businesses should restrict access to information and require non-disclosure agreements from partners, suppliers, and workers in order to preserve their trade secrets (NDAs).

3.2.15 Brand Protection [7]:

[TECHNICAL CONTROL]

Brand protection refers to the steps businesses take to maintain the integrity of their brand and stop third parties from exploiting it without their consent. To safeguard their brand reputation and revenue, businesses with strong brand presences in the market should think about putting brand protection measures in place. Monitoring for brand mentions, infringement, and other unlawful uses entails routinely scanning the internet, social media, and other channels. An organization can take steps to stop any unlawful use of its brand and preserve the reputation of the brand by recognizing such use. Finding and removing counterfeit goods from the market, which can harm a company's brand reputation and sales, is the goal of counterfeit detection.

3.2.16 Competitive Intelligence:

[TECHNICAL CONTROL]

The process of obtaining and studying information about rivals in order to achieve a competitive advantage is known as competitive intelligence. In order to make wise business decisions, it entails gathering information on the strengths, weaknesses, opportunities, and dangers of rivals. Businesses utilize a range of research techniques, including surveys, interviews, market research, and social media monitoring, to do this. It's crucial to collect this data responsibly and lawfully, without engaging in questionable practices like hacking or industrial espionage.

3.2.17 Security Information and Event Management (SIEM) Systems [8]:

[TECHNICAL CONTROL]

SIEM systems gather and examine security event data from a company's network and IT system. They aid in the detection of potential security breaches and give forensic investigators comprehensive information about the incident.

3.2.18 Acceptable Use Policy:

[NON-TECHNICAL CONTROL]

A collection of guidelines and restrictions known as an acceptable usage policy (AUP) specify how staff members and other authorized users are permitted to use the company's computer systems and resources. An AUP's goal is to guarantee that firm resources are utilized properly and that staff members are aware of their duties when using those resources. An AUP often contains guidelines for how email, the internet, and social media should be used. For instance, the policy might forbid staff from utilizing business tools to access objectionable or harmful material, including porn or hate speech. Additionally, it might forbid staff members from using company resources for actions that might pose a security risk, like downloading unauthorized software or visiting unsecured websites.

3.2.19 Asset Inventory Policy:

[NON-TECHNICAL CONTROL]

A policy for maintaining an inventory of hardware and software assets, as well as for monitoring their use and disposal, is described. The policy should specify how regular audits should be carried out to make sure that all assets are tracked and utilized properly.

3.3 Categorizing Controls:

Detective	*Preventative*	*Forensic*	*Audit*
Metadata Removal Tools	Email Filtering	Security Information and Event Management (SIEM) Systems	Regular Vulnerability Assessments
Competitive Intelligence	Multi-factor Authentication		Asset Inventory Policy
	Employee Training & Awareness		
	Regularly Updating & Patching web server		
	Implement a Content Security Policy		
	Enabling CAA & Http Cookies Only		
	Enable Certificate Authority Authorization (CAA)		
	Network Segmentation		
	Access Controls		
	Using Encryption		
	Document Classification and Handling Policies		
	Intellectual Property Protection		
	Brand Protection		
	Acceptable Use Policy		

Table 3: Categorizing controls into subcategories

Technical	Non-Technical
(SIEM) Systems	Asset Inventory Policy
Competitive Intelligence	Acceptable Use Policy
Brand Protection	*Intellectual Property Protection*
Metadata Removal Tools	*Document Classification and handling policies*
Using Encryption	*Access Controls*

Network Segmentation	Employee Awareness
Enable CAA	
Regular Vulnerability Assessments	
Enabling CAA & Http Cookies Only	
Implement CSP	
Regularly Updating & Patching web server	
Email Filtering	
Multifactor Authentication	

Table 4: Categorizing Controls as Technical / Non-Technical

Part 4- Budget

4.1 Executive Summary:

The cost for minimal set of controls needed is between 7 million USD to 7.5 million USD. The cost for practical budget is 18 million USD to 19 million USD and the cost of money not an object budget is 27 million to 30 million USD for the enterprise Amgen. For large biotechnology companies like Amgen, allocating funds for cybersecurity is essential. This is because cybercriminals frequently target the biotech industry because of its valuable intellectual property, research data, and private information. Significant financial losses, reputational harm, regulatory fines, and legal liabilities can result from a cybersecurity breach. Therefore, making an investment in cybersecurity measures is a pro-active move that can lessen the impact of any potential security incidents and assist prevent them altogether. Additionally, setting aside money for cybersecurity enables businesses to stay abreast of emerging security technology, carry out routine risk analyses and audits, train staff on best practices for cybersecurity, and react quickly to security crises.

4.2 Organising List of Controls

I will prioritize the list of controls according to what I feel is most urgent for the organization. The most urgent group of controls will determine the "*minimal cost*" and the following group will address the "*Practical cost*" and "*Money, not an object cost*".

Minimal/Urgently required:

1. Email Filtering
2. Multi-factor Authentication
3. Employee Training & Awareness
4. Regularly Updating & Patching the web server
5. Implement Content Security Policy (CSP)
6. Enabling CAA & Http Cookies Only
7. Regular Vulnerability Assessments

Practically required:

1. Email Filtering
2. Multi-factor Authentication
3. Employee Training & Awareness
4. Regularly Updating & Patching the web server
5. Implement Content Security Policy (CSP)
6. Enabling CAA & Http Cookies Only
7. Regular Vulnerability Assessments
8. Enable Certificate Authority Authorization (CAA)
9. Network Segmentation
10. Access Controls
11. Using Encryption

Money, not an Object:

This group will include the implementation of all the controls and their respective costs. Implementing all the controls will not fully mitigate the risks attached but an enterprise will be much safer and less likely to suffer a breach. The risks which cannot be mitigated are listed in the last section of the document.

4.3 Budget:

When creating a budget for security controls, it's important to find a balance between the cost of implementing controls and the potential risks and consequences of a security breach. While it may be tempting to allocate less money to security, doing so could end up being more expensive in case of a breach. To ensure that the budget is properly allocated and aligned with the organization's overall risk management strategy, it's crucial to involve all relevant stakeholders, such as IT, security, and senior management, in the process. I will be taking into account the factors for my chosen enterprise Amgen like 23000 employees, several geographical locations, vast infrastructure, etc.

4.3.1 Minimal Budget:

1. Email Filtering

   It's crucial to evaluate the email infrastructure of the company before deploying email filtering in order to choose the best option. To do this, it may be necessary to examine email usage trends, the email platform and user base, as well as any current email security measures.

   Depending on the characteristics of the system, the number of users, and the deployment style, the price of an email filtering solution might vary significantly. A cloud-based solution may cost an organization with 23,000 employees anything between $1 and $5 per user per month, whereas an on-premise solution could cost upwards of $50,000 for hardware and software licenses. Plus another $200000 to $500000 in hiring capable people for building in-house solutions. Plus the infrastructure cost will be around $50000 to $100000.

   Depending on the delivery method, the number of employees, and the training subject, the cost of employee training can vary greatly. The annual cost of training for a company with 23,000 employees might be between $50,000 and $100,000.

   Hence the total cost for a year can cost around between $600000 to 1 million depending on whether you use in house solution or third party service for email filtering.

2. Multi-factor Authentication

   There are numerous costs associated with establishing multi-factor authentication (MFA) for a company with 23,000 employees and a global presence. The cost of licensing will change depending on the solution selected, the number of users, and the degree of features needed. An MFA license can cost anything between a few dollars and several hundred dollars per user per year, with a monthly fee per user of around $5. This would result in a $1,380,000 yearly licensing fee.

   The amount it will cost to deploy MFA will depend on how integrated it needs to be, how sophisticated the corporate infrastructure is, and how many locations it needs to be used. The overall cost of implementation might be $1,150,000 if there is a reasonable level of integration and a cost of $50,000 per location. The cost of training will vary depending on the number of individuals who need to be trained and the method used; online training is expected to cost $50 per employee, with a $1,150,000 overall cost.

   Depending on the level of maintenance and support necessary, operational costs are expected to range from $25,000 per month for continuing maintenance and support to $300,000 per year. So, the overall cost of deploying MFA for the first year, which covers licensing, installation, training, and operational expenditures, might be around **$4, 980,000**.

3. *Employee Training & Awareness*

   An annual cybersecurity awareness training program costs $50 per employee, then training 23,000 employees would cost roughly $1,150,000 annually. However, if additional training is necessary, such as specialized training for IT workers or high-risk employees, the cost can go up.

4. Regularly Updating & Patching the web server

   Assuming that the cost of each hour of work for a system administrator is $50 and that they spend 10 hours per month updating and patching the web server, the cost of regularly updating and patching the web server for one year would be:

   $50/hour * 10 hours/month * 12 months * team of 10 admins = $60,000

5. *Implement Content Security Policy (CSP)*

   Evaluation and planning: Before implementing CSP, an evaluation of the website's existing code and infrastructure is necessary to determine how to implement CSP effectively. This may require hiring a cybersecurity consultant or a team of experts, which could cost anywhere from $50,000 to $200,000 depending on the complexity of the website.

   Implementation: Implementing CSP on a website typically involves modifying the website's code, which can be time-consuming and require expertise in web development and cybersecurity. Assuming a cost of $100 per hour for each developer and an estimated 500 hours of work, the total implementation cost could be $50,000.

   Testing and validation: Once CSP is implemented, it needs to be thoroughly tested and validated to ensure that it is effective and does not break any website functionality. This may require hiring a third-party testing service, which could cost anywhere from $5,000 to $20,000 depending on the scope of the testing.

   Maintenance and updates: CSP needs to be regularly maintained and updated to ensure that it remains effective as new threats emerge. This may require hiring a cybersecurity professional to monitor the website's CSP and make updates as necessary, which could cost $75,000 to $100,000 per year.

   Therefore, the total cost of implementing and maintaining CSP for a large enterprise like Amgen.com could be approximately $200,000 to $375,000 for the first year, with ongoing costs of $75,000 to $100,000 per year for maintenance and updates. It's important to note that these are rough estimates, and the actual cost may vary depending on the specific needs and circumstances of the organization.

6. *Enabling CAA & Http Cookies Only*

   Implementing the CAA would cost around $6,000 per year, assuming a consultant's fee of $5,000 to examine and provide advice on CAA records and an annual fee of $1,000 for continuous monitoring and maintenance.HTTP cookies alone: Assuming a $5,000 consultant fee to make the required alterations to the server and website setups, as well as a $1,000 annual fee for monitoring and maintenance, the total cost for deploying HTTP cookies only might be close to $6,000.

Therefore, for a website like amgen.com, the total cost for adopting both CAA and HTTP cookies solely might be close to $12,000 per year.

7. Regular Vulnerability Assessments

   Regular vulnerability assessments are an essential component of any enterprise's security strategy. The cost of vulnerability assessments will depend on the size of the enterprise, the complexity of the IT infrastructure, and the frequency of assessments. Assuming an enterprise similar to Amgen, with a budget of $25,000 to $50,000 per assessment, and assessments performed twice a year, the total annual cost could be between $50,000 to $100,000. This includes the cost of external consultants or a dedicated internal team to conduct the assessments.

Hence the total budget required for the minimal plan is between 7 million USD to 7.5 million USD for Amgen.

4.3.2 Practical Budget:

For the practical budget, we will add the cost of the minimal budget plus the additional cost of the controls required for the practical budget. So now we list out the additional controls for the practical budget and add the cost in minimal budget.

1. Enable Certificate Authority Authorization (CAA)

   Enabling Certificate Authority Authorization (CAA) for an enterprise like Amgen may involve some costs. The cost of implementing CAA depends on various factors such as the size of the enterprise, the complexity of the domain, and the number of domains to be protected. Assuming a similar-sized enterprise like Amgen, implementing CAA may cost around $5,000 to $15,000 for initial setup, configuration, and deployment. This cost may also include employee training and ongoing maintenance and support.

2. *Network Segmentation*

   Assessment and Planning:

   Cost: $50,000 to $100,000
   Includes: Hiring external consultants to perform a thorough assessment of the current network infrastructure and creating a plan to segment the network.
   Design and Implementation:

   Cost: $500,000 to $1,000,000
   Includes: Upgrading existing network hardware and software, implementing firewalls, and deploying intrusion detection and prevention systems.
   Testing and Verification:

   Cost: $50,000 to $100,000
   Includes: Conducting thorough testing to ensure the new network segmentation is effective and secure.

Ongoing Maintenance:
Cost: $250,000 to $500,000 per year
Includes: Regular updates, patches, and ongoing monitoring to ensure the effectiveness and security of the network segmentation.
Therefore, the total estimated cost to implement network segmentation for an enterprise like Amgen would be between $850,000 and $1,700,000 for the first year, with an ongoing maintenance cost of $250,000 to $500,000 per year.

3. Access Controls

Access control implementation might cost an organization like Amgen between $500,000 to $1,500,000 if complexity is moderate and consultation costs are $75 per hour. Included in this are the costs associated with creating access control policies, setting up access control systems, testing the solution, and deploying it.

The expenses of maintaining and updating the access control systems could be in addition to the ones associated with implementation. For a business like Amgen, the yearly operating cost may be as high as $500,000 if maintenance and support costs are assumed to be $50,000 annually.

4. Using Encryption

Encryption technology: The cost of encryption technology can vary depending on the solution selected and the level of encryption required. For an enterprise like Amgen, assuming a cost of $500 per license and 10,000 licenses required, the total cost for encryption technology would be $5,000,000.

Implementation costs: Implementation costs will depend on the level of integration required with existing systems, the complexity of the enterprise infrastructure, and the number of locations where encryption needs to be implemented. Assuming a moderate level of integration and a cost of $50,000 per location, the total implementation cost could be $1,150,000.

Training costs: Training costs will depend on the number of employees who need to be trained and the training approach. Assuming a cost of $50 per employee for online training, the total training cost would be $1,150,000.

Operational costs: The operational costs will depend on the level of maintenance and support required. Assuming a cost of $25,000 per month for ongoing maintenance and support, the annual operational cost would be $300,000.

Therefore, the total cost of implementing encryption for an enterprise like Amgen could be approximately $7,600,000 for the first year, which includes encryption technology, implementation, training, and operational costs.

Total budget for Practical category is 18 million USD to 19 million USD.

4.3.3 Money not an object Budget:

This budget will include all the costs for all the controls including cost of minimal and practical controls. We list the cost for all the controls which I mentioned in part 3 and add that cost to minimal and practical controls.

1. Metadata Removal Tools*:*

   While some programs for removing metadata are cost-free, others can run up annual costs of several hundred dollars for each user. For an organization with 23,000 employees, the annual licensing cost maybe $1,150,000 if the features are of a modest level and the fee is $50 per user per year.

   The complexity of the enterprise infrastructure, the number of sites where the tool needs to be installed, and the degree of interaction with current systems that is necessary will all affect how much it will cost to implement a tool. The overall cost of implementation might be $1,150,000 if there is a reasonable level of integration and a cost of $50,000 per location.

   The number of employees that need training and the training methodology will determine the cost of the training. The entire cost of training would be $1,150,000 if online training were to cost $50 per employee.

   The amount of upkeep and assistance needed will determine operational costs. The annual operating cost would be $300,000 if the cost of continuous maintenance and support was assumed to be $25,000.

   So, for a company with 23,000 people and a global presence, the overall cost of installing metadata removal tools for the first year might be around $3,750,000, which includes license, implementation, training, and operations expenditures.

2. *Document Classification and handling policies:*

   Creating policies can be done in house but there is a cost associated with tagging all the documents and training the employees. Assuming a cost of $50,000 for software licenses and implementation services, the total implementation cost for a enterprise could be around $1,150,000.

3. *Intellectual Property Protection:*

   Hiring an IP lawyer or consultant: This may involve costs such as hourly rates, retainer fees, and project fees. The cost of hiring an IP lawyer or consultant may range from $200 to $500 per hour.

   Conducting IP audits: An IP audit involves assessing the enterprise's intellectual property assets and identifying potential risks and vulnerabilities. The cost of an IP audit may range from $5,000 to $50,000 or more, depending on the scope of the audit.

   Implementing IP protection measures: This may include measures such as employee training, patent filings, trademark registrations, and software licensing. The cost of implementing these measures may vary depending on the specific measures required.

   Litigation costs: In the event of an IP dispute, the enterprise may incur costs such as legal fees, court costs, and damages. These costs can vary widely depending on the nature and complexity of the dispute.

   The yearly cost could be around 1 million USD to 2 million USD.

4. Brand Protection:

For a company like Amgen, the cost of brand protection implementation would rely on a number of variables, including the program's breadth, the organization's size, and the tools and technology used. Without additional details, it is challenging to provide a precise estimate. According to estimates from the industry, a large company's annual implementation costs for trademark protection systems might be anywhere from tens of thousands and millions of dollars.

5. Competitive Intelligence:

The cost of hiring or training staff to perform the work, the cost of any necessary software or technology tools, the cost of performing market research or data collection, and the cost of creating and implementing policies and procedures to guide the effort are some of the costs connected with implementing competitive intelligence controls. Hiring employees is going to cost about $200000 to $500000 dollars.

6. Security Information and Event Management (SIEM) system:

A company like Amgen may spend more or less money on a Security Information and Event Management (SIEM) system, depending on the size of the company, the complexity of its IT infrastructure, and the particular features and capabilities of the SIEM solution selected. A rough estimate for the cost of implementing a SIEM system for a company like Amgen, based on industry estimates and vendor pricing, could, however, range from $100,000 to $500,000 for the initial implementation, with ongoing costs for licensing, maintenance, and upgrades averaging around $50,000 to $150,000 per year.

7.Acceptable use Policy:

Here are some potential costs that could be associated with implementing an AUP for an enterprise like Amgen:

Policy development: This could involve hiring a team of consultants and lawyers to develop a comprehensive AUP, which could cost anywhere from $50,000 to $250,000.

Training and education: Developing and delivering training programs for thousands of employees across multiple locations could cost $20 to $50 per employee, resulting in a total cost of $400,000 to $1,000,000.

Enforcement: The cost of enforcing an AUP could vary depending on the level of effort required to monitor and investigate potential violations. This could involve hiring additional staff, investing in new security technologies, and conducting regular security audits. The cost of enforcement could range from $100,000 to $500,000 per year.

Ongoing maintenance: As with any security policy, an AUP requires ongoing maintenance and updates to remain effective. This could involve periodic reviews of the policy, updates to training materials, and revisions to enforcement procedures. The cost of ongoing maintenance could range from $50,000 to $100,000 per year. Based on these estimates, the total cost of implementing an AUP for an enterprise like Amgen could range from $600,000 to $1,850,000 in the first year, with ongoing costs of $150,000 to $600,000 per year.

8. Asset Inventory Policy:

For a company like Amgen with more than 20,000 employees, implementing an asset inventory strategy could include multiple cost categories. First, it might be necessary to buy or license asset discovery tools, which could cost between $10,000 and $50,000. Second, it could be required to provide employee training to make sure that staff members are aware of the policy and how to follow it. Creating and implementing training programs could cost between $50,000 and $100,000. Thirdly, maintaining the inventory may necessitate hiring more workers, which may cost between $25,000 and $75,000. Last but not least, continued monitoring would entail updating and reviewing the inventory on a monthly basis, which could cost $50,000 to $100,000. The actual expenses may differ from these estimates depending on the organization's unique demands and requirements.

Total budget for Money not an object category is 28 milllion USD to 31 million USD.

4.4 Categorizing Budget (Need vs Value)

Control Category	Budget Required	Cost per employee	Cost per site
Minimal	7-7.5 million USD	318-340 USD	70k-80k USD
Practical	18-19 million USD	818-864 USD	180k-200k USD
Money not an object	28-31 million USD	1272-1400 USD	300k-350k USD

Table 5: Summarizing Budget

When it comes to cybersecurity, a company like Amgen, which works in the highly regulated and delicate sector of biotechnology, has certain requirements. The business probably handles patient information, research data, and intellectual property that is extremely valuable and confidential. The company could suffer serious repercussions from a breach of this sensitive data, including a reduction in its ability to compete, harm to its brand, and potential legal and regulatory obligations. The importance of cybersecurity for a business like Amgen cannot be more emphasized given the significant risks involved. For such a business, investing in cybersecurity is essential since it helps to protect its most important assets and provides protection from potential online attacks. Effective cybersecurity measures can aid in preventing unauthorized access to sensitive data, identifying and quickly responding to cyber threats, and maintaining the integrity and accessibility of crucial systems and data. Overall, a firm like Amgen places a high priority on cybersecurity since it is so important to safeguard the company's assets and reputation in the highly competitive and regulated biotech sector.

4.5 Protecting against threats with no Technical Control

Non-technical controls like security policies can be very beneficial in defending against risks like social engineering attacks that cannot be directly controlled technically. The exact security measures you listed can help in the following ways:

Asset Inventory Policy: With the use of this policy, businesses can maintain tabs on all of their assets, including their data, software, and hardware. Organizations can more effectively identify potential security flaws, spot and address unauthorized changes to the network or data, and swiftly address security issues by keeping an accurate inventory of their assets.

An acceptable use policy (AUP) can assist organizations in setting standards for the proper use of their systems and resources, such as email, internet access, and social media. Organizations can assist lower the danger of social engineering assaults, such as phishing and other types of online fraud, by clearly defining for staff what constitutes acceptable use of business resources.

Intellectual Property Protection: This strategy can assist organizations in preventing the theft or unauthorized use of their priceless intellectual property, such as patents, trademarks, and trade secrets. Organizations can assist lower the danger of social engineering attacks by setting up rules and procedures for the protection of intellectual property that target employees who have access to sensitive data.

Policies for document handling and classification can aid organizations in making sure that private information is handled, disseminated, and categorized appropriately. Organizations can significantly lower the danger of social engineering attacks by outlining clear procedures for how to handle confidential information. These attacks rely on employees accidentally disclosing sensitive information.

Access Controls: Access controls, such as processes for authentication and authorization, can assist organizations in making sure that only individuals with the proper authorization have access to critical information and systems. Organizations can assist lower the risk of social engineering attacks by putting access controls in place. These attacks depend on unauthorized access to sensitive data.

Type Of Control	Total Cost	Cost per employee	Cost per site
Technical	22-24 million USD	1000-1400 USD	220k-250k USD
Non - Technical	5.5-7 million USD	500-700 USD	60k-80k USD

Table 6: Technical vs Non-Technical Controls

The cost compares similar to many competitive companies. According to a survey by Deloitte, in 2020, healthcare organizations, including pharmaceutical companies like Amgen, were estimated to spend an average of 4.1% of their overall IT budgets on cybersecurity.

4.6 Risk/Vulnerabilities which cannot be mitigated by these budgets

The incidence and impact of cyber risks and threats can be significantly reduced by implementing various cybersecurity safeguards, but it's crucial to understand that no system is 100% secure. Any digital system will inevitably have some level of risk, and some risks might still persist even after all reasonable safeguards have been implemented. For instance, it can be challenging to identify and stop insider threats and human mistakes, and new, highly effective malware and cyberattacks are continually being developed. Furthermore, even with the finest security measures in place, there is always a chance that the system may have unforeseen flaws or vulnerabilities that might be exploited.

Zero-day vulnerabilities are flaws that have not yet been patched or fixed and are unknown to the general public. No safeguards can be put in place to reduce the risk until a patch or remedy is created because they are unknown.

Insider threats: It is challenging to totally eliminate the risk provided by an insider with malicious intent, despite the fact that access controls and monitoring can assist limit insider threats to some extent.

Physical security risks: Although physical security measures can lessen the likelihood of theft, sabotage, or other physical attacks occurring, they cannot totally do so.

Despite the use of policies and training programs, human error remains a serious danger that cannot be completely eliminated. Employees may unintentionally reveal private information, fall prey to social engineering scams, or commit errors that result in security issues.

5. References

5.1 Part 1- Large Enterprise Criteria Report

1. IFC Org - https://www.ifc.org/wps/wcm/connect/b8f8dde7-893b-4809-873c-0c825f0284ef/InterpretationNote_SME_2012.pdf?MOD=AJPERES&CVID=mUtZ1jJ IFC Org – Dated 1st May 2023

2.https://www.open.edu/openlearn/money-business/business-strategy-studies/different-types-business/content-section-2 – Dated 1st May 2023

3.OECD Data https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm Dated 1st May 2023

4. Deloitte https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-connected-small-businesses-Dec2017-old.pdf– Dated 1st May 2023

5.IFC ORG
https://www.ifc.org/wps/wcm/connect/industry_ext_content/ifc_external_corporate_site/financial+institutions/priorities/ifcs+definitions+of+targeted+sectors - Dated 1st May 2023

6. ZoomInfo - https://www.zoominfo.com/c/itx-corp/20365530 - Dated 1st May 2023

7. Zoominfo - https://www.zoominfo.com/c/amgen/7834830 - Dated 1st May 2023

8. Solar Fi - https://solar-fi.com/ Dated 1st May 2023

5.2 Part 2- List Of Vulnerabilities

[1] Aeroleads - https://aeroleads.com/company/amgen-email-format - *"Dated 16th March 2023"*

[2] Upguard Security Report - https://www.upguard.com/security-report/amgen *"Dated 16th March 2023"*

[3] Shodan search Engine – shodan.io *"Dated 16th March 2023"*

[4] Metadata tool - https://www.metadata2go.com/ *"Dated 16th March 2023"*

[5] Competitor information Comparably -
https://www.comparably.com/companies/amgen/competitors *"Dated 16th March 2023"*

[6] Amgen website – amgen.com

5.3 Part 3- Controls

[1] https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA "What is multifactor authentication (MFA) and how does it work?" Dated – April 8th 2023.

[2] https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP "Content Security Policy (CSP) - HTTP: MDN" dated – April 8th 2023

[3] https://letsencrypt.org/docs/caa/ "Certificate Authority Authorization (CAA)" dated – April 8th 2023

[4] https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html "What Is Network Segmentation?" Dated – April 8th 2023

[5] https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control "What is Access Control? | Microsoft Security" – Dated April 8th 2023

[6] https://www.investopedia.com/terms/i/intellectualproperty.asp "What Is Intellectual Property, and What Are Some Types?" – Dated April 8th 2023

[7] https://www.mimecast.com/content/brand-protection/ "Brand Protection" – Dated April 8th 2023

[8] https://www.microsoft.com/en-us/security/business/security-101/what-is-siem "What is SIEM?" –Dated April 8th 2023

5.4 Part 4- Budget

E-mail filtering to protect from phishing

1. https://www.microsoft.com information from Microsoft Office 365 Advanced Threat Protection, April 15th 2023.
2. https://workspace.google.com- Google Workspace,April 15th 2023.
3. https://www.mimecast.com - Mimecast,April 15th 2023.
4. https://www.barracuda.com- Pricing information from vendors such as Barracuda Networks,April 15th 2023.
5. https://www.sophos.com -Sophos, April 15th 2023.
6. https://www.cisco.com- Cisco,April 15th 2023.
7. https://www.securityawarenesstraining.info/ - Estimates from industry sources such as Security Awareness Training,April 15th 2023.
8. https://cyberriskalliance.com- CyberRisk Alliance,April 15th 2023.
9. https://www.infosecinstitute.com- Infosec,April 15th 2023.

Multi-factor authentication (MFA)

1. https://www.onelogin.com - A casestudy by Onelogin, April 15th 2023.
2. https://duo.com -A blog post by Duo Security, an MFA provider,April 15th 2023.
3. https://www.csoonline.com - Article by CSO Online, April 15th 2023.
4. https://ww2.frost.com- A study by Frost and Sulivan April 15th 2023.

Employee awareness and training in cybersecurity

1. https://www.mediapro.com - "2020 State of Privacy and Security Awareness Report" by MediaPRO, April 15th 2023.
2. https://securityboulevard.com-"The True Cost of Security Training" by Security Boulevard, April 15th 2023.

3. https://www.techrepublic.com- "The Cost of Employee Cybersecurity Training" by TechRepublic, April 15th 2023.

Implementing Content Security Policy (CSP)

1. https://www.glassdoor.com/Salaries/web-developer-salary-SRCH_KO0,13.htm - estimated cost of a full-time web developer is based on data from Glassdoor, April 15th 2023.

2. https://www.ziprecruiter.com- cost of an external consultant is based on data from ZipRecruiter, April 15th 2023.

3. https://www.imperva.com- cost of a web application firewall (WAF) is based on data from Imperva , April 15th 2023.

4. https://report-uri.com CSP report-only implementation is based on data from report-uri.com, April 15th 2023.

5. https://www.tripwire.com -CSP implementation is based on data from a study by the Ponemon Institute, April 15th 2023.

Implementing CAA and HTTP cookies

1. https://cybersecurityventures.com - "The Cost of Cybersecurity in 2020" by Cybersecurity Ventures- April 15th 2023.

2. https://www.akamai.com - Case Study: Amgen Uses Akamai for Fast and Secure Web Experience by Akamai Technologies , April 15th 2023.

Implementing network segmentation and enabling Certificate Authority Authorization (CAA)

1. https://www.vmware.com- The Cost of Network Segmentation" by Larry Ponemon and sponsored by VMware, April 15th 2023.

2. https://www.varonis.com - "What Is Network Segmentation? Benefits, Types, Best Practices" by Varonis, April 15th 2023.

3. https://www.darkreading.com - The Real Cost of Network Segmentation" by Dark Reading, April 15th 2023.

Implementing access controls

1. https://www.gartner.com - Gartner: "How Much Will Security and Risk Management Spending Increase?" , April 15th 2023.

2. https://www.csoonline.com - CSO Online: "How much does a data breach cost? Here's what you need to know" , April 15th 2023.

3. https://www.securitymagazine.com - Security Magazine: "How Much Should You Spend on Cybersecurity?" , April 15th 2023.

Implementing encryption

1. https://www.bankinfosecurity.com -"The Cost of Encryption: Getting It Right" by Tracy Kitten, BankInfoSecurity, April 15th 2023.

2. https://www.sans.org -"The Cost of Encryption: TrueCrypt, VeraCrypt, and BestCrypt" by Jorge Orchilles, SANS Institute, April 15th 2023.

3. https://451research.com- "The Cost of Encryption: Why and How to Do It" by Amy Larsen DeCarlo,

April 15th 2023.

Implementing metadata removal tools

1. https://digitalguardian.com- Digital Guardian, April15th 2023.
2. https://www.itqlick.com - It Qlick, April15th 2023.

Implementing intellectual property protection

1. "Intellectual Property: Protecting Your Company's Most Valuable Assets" by Forbes,April 15th 2023.
2. "The Cost of Intellectual Property Theft" by The Balance Small Business,April 15th 2023.
3. "The Cost of Intellectual Property Protection" by PatSnap,April 15th 2023.
4. "The Cost of Intellectual Property Protection for Startups" by SeedLegals, April 15th 2023.

Licensing cost for the SIEM solution

1. Gartner's Magic Quadrant for Security Information and Event Management, April 15th 2023.
2. Cybersecurity Ventures' Cybersecurity Market Report,April 15th 2023.
3. Info-Tech Research Group's Security Information and Event Management (SIEM) Software Category Report, April 15th 2023.