CSEC.603.01 - Enterprise Security

Organizational Cybersecurity Evaluation (Final Report)

Pranjali Thakur (pt4202)

April 30, 2024

Contents

List of Tables

List of Figures

1 EXECUTIVE SUMMARY

This report addresses vulnerabilities in many areas of eBay's digital infrastructure and operations by outlining a thorough security assessment and suggested remedial actions. Understanding the size and features of different business categories depends on the classification of businesses into three groups: small and medium-sized businesses (SMB), small and medium-sized enterprises (SMEs), and large enterprises. Three main criteria are used to determine this classification: the total number of employees, annual revenue, and the capital expenditure (CapEx).

Typically, small and medium-sized businesses (SMBs) are those with 10 to 100 employees, yearly revenues under \$50,000, and minimal capital expenditures (CapEx). Small and medium-sized businesses, or SMEs, often employ between 100 and 500 people. Their annual revenue ranges from approximately \$50 million to \$1 billion, and they have a low capital expenditure. Large enterprises are defined as those with more than 500 employees, large capital expenditures (CapEx), and yearly revenues of more than \$1 billion. All businesses, regardless of their category, face similar security concerns despite differences in size and scope. These include ransomware, phishing assaults, data breaches, insider threats, and the difficulties of adhering to the ever-changing privacy and data protection regulations. Understanding the classification of businesses into SMBs, SMEs, and Large Enterprises provides valuable insights into their operational scales and challenges. It also highlights the universal nature of certain risks like cybersecurity threats, underscoring the need for tailored strategies and policies appropriate to each business category.

eBay as a large enterprise has several key vulnerabilities present across different areas of its digital footprint and operations. Website vulnerabilities are a notable problem as they may put consumers at risk of cross-site scripting (CSRF) and other web-based attacks. There were discovered weaknesses in the network security, such as the absence of DNSSEC, enabling DNS spoofing attacks. Due to the unintentional exposure of upper management's email addresses, there is an increased danger of phishing attacks and other email-related problems. A wide range of operating systems, open service ports, and the usage of web technologies that need to be updated often to prevent exploitations were all discovered by Shodan scans. To maintain its market position and safeguard its stakeholders, eBay needs to strengthen its security measures and make constant improvements. Payment Security Vulnerabilities being one of the most critical for a marketplace like eBay along with Supply Chain Vulnerabilties that can be mitigated with regular audits.

Further, this report proposes security controls that are designed to mitigate identified vulnerabilities within eBay's digital infrastructure. The controls have been categorized based on their direct impact on addressing technical vulnerabilities, supporting organizational security policies, and ensuring compliance with regulatory standards. The security controls implemented to safeguard eBay's infrastructure are not only categorized based on their effectiveness but are also flagged according to their functional roles as preventative, detective, forensic, and audit controls. This multi-faceted classification ensures that our security measures not only proactively prevent incidents but also provide the necessary tools to detect breaches, conduct in-depth forensic analysis, and facilitate comprehensive audits to uphold standards and improve our security posture continually.

The "Most Effective Controls," which handle urgent and severe vulnerabilities including Cross-Site Scripting (XSS), unauthorized access, and data breaches, are a primary focus of our strategy. Using Web Application Firewalls (WAF), Multi-Factor Authentication (MFA), and strong encryption methods are some examples of these controls. These are essential because they offer immediate protection against intrusions that can compromise the integrity of the system and user data. Through the mitigation of common risks and reduction of the overall attack surface, the "Highly Effective Controls" are intended to support our primary defenses. In order to protect sensitive transactions and prevent phishing attacks, this layer of defense includes crucial components including network segmentation, email filtering, and increased transaction verification.

"Moderately Effective Controls" include regular Threat Intelligence, vulnerability scanning, and the usage of Security Information and Event Management (SIEM) for ongoing security management and vulnerability mitigation. These controls are necessary to identify possible vulnerabilities and make sure they're fixed immediately. "Supportive & Procedural Controls" are designed to enhance organizational security by implementing comprehensive policies, training, and best practices, in addition to supporting these technical measures. Enforcing strict document handling guidelines and safeguarding intellectual property fall under this category. These measures are essential for preserving the integrity and confidentiality of sensitive data. "Audit Controls" ensure continuous compliance and validation of our security framework. Regular IT security audits and compliance checks are crucial for assessing the effectiveness of our security measures and making necessary adjustments in response to evolving threats and regulatory requirements. This structured approach to security controls enables eBay to robustly defend against a diverse range of threats while maintaining compliance and supporting business continuity. This strategy not only protects against current vulnerabilities but also enhances our ability to adapt to future security challenges.

Lastly, the report presents the security budget scenarios for eBay, providing detailed analysis for three budget approaches: Minimal, Practical, and Money No Object. The goal is to address eBay's key security requirements while considering various financial constraints. This report also discusses the risks and trade-offs associated with each budget scenario, offering insight into the most effective strategies for safeguarding eBay's infrastructure, data, and operations.

The Minimal budget focuses on the absolute minimum controls necessary to address the most pressing risks. It is designed for cost-effective security, emphasizing Multi-Factor Authentication (MFA), Network Segmentation, and Secure Backup within the network and infrastructure security group. Compliance efforts focus on Access Control and Compliance Audits, while data protection includes Encryption and Content Security Policy (CSP). Basic threat detection is achieved with Security Information and Event Management (SIEM) and Penetration Testing. Vendor Risk Management (VRM) and Continuous Monitoring are also part of this budget. While this minimal approach is cost-effective, it may leave certain risks unaddressed, offering limited redundancy and reduced threat detection capabilities. The total cost for minimal budget is $1,958,450.

The Practical budget has a more balanced approach which offers a broader range of controls that address both network and infrastructure security and data protection, with a moderate cost. It includes MFA, Network Segmentation, Secure Configuration Management, Patch Management Systems, and Secure Backup to ensure robust infrastructure security. Compliance efforts are strengthened with comprehensive security policies, training, and monitoring of legal and regulatory changes. Data protection expands to include Secure Storage and Handling of Logs, Email Filtering, and other essential controls. Threat detection and response are improved with SIEM, Enhanced Transaction Verification, User and Entity Behavior Analytics (UEBA), and Incident Response. Vendor risk management is broadened with Third-Party Audits, while logging and monitoring are enhanced with Continuous Monitoring and Threat Intelligence. Although more comprehensive than the minimal budget, the practical budget might still have limitations in redundancy and audit scope. Total calculated annual cost for practical budget is $16,117,926.

The "Money No Object" budget address all potential risks with top-tier controls and comprehensive security solutions. This budget includes a wide range of controls to ensure maximum security and compliance. Network and infrastructure security is reinforced with premium tools, including Web Application Firewalls, Intrusion Detection/Prevention Systems, and advanced patch management. Compliance and audits are extended to encompass Third-Party Audits and IT Audits, with additional focus on policy development and enforcement. Data protection and encryption are covered with high-end encryption solutions and secure communication protocols. Threat detection and response are optimized with comprehensive tools and premium services, ensuring robust incident response capabilities. This budget also includes extensive logging, monitoring, and analytics with advanced threat intelligence. While this approach offers the most comprehensive security coverage, it involves significant financial investment and operational complexity. Approximate annual total cost for money not an object budget is $21,371,056.

Each budget scenario addresses a different level of security and risk mitigation. The minimal budget ensures basic security controls, the practical budget strikes a balance between risk mitigation and cost, and the money no object budget offers comprehensive security coverage. Depending on eBay's financial resources and risk tolerance, these scenarios provide tailored solutions to maintain a secure and compliant environment.

2 CLASSIFICATION FACTORS FOR ENTERPRISES

SMB, SME, and Large Enterprise are classified on several factors. They sometimes depend on the geographical location and the sector the organization belongs to. These are some of the factors majorly used to classify these organizations:

2.1 Number of Employees

- **Organization for Economic Co-operation and Development(OECD):[1]** According to OECD, the classification is straightforward with small businesses defined as having 10-49 employees. Medium-sized businesses employ between 50 and 249 individuals. This range suggests significant growth from the small business phase, likely indicative of expanded market reach, increased capital, and a more complex organizational structure. Large enterprises employ 250 or more people. This threshold marks a transition into a major business category, often accompanied by a broader geographic presence, a more complex hierarchical structure, and a greater impact on the market.

- **International Finance Corporation(IFC):[2]** IFC offers a slightly broader definition, extending the upper limit for medium-sized businesses to 299 employees. The IFC sets the bar slightly higher, categorizing enterprises with 300 or more employees as large. This demarcation aligns with a business's evolution into a major player in its industry, typically featuring extensive operations, a wide product or service range, and a significant influence on market trends and competition.

- **Corporate Finance Institute:[3]** In the United States, the definition of SMB/SME is further tailored to industry sectors. For example, in certain sectors like wholesale, a medium-sized business may have a maximum of 100 employees, whereas in sectors like nickel or copper mining, the limit can extend up to 1,500 employees, and in silver mining, up to 250. This variation reflects the differing operational and labor demands across industries. In North America, the threshold for large enterprises often starts at 500 employees. This distinction reflects the scale and scope of businesses in the US and Canadian markets, where companies of this size usually have a national or international reach. If the number of employees exceeds 500 it falls under the Large enterprise category.

The number of employees is a fundamental factor in classifying organizations. While there is general agreement on the ranges, some variability exists, especially in the upper limit for medium-sized businesses and the starting point for large enterprises. Looking at all three resources we can say that SMBs can have 10-100 employees. This range is an approximation that considers the lower end defined by the OECD (10-49 employees) and the broader classifications from other sources. It reflects SMBs as businesses that have moved beyond the startup phase but are not yet large-scale operations.

SMEs can be shown with 100-500 employees, encapsulating the upper limit of SMBs and approaching the lower threshold of large enterprises. This range indicates businesses that have experienced significant growth, likely with expanded market reach and increased operational complexity.

Large enterprises can be classified as having 500 or more employees, reflecting the transition into major business entities. This suggests extensive operations, possibly on a national or international scale, with a significant market impact and a complex organizational structure.

2.2 Annual Revenue

- **International Finance Corporation(IFC):**[2] The IFC categorizes small businesses as those with annual revenues between $1 million and $3 million. Medium businesses have annual revenues ranging from $3 million to $15 million. This classification captures businesses that have grown beyond the small business stage and demonstrate a more significant impact in their industry. For large enterprises, the IFC suggests an annual revenue threshold of more than $15 million.

- **Gartner:**[4] Gartner extends the upper revenue limit for small businesses to about $50 million. This broader range can include businesses that are more established than those in the IFC's small business category and are likely competing in markets or industries where the revenue scales are inherently higher. They define medium businesses as those with revenues ranging from $50 million to $1 billion. Similar to the IFC, they identify large enterprises as those with annual revenues exceeding $1 billion, underlining their extensive operational scale and significant market influence.

- **Investopedia:**[5] Investopedia's definition of small businesses in terms of revenue is aligned with Gartner, placing the upper limit at less than $10 million. This threshold encompasses a broad spectrum of small businesses, from start-ups and local businesses to more established companies in certain industries. Investopedia categorizes medium businesses as those having annual revenues between $10 million and $1 billion. Aligning with both the IFC and Gartner, Investopedia defines large enterprises as businesses with annual revenues of more than $1 billion.

Annual revenue is a significant indicator of a business's size. The annual revenue for SMBs should be anywhere less than $20 million, acknowledging the lower threshold from the IFC and the broader range from Gartner and Investopedia. This range covers businesses from early revenue generation to more established businesses.

For SMEs, the revenue range can be set between $20 million and $1 billion. This captures the growth from the higher end of the SMB category and includes businesses that are to the point of becoming large enterprises, as per the varied definitions from IFC, Gartner, and Investopedia.

Large enterprises are businesses with annual revenues exceeding $1 billion, consistent across the IFC, Gartner, and Investopedia definitions. This signifies a high level of market dominance and operational scale.

2.3 Capital Expenditure (CapEx)

- **Your Digital Resources:**[6] This source highlights that SMBs typically have limited CapEx. This limitation is reflective of their smaller operational scale and financial resources. SMEs, being a step above SMBs, typically have a moderate level of CapEx. While not as constrained as SMBs, SMEs still operate within certain financial limits. Large enterprises have the financial capability for large CapEx investments.

- **Vocalcom:**[7] Echoing a similar perspective, Vocalcom notes that SMBs usually have part-time individuals managing their data and IT infrastructure. The implication here is that SMBs, due to their limited CapEx, are likely to outsource major IT and infrastructure needs rather than invest heavily in them. SMEs are described as having more full-time employees managing data and IT infrastructure compared to SMBs, indicating a moderately higher CapEx. This increased investment in CapEx for SMEs suggests that they are likely to engage in more substantial projects and may have better infrastructure and technology compared to SMBs. Large enterprises have a full-time, specialized IT staff and extensive operations, indicating significantly higher CapEx. This substantial financial capacity for investments in infrastructure and technology differentiates large enterprises from SMEs and SMBs.

- **Cubeler:**[8] SMBs typically have limited CapEx, reflecting their smaller operational scale and financial resources. SMEs generally employ full-time employees for managing data and IT infrastructure, indicating a higher CapEx than SMBs. These employees are often IT generalists handling multiple tasks, which reflects a balance between growth and financial caution. Large enterprises have significant CapEx, supporting their extensive operations and strategic goals. Large enterprises have dedicated, full-time IT staff with specific expertise, reflecting their substantial financial capacity for major investments.

CapEx varies markedly across these categories. The CapEx for SMBs is noted as 'Limited', reflecting their smaller scale operations and constrained financial resources, as mentioned in the sources. SMEs are described with 'Moderate' CapEx, indicating a higher level of investment than SMBs but still within certain financial limits, suitable for their scale of operations. Large enterprises have 'High' CapEx, aligning with their extensive operations and strategic goals, as well as their ability to invest substantially in technology, infrastructure, and innovation.

Category	**Number of Employees**	**Annual Revenue**	**Capital Expenditure**
SMB	10 - 100	Less than $20 million	Limited
SME	100 - 500	$20 million - $1 billion	Moderate
Large Enterprise	500+	Over $1 billion	High

Table 1: Comparison of Classification Factors for SMB, SME, and Large Enterprises

3 SMALL OR MEDIUM SIZE BUSINESS

CustomerGlu represents a small or medium-sized business, with a workforce of 31 employees. Operating with an annual revenue of less than $5 million, it falls within the smaller scale of the business spectrum. Its capital expenditure, amounting to approximately $490K, reflects the typical financial constraints and investment capabilities of businesses in this category. This level of CapEx suggests focused, strategic investments, likely in areas critical to sustaining and growing their business operations.[9][10]

SMBs such as CustomerGLu, face unique cybersecurity challenges that differ in some aspects from those faced by larger enterprises. Here are some security risks that are specific to SMBs like CustomerGlu:

1. SMBs often have limited budgets and fewer resources to allocate to cybersecurity. This can lead to gaps in their security defenses, such as outdated security software, lack of advanced threat detection systems, and inadequate employee training on security best practices.

2. With potentially less training and awareness among employees, SMBs like CustomerGlu can be more susceptible to phishing and social engineering attacks. These attacks often rely on tricking employees into revealing sensitive information or granting access to company systems.

3. SMBs often rely heavily on third-party cloud services for cost-effective and scalable solutions. However, if these services are not properly secured, they can introduce vulnerabilities. SMBS must understand the security measures of their cloud providers and ensure that their data is adequately protected.

4. Many SMBs lack comprehensive data backup and recovery strategies. This makes them particularly vulnerable to ransomware attacks, where access to data is blocked until a ransom is paid. Without proper backups, SMBs could face significant operational disruptions and data loss.

5. SMBs like CustomerGlu may not have the luxury of a large, dedicated IT security team. Limited in-house IT expertise can lead to slower detection and response to security incidents. Additionally, without dedicated security personnel, ongoing security risks might not be adequately identified and mitigated.

4 SMALL OR MEDIUM ENTERPRISE

Uniswap is classified as a small or medium enterprise, a step above smaller businesses like CustomerGlu. With 131 employees, it has a larger organizational structure and a broader operational scope. Its annual revenue of $23.2 million signifies a significant market presence and financial stability. The company's CapEx of $176 million indicates a substantial capacity for reinvestment into business growth, technological advancement, and market expansion strategies, typical of enterprises at this scale.[11][12]

1. SMEs, due to their increased financial turnover and growing market presence, can become attractive targets for cybercriminals. These businesses might face more sophisticated cyber attacks, including targeted phishing, advanced persistent threats (APTs), and complex ransomware attacks.

2. As SMEs often work with a network of suppliers and third-party service providers, they are exposed to supply chain vulnerabilities. A breach in any part of the supply chain can compromise the security of the entire network.

3. With a larger operational scale, SMEs like Uniswap may have to adhere to more stringent regulatory requirements. Staying compliant with various industry standards and regulations, such as GDPR, can be challenging and requires dedicated resources and expertise.

4. As SMEs handle larger volumes of data, including sensitive customer information, they face increased risks related to data management and privacy. Ensuring data is securely stored, handled, and transmitted is crucial to prevent breaches and maintain customer trust.

5. With a higher number of employees, internal security management becomes more complex. This includes ensuring that all employees are adequately trained on security best practices, managing access controls effectively, and monitoring internal systems for any signs of suspicious activity.

5 LARGE ENTERPRISE

eBay stands as a large enterprise, evident from its extensive workforce of 10,600 employees and an impressive annual revenue of $10.1 billion. These figures place eBay in a significantly different operational bracket compared to smaller businesses and SMEs. The company's capital expenditure of $1.2 billion highlights its vast resource pool and investment capabilities, enabling it to maintain its competitive edge, innovate, and expand its global market reach.[13][14]

1. Large enterprises often have complex and heterogeneous IT infrastructures, incorporating legacy systems along with modern technologies. This complexity can create security gaps and makes it challenging to maintain a consistent security posture across all systems and platforms.

2. Due to their size and influence, large corporations like eBay are more likely to be targets of nation-state actors or get embroiled in geopolitical cyber conflicts. These attacks can be highly sophisticated and may aim at either corporate espionage or disrupting business operations.

3. Large enterprises typically integrate with a myriad of third-party services and platforms for various business functions. Each integration point potentially opens up a new attack vector, making it essential to rigorously vet and monitor all third-party partners for security compliance.

4. For a large enterprise, the impact of a cyber incident extends beyond immediate financial losses. The damage to the brand reputation and customer trust can have long-lasting effects on the business. Thus, managing public relations and customer communication becomes a critical aspect of cybersecurity incident response.

5. DDoS attacks threaten large enterprises like eBay by overwhelming their networks, disrupting operations, and causing financial losses, necessitating robust mitigation strategies for these high-profile, online-dependent businesses.

6 SECURITY ISSUES COMMON FOR ALL SIZE ENTERPRISES

1. This is a universal threat where attackers use deceptive emails or messages to trick employees into revealing sensitive information or installing malware. No company size is immune to phishing, as it targets individual behavior rather than technological vulnerabilities.

2. These can arise intentionally or accidentally from employees, contractors, or partners who have access to the company's systems and data. The impact of insider threats can be substantial, regardless of the size of the organization.

3. Unpatched or outdated software can present vulnerabilities that are exploitable by attackers. This risk is universal, as all businesses use software that requires regular updates and maintenance.

4. While often overlooked in discussions about cybersecurity, physical security breaches, like unauthorized access to buildings or data centers, can lead to significant data loss and are a concern for businesses of every size.

7 LIST OF VULNERABILITIES

When discussing general vulnerabilities at eBay, it's important to consider the broad spectrum of potential threats that an enterprise of its scale could face. These can range from technical issues within their web infrastructure to broader operational and strategic challenges. To create a probability vs. impact matrix for the vulnerabilities, each vulnerability is assigned a likelihood (probability) and an impact level. The risk value for each vulnerability is calculated by multiplying the likelihood by the impact (Risk Value = Likelihood x Impact).The Probability and Impact scale is taken to be between 1 and 5, 1 being the lowest and 5 being the highest. Here's an overview of the types of vulnerabilities that could potentially affect eBay:

7.1 Web Vulnerabilities

eBay's vulnerability report from UpGuard highlights[15] various security risks and evaluates the platform's security posture based on several factors, such as website security. he report uses UpGuard's continuous monitoring to assess eBay's external attack surface, offering a comprehensive view of its security landscape. It examines several key risk categories, including potential vulnerabilities in website security. It provides insights into areas where eBay might need to improve its security practices to mitigate risks. These assessments can guide eBay in addressing vulnerabilities and enhancing its security measures.

1. **Set-Cookie Headers Without 'SameSite' Attribute:**
   Cookies lacking the 'SameSite' attribute are vulnerable to Cross-Site Request Forgery (CSRF) attacks, where an attacker tricks a user's browser into performing unintended actions on a trusted website. CSRF attacks can lead to unauthorized account access, data manipulation, and other malicious activities. This vulnerability can compromise user security and trust in eBay's platform.

2. **Transfer-Encoding - Chunked:**
   The 'Transfer-Encoding: chunked' HTTP header can lead to buffer overflow attacks when improperly handled. Attackers can exploit this vulnerability to inject malicious code or disrupt server operations. Buffer overflow attacks can cause server crashes, data corruption, or unauthorized code execution. This vulnerability poses a significant risk to eBay's server stability and data integrity.

3. **Information Disclosure in Server Header:**
   The server header in HTTP responses may reveal sensitive information about eBay's server configuration, such as the server software version or platform details. Information disclosure can provide attackers with valuable insights into eBay's server setup, making it easier to exploit known vulnerabilities or plan targeted attacks.

4. **Cross-Site Scripting (XSS):**
   Cross-Site Scripting (XSS) occurs when an attacker injects malicious scripts into a trusted website, allowing them to execute code in the context of another user's session. XSS attacks can lead to unauthorized data access, session hijacking, or distribution of malware. This vulnerability can compromise user data and damage eBay's reputation.

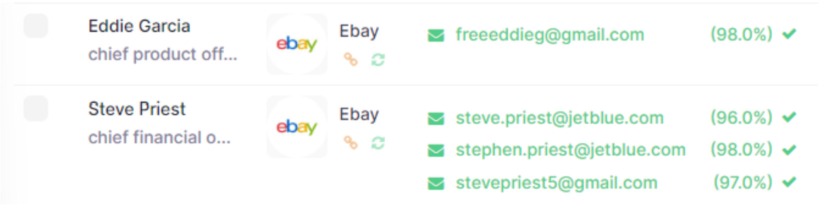
5. **Security Configuration:**
Misconfigurations in server settings can create security vulnerabilities, allowing attackers to bypass security controls or access sensitive data. Improper security configurations can lead to unauthorized access, data breaches, or service disruptions. This risk is heightened if security controls are not properly implemented.

Vulnerability	Likelihood	Impact	Risk Value
Set-Cookie Headers Without 'SameSite' Attribute	4	3	12
Transfer-Encoding - Chunked	3	2	6
Information Disclosure in Server Header	3	2	6
Cross-Site Scripting (XSS)	4	4	16
Security Configuration	3	3	9

Table 2: Web Vulnerabilities Risk Score

7.2 Email Vulnerabilities

This image illustrates potential email vulnerabilities within eBay's system, specifically focusing on email addresses that could be targets for phishing attacks or unauthorized access. It indicates the importance of safeguarding high-profile email addresses[16] and implementing security measures to protect against phishing, spoofing, and unauthorized access.



Eddie Garcia chief product off...	Ebay	freeeddieg@gmail.com	(98.0%) ✓
Steve Priest chief financial o...	Ebay	steve.priest@jetblue.com stephen.priest@jetblue.com stevepriest5@gmail.com	(96.0%) ✓ (98.0%) ✓ (97.0%) ✓

Figure 1: Exposed Email addresses

1. **Phishing Attacks:**
Phishing can occur when attackers send emails that appear legitimate to trick users into providing sensitive information. The high verification scores suggest that these email addresses are commonly used, potentially making them targets for phishing attempts. Implementing strong email filters and user training can help mitigate this risk.

2. **Email Spoofing:**
Spoofing involves sending emails that appear to come from a trusted source. Given that these email addresses belong to high-level eBay executives, spoofing could lead to significant security risks. Implementing Domain-based Message Authentication, Reporting, and Conformance (DMARC) can prevent spoofing.

3. **Unauthorized Email Access:**
The presence of multiple email addresses linked to eBay officials, some with high verification scores, suggests a need for strict email access controls. Unauthorized access to these accounts could compromise sensitive information. Regular reviews of email access controls can mitigate this risk.

Vulnerability	Likelihood	Impact	Risk Value
Phishing Attacks	4	3	12
Email Spoofing	4	3	12
Lack of Email Encryption	3	3	9
Unauthorized Email Access	3	4	12

Table 3: Email Vulnerabilities Risk Score

7.3 Network Vulnerabilities

1. **DNSSEC Not Enabled:**
   DNS Security Extensions (DNSSEC) ensure the authenticity and integrity of DNS responses. When DNSSEC is not enabled, eBay's DNS infrastructure is vulnerable to DNS spoofing and cache poisoning, allowing attackers to redirect users to malicious sites. To address this risk, eBay should implement DNSSEC, ensuring all DNS responses are validated.

2. **Open Ports/Services:**
   Open ports and services on eBay's network can be exploited by attackers to gain unauthorized access or launch attacks. A comprehensive scan of the network should identify unnecessary open ports and services. Once identified, these should be closed or restricted to limit exposure.

3. **Weak Network Access Controls:**
   Weak access controls increase the risk of unauthorized access to sensitive network segments. This vulnerability can lead to data breaches and insider threats. eBay should enforce stricter access controls, using role-based access and multi-factor authentication to limit access to critical systems and data.

4. **Insider Threats:**
   Insider threats stem from employees or contractors with access to sensitive information. This can lead to data theft, sabotage, or unauthorized sharing of confidential data. Implementing robust network monitoring and controls can help detect and prevent insider threats. Regular audits of access controls and employee activities are recommended.

Vulnerability	Likelihood	Impact	Risk Value
DNSSEC Not Enabled	3	3	9
Open Ports/Services	4	3	12
Weak Network Access Controls	3	3	9
Insider Threats	4	4	16

Table 4: Network Vulnerabilities Risk Score

7.4 Third-Party Vulnerabilities

Third-party vulnerabilities refer to risks associated with using external plugins, services, or components that are not directly under eBay's control. Given the interconnected nature of modern e-commerce platforms, third-party risks can pose significant threats to eBay's security and operations.

1. **Third-party Plugins/Services:**
   Third-party plugins and services are commonly used to extend functionality, but they can introduce vulnerabilities into eBay's environment. These vulnerabilities can stem from outdated or insecure code, lack of regular security updates, or inadequate security practices by the third-party provider. Vulnerabilities in third-party plugins/services can lead to unauthorized access, data breaches, or even a complete compromise of eBay's systems. These risks can also impact eBay's compliance with industry regulations and lead to reputational damage. One such example of the previous vulnerabilities is CVE-2024-22307 which is a specific vulnerability that exposes a risk in third-party components or systems. This vulnerability, if exploited, can lead to unauthorized access, data loss, or service disruption. The criticality of this vulnerability depends on its impact on eBay's operations and data security.

Vulnerability	Likelihood	Impact	Risk Value
Third-party Plugins/Services	3	3	9

Table 5: Third-Party Vulnerabilities Risk Score

7.5 Reputation Vulnerabilities

Reputation vulnerabilities pose significant risks to eBay's brand image and financial stability. Two key areas where eBay must focus on reducing these vulnerabilities are legal issues and brand reputation damage.

1. **Legal Issues:**
   Legal issues arise from non-compliance with regulations or contractual obligations. Non-compliance can lead to fines, lawsuits, and reputational harm.

2. **Brand Reputation Damage**
   Brand reputation damage can result from negative publicity, customer dissatisfaction, or security incidents. The impact can lead to loss of customer trust and decreased business.

Vulnerability	Likelihood	Impact	Risk Value
Legal Issues	3	4	12
Brand Reputation Damage	3	5	15

Table 6: Reputation Vulnerabilities Risk Score

7.6 Infrastructure Vulnerabilities

Infrastructure vulnerabilities are risks within eBay's network and server infrastructure. These vulnerabilities can lead to unauthorized access, data loss, or system disruptions.

1. **Vulnerable Systems/Services Identified by Shodan.io:**
   Shodan.io is a search engine that identifies publicly exposed systems and services on the internet. Vulnerabilities found through Shodan.io can indicate that eBay's systems are accessible to unauthorized parties, posing significant security risks. Exposed systems can lead to unauthorized access, data theft, or service disruptions. Attackers may exploit these vulnerabilities to launch attacks or gain control over critical systems.[17][18]

2. **Inadequate Data Backup and Recovery Measures:**
   Data backup and recovery are critical for ensuring business continuity in the event of a security incident or system failure. Inadequate backup practices can lead to data loss and prolonged downtime. Without proper backup and recovery measures, eBay risks losing critical data, including customer information, transaction records, and other business-critical data. This can lead to reputational damage and legal issues.

Vulnerability	Likelihood	Impact	Risk Value
Vulnerable Systems Identified by Shodan.io	3	3	9
Inadequate Data Backup and Recovery	3	4	12

Table 7: Infrastructure Vulnerabilities Risk Score

7.7 Data Security Vulnerabilities

Data security vulnerabilities in eBay refer to potential weaknesses in how data is stored, accessed, and handled. These vulnerabilities can lead to data breaches, unauthorized access, and insider data theft.

1. **Insecure Data Storage:**
   Insecure data storage occurs when sensitive data, such as customer information or payment details, is not adequately protected. This can happen due to a lack of encryption, weak access controls, or improper data storage practices. If data is stored insecurely, it can lead to unauthorized access, data breaches, and legal consequences. Attackers could exploit these vulnerabilities to gain access to sensitive information, leading to reputational damage and regulatory penalties.

2. **Insider Data Theft**
   Insider data theft occurs when employees or contractors with authorized access misuse or steal sensitive information. This vulnerability can result from weak access controls or inadequate monitoring of employee activities. Insider data theft can lead to significant data breaches, loss of customer trust, and legal repercussions. This risk can be particularly damaging because insiders have authorized access to sensitive data.

Vulnerability	Likelihood	Impact	Risk Value
Insecure Data Storage	4	4	16
Insider Data Theft	4	4	16

Table 8: Data Security Vulnerabilities Risk Score

7.8 Payment Security Vulnerabilities

Payment security vulnerabilities encompass risks related to eBay's handling of payment card information and transaction processing. These vulnerabilities can lead to data breaches, fraudulent activities, and compliance issues.

1. **Payment Card Data Breaches:**
   Payment card data breaches occur when sensitive payment information, such as credit card numbers or CVV codes, is compromised. This can result from insecure payment systems, weak encryption, or unauthorized access. A breach in payment card data can lead to financial losses, identity theft, and significant reputational damage. eBay may also face regulatory penalties for failing to protect customer information.

2. **Fraudulent Transactions:**
   Fraudulent transactions occur when unauthorized parties manipulate payment processes to conduct unauthorized purchases or transfers. This can result from weak transaction verification, inadequate fraud detection systems, or insecure authentication methods. Fraudulent transactions can cause financial losses, damage customer trust, and lead to increased charge backs. This vulnerability can also impact eBay's compliance with financial regulations.

Vulnerability	Likelihood	Impact	Risk Value
Payment Card Data Breaches	4	5	20
Fraudulent Transactions	4	4	16

Table 9: Payment Security Vulnerabilities Risk Score

7.9 Mobile Application Vulnerabilities

Mobile application vulnerabilities are risks related to eBay's mobile apps, potentially leading to data breaches, unauthorized access, and user privacy violations.

1. **Insecure Mobile APIs:**
   Insecure mobile application programming interfaces (APIs) can expose eBay's mobile apps to unauthorized data access, allowing attackers to extract sensitive information. If mobile APIs are not secured, attackers can exploit them to steal user data or manipulate app functionality. This poses risks to user privacy and eBay's data security.

2. **Poor Session Management:**
   Poor session management occurs when mobile app sessions are not handled securely, allowing attackers to hijack sessions or gain unauthorized access to user accounts. Session hijacking can lead to unauthorized account access, data breaches, and fraudulent transactions. This can damage user trust and eBay's reputation.

Vulnerability	Likelihood	Impact	Risk Value
Insecure Mobile APIs	3	3	9
Poor Session Management	3	4	12

Table 10: Mobile Application Vulnerabilities Risk Score

7.10 Supply Chain Vulnerabilities

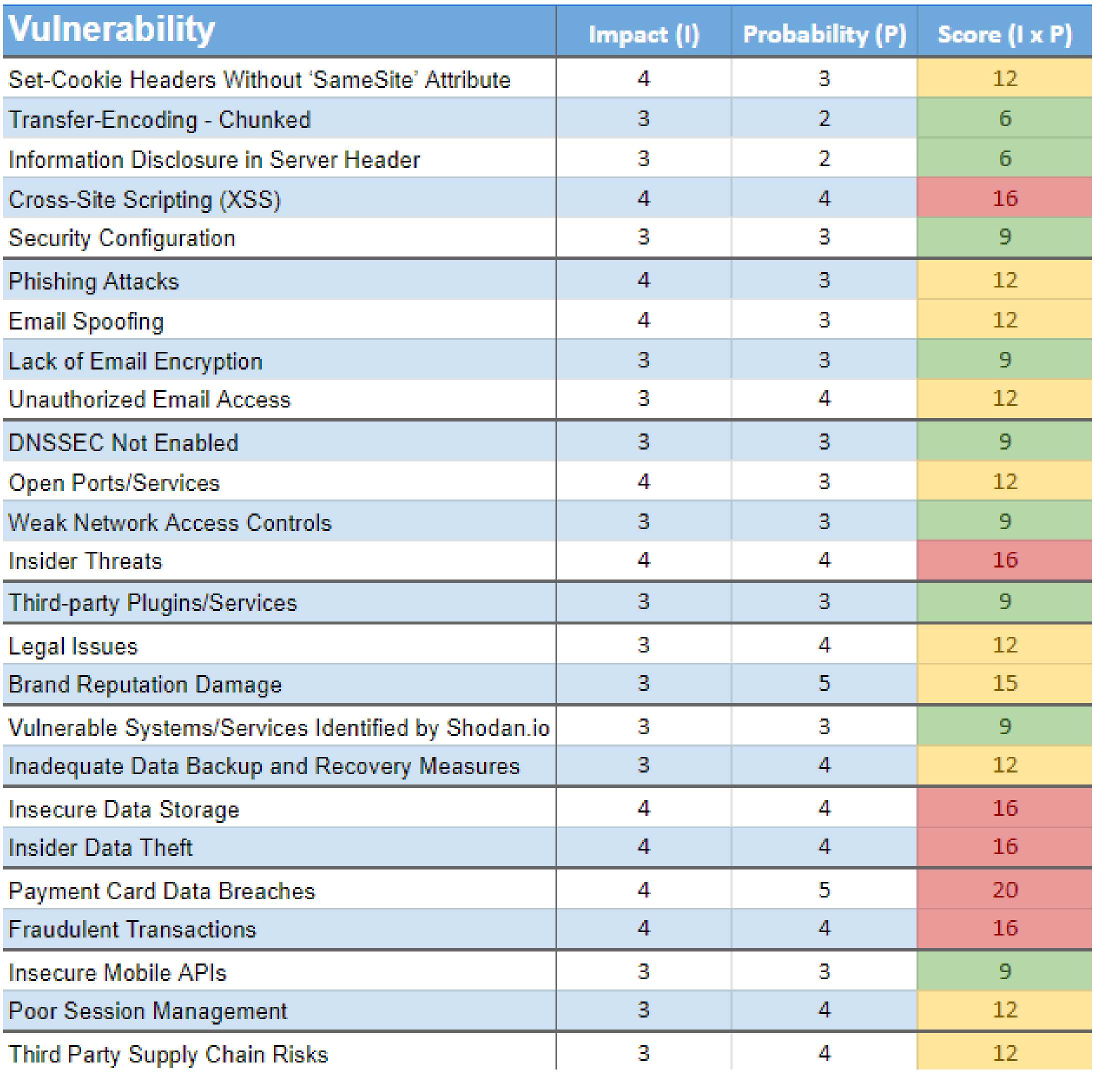
Supply chain vulnerabilities represent risks arising from third-party suppliers, vendors, and external service providers. These vulnerabilities can impact eBay's security posture, leading to data breaches, disruptions in service, or compliance issues.

1. **Third-party Supply Chain Risks:**
   Third-party supply chain risks occur when eBay's external suppliers or vendors have inadequate security practices. These risks can stem from insecure data handling, lack of security controls, or insufficient compliance measures. If a third-party supplier is compromised, it can lead to data breaches or service disruptions within eBay's ecosystem. This can affect customer data, e-commerce operations, and eBay's compliance with industry regulations.

Vulnerability	Likelihood	Impact	Risk Value
Insecure Mobile APIs	3	4	12

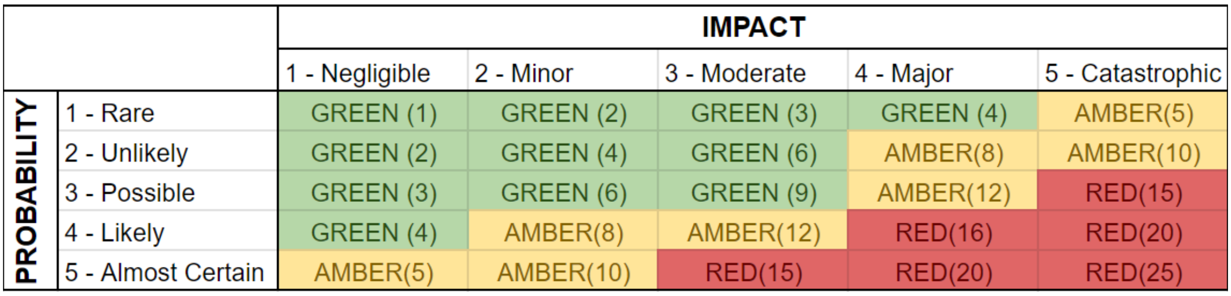
Table 11: Supply Chain Vulnerabilities Risk Score

8 PROBABILITY VS IMPACT MATRIX



Vulnerability	Impact (I)	Probability (P)	Score (I x P)
Set-Cookie Headers Without 'SameSite' Attribute	4	3	12
Transfer-Encoding - Chunked	3	2	6
Information Disclosure in Server Header	3	2	6
Cross-Site Scripting (XSS)	4	4	16
Security Configuration	3	3	9
Phishing Attacks	4	3	12
Email Spoofing	4	3	12
Lack of Email Encryption	3	3	9
Unauthorized Email Access	3	4	12
DNSSEC Not Enabled	3	3	9
Open Ports/Services	4	3	12
Weak Network Access Controls	3	3	9
Insider Threats	4	4	16
Third-party Plugins/Services	3	3	9
Legal Issues	3	4	12
Brand Reputation Damage	3	5	15
Vulnerable Systems/Services Identified by Shodan.io	3	3	9
Inadequate Data Backup and Recovery Measures	3	4	12
Insecure Data Storage	4	4	16
Insider Data Theft	4	4	16
Payment Card Data Breaches	4	5	20
Fraudulent Transactions	4	4	16
Insecure Mobile APIs	3	3	9
Poor Session Management	3	4	12
Third Party Supply Chain Risks	3	4	12

Figure 2: Risk Register



		IMPACT				
		1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
PROBABILITY	1 - Rare	GREEN (1)	GREEN (2)	GREEN (3)	GREEN (4)	AMBER(5)
	2 - Unlikely	GREEN (2)	GREEN (4)	GREEN (6)	AMBER(8)	AMBER(10)
	3 - Possible	GREEN (3)	GREEN (6)	GREEN (9)	AMBER(12)	RED(15)
	4 - Likely	GREEN (4)	AMBER(8)	AMBER(12)	RED(16)	RED(20)
	5 - Almost Certain	AMBER(5)	AMBER(10)	RED(15)	RED(20)	RED(25)

Figure 3: Master Risk Matrix

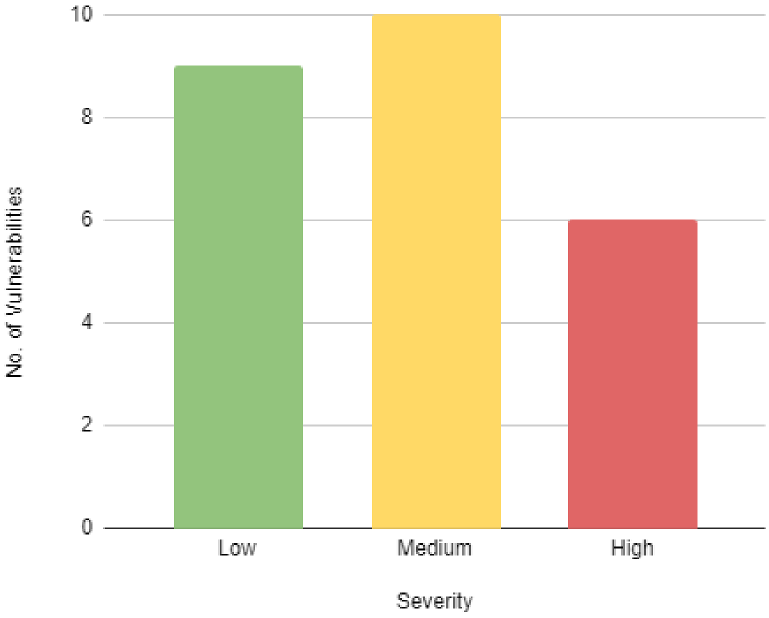


Figure 4: Total Severity Levels

9 TYPES OF CONTROLS

To ensure the protection of organizational assets, information, and systems against a myriad of potential threats and vulnerabilities, it becomes imperative to establish and maintain a robust framework of security controls. These controls, spanning across a spectrum of methodologies and technologies, are categorized into four fundamental pillars: Preventative measures, designed to thwart threats before they materialize; Detective controls, geared towards identifying and alerting about security breaches in real-time; Forensic measures, facilitating post-incident analysis and investigation to understand the nature and impact of security incidents; and Audit mechanisms, enabling continuous monitoring and evaluation of the security posture to ensure compliance and effectiveness. By integrating these diverse controls into a cohesive strategy, organizations can construct a formidable defense mechanism to mitigate risks and fortify their resilience against evolving cyber threats.

9.1 Preventative

Preventative controls are designed to stop security incidents before they occur. They are proactive measures intended to prevent unauthorized access, data breaches, and other security threats. These controls include strong authentication methods, such as multi-factor authentication, which ensure that only authorized users can access sensitive systems and information. Additionally, firewalls and intrusion prevention systems (IPS) are employed to filter out unauthorized or potentially harmful traffic before it can enter the network. Regular software updates and patches also play a crucial role in closing vulnerabilities that could be exploited by attackers.

9.2 Detective

Detective controls are essential for identifying and signaling the occurrence of a security event. These controls come into play during or after an incident to ensure that threats are detected in a timely manner. They include intrusion detection systems (IDS), which monitor network traffic for suspicious activity and anomalies that may indicate a breach or an attack. Log management tools and security information and event management (SIEM) systems are also used to aggregate and analyze logs from various sources within the organization, helping to uncover patterns that might signify malicious activities.

9.3 Forensic

Forensic controls are focused on providing methods and tools for capturing and analyzing information about past security incidents. This analysis helps in understanding how the breach occurred and in identifying the perpetrators. These controls include digital forensic tools and techniques designed to collect, preserve, and analyze data from computer systems, networks, and storage devices in a way that maintains the integrity of the evidence. Forensic controls are critical for legal proceedings and for improving the organization's security posture by learning from past incidents.

9.4 Audit

Audit controls involve the regular review and examination of records and activities to ensure compliance with established policies and procedures. They are essential for verifying that the other controls are functioning correctly and are effective in mitigating security risks. Audit controls include both automated systems and manual checks that perform regular audits on various aspects of the IT infrastructure. This includes access logs, permission settings, and other security configurations. Internal or external audits are also conducted to ensure compliance with legal, regulatory, and internal standards.

10 LIST OF CONTROLS

In establishing a robust cybersecurity framework for eBay, it's essential to utilize a categorized control system that addresses the various layers of security needs. These controls are organized into different groups according to their primary functionality and effectiveness, ranging from direct threat mitigation to compliance and investigative measures. Each type of control plays a pivotal role in fortifying eBay's defenses against a myriad of cybersecurity challenges.

The first sheet, "Controls List"[19], details specific security controls eBay implements, such as Web Application Firewalls (WAF) and Multi-Factor Authentication (MFA), and categorizes them based on their effectiveness—from most to moderately effective. This sheet is instrumental in understanding the direct actions eBay is taking to secure its digital landscape against potential cyber threats. The second sheet, "Vulnerability List"[20], identifies key vulnerabilities within eBay's system, such as Cross-Site Scripting (XSS) and Insider Threats, and maps out the controls(Preventative, Detective, Forensic, and Audit) that address these vulnerabilities. This sheet provides a comprehensive view of how specific controls correlate with the vulnerabilities they are designed to mitigate.

The controls are color-coded in an Excel sheet to highlight their function: Blue is used for preventative measures that aim to stop threats before they occur, red denotes detective controls designed to identify and alert on breaches, green signifies forensic controls which are crucial for investigating and analyzing post-incident data and yellow is used for audit controls that ensure compliance and operational integrity.

This strategic categorization and color-coding facilitate easier management and a clearer understanding of how each control contributes to overall security objectives. By implementing such a layered and color-coordinated approach, eBay can ensure comprehensive coverage of security measures, addressing vulnerabilities effectively and maintaining a robust defense against potential cyber threats.

10.1 Most Effective Controls

These controls directly address high-impact technical vulnerabilities and threats that can lead to significant security breaches. They are designed to mitigate risks from the most damaging types of attacks, such as unauthorized access and data breaches, which have direct financial, operational, and reputational consequences. These controls are both preventative and active in nature, often operating continuously to defend key assets.

10.1.1 Application of Web Application Firewalls (WAF) and XSS Filters

[Preventative Control][Technical]
Web Application Firewalls (WAF) are designed to protect web applications by monitoring and filtering HTTP traffic between a web application and the Internet. WAFs are deployed to establish a protective barrier against malicious attempts to exploit web applications. For eBay, which is an extensive online marketplace involving numerous transactions and data exchanges daily, implementing WAFs is crucial. WAFs can dynamically detect and block malicious requests that could exploit vulnerabilities in the application, thus protecting both the data and integrity of eBay's operations.

XSS Filters are used to detect and mitigate Cross-Site Scripting (XSS) attacks where malicious scripts are injected into otherwise benign and trusted websites. By implementing XSS Filters, eBay can prevent the execution of malicious scripts that may be injected via user inputs, thus safeguarding user data and enhancing the security of user sessions on eBay's platform.

Here is a list of Vulnerabilities Addressed by this Control:

- **Information Disclosure in Server Header:** This vulnerability involves the potential exposure of sensitive information through HTTP headers, which can reveal details about the underlying server software and its configuration to an attacker. By using WAF, eBay can customize and minimize the information available in the server headers, reducing the risk of targeted attacks by obscuring details about the server's software and setup.

- **Cross-Site Scripting (XSS):** XSS attacks involve injecting malicious scripts into web pages viewed by other users, which can steal cookies, session tokens, or other sensitive information that leads to identity theft or session hijacking. For eBay, XSS Filters integrated within the WAF can automatically detect and neutralize such malicious scripts before they render in the user's browser, thereby protecting both the users and the integrity of eBay's web pages.

10.1.2 Multi-Factor Authentication (MFA)

[Preventative Control][Technical]
Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to gain access to a resource, such as an online account, a computing device, or a network.[21] MFA combines two or more independent credentials: what the user knows (password), what the user has (security token), and what the user is (biometric verification). At eBay, implementing MFA means adding an extra layer of protection against unauthorized access to user accounts and sensitive company data. This not only helps secure customer and seller accounts but also enhances the security of the internal systems accessed by eBay employees.

Here is a list of Vulnerabilities Addressed by this Control:

- **Unauthorized Email Access:** Unauthorized access to email accounts can lead to data breaches, phishing attacks, and other malicious activities. For eBay, securing email accounts is crucial as they contain sensitive communications related to transactions, customer data, and business operations. MFA can significantly decrease the risk of such unauthorized access by ensuring that the entity attempting access has multiple ways to prove its identity.

- **Weak Network Access Controls:** Weak network access controls can expose eBay to potential intrusions, where unauthorized individuals could gain access to the network and the data flowing through it. MFA strengthens these controls by requiring additional authentication steps beyond just a username and password, thereby reducing the risk of unauthorized network access.

- **Insider Threats:** Insider threats involve malicious actions by employees or contractors who have inside information about the company's security practices and data. By implementing MFA, eBay can mitigate these risks by making it more difficult for insiders to misuse their access privileges, as they would need to authenticate through multiple layers of security.

- **Poor Session Management:** Poor session management can lead to sessions being hijacked, where an attacker takes over a user session after the user has authenticated. MFA can be used to regularly re-authenticate users during sessions, especially when accessing sensitive parts of the system, thus reducing the chance of session hijacking.

10.1.3 Validate and Sanitize All Inputs

[Preventative Control][Technical]
Validation and sanitization of all inputs is a fundamental security measure that ensures only properly formatted data is accepted through the user interfaces or API endpoints of an application. eBay processes countless transactions and user interactions daily, and implementing stringent input validation and sanitization protocols helps prevent malicious data from causing harm. This control is integral to the security architecture, mitigating risks by examining all incoming data for potential threats before processing.

Here is a list of Vulnerabilities Addressed by this Control:

- **Cross-Site Scripting (XSS):** By rigorously validating and sanitizing user inputs, we can prevent attackers from embedding malicious scripts into pages that are viewed by other users. This is crucial for preventing XSS, where attackers exploit input fields to inject scripts that can hijack user sessions or steal sensitive information.

- **Vulnerabilities in Third-party Plugins/Services:** Third-party plugins often introduce security risks. By sanitizing inputs, eBay can limit the data that these plugins process, thereby mitigating potential exploits that leverage input data to attack underlying systems or software.
- **Insider Data Theft:** Effective input validation helps prevent insiders from injecting malicious data that could facilitate data theft, such as commands that could expose sensitive data through illicit queries or operations within the systems.

10.1.4 Use of Encryption and Secure Communication Protocols

[Preventative Control][Technical]
Encryption and secure communication protocols are critical tools for safeguarding sensitive data transmitted across networks[22]. In the context of eBay, which handles millions of transactions and communications daily, implementing robust encryption methods (like SSL/TLS for data in transit) and secure communication protocols ensures that all data exchanges are encrypted. This protects against eavesdropping and unauthorized access during transmission.

Here is a list of Vulnerabilities Addressed by this Control:

- **Lack of Email Encryption:** Without email encryption, sensitive information sent via emails can be intercepted and read by unauthorized parties. For eBay, this could include confidential business information or user data, leading to privacy violations and loss of trust. By applying email encryption protocols such as PGP or S/MIME, eBay can ensure that all email content is securely encrypted. This not only protects user data but also secures communication between eBay and its partners or customers.
- **Insecure Data Storage:** Insecure storage of data, especially on cloud services or databases, can lead to unauthorized access and data breaches. This risks user data, including account details and financial information. Encryption of stored data (at rest) using AES or similar encryption standards can prevent unauthorized access to eBay's data stores, ensuring that even if the storage medium is compromised, the data remains unreadable.
- **Payment Card Data Breaches:** As a major online marketplace, eBay processes numerous payment transactions daily. Payment card data breaches can lead to financial loss for users and severe reputational damage for eBay. Using end-to-end encryption for payment data and adhering to PCI-DSS requirements can help secure card transactions over eBay's platforms. This minimizes the risk of payment card data being accessed or stolen during the transaction process.
- **Insecure Mobile APIs:** Implementing SSL/TLS for data transmitted via mobile APIs and ensuring robust authentication and encryption protocols are in place can mitigate these risks, safeguarding mobile transactions and user interactions on eBay's mobile platform.

10.1.5 Implementation of SameSite Cookie Attribute and Secure Headers

[Preventative Control][Technical]
This involves configuring cookies with the SameSite attribute to enhance security against cross-site request forgery (CSRF) attacks. By setting the SameSite attribute to either Lax or Strict, cookies are not sent with cross-site requests, which helps mitigate the risk of CSRF attacks. Additionally, secure headers such as Content-Security-Policy, X-Content-Type-Options, and X-Frame-Options are implemented to provide further security enhancements. Implementing this control will involve updating the web servers and application frameworks to automatically include these attributes and

headers in HTTP responses. This can be managed through eBay's existing web development and operations teams, ensuring that all new and existing cookies adhere to this policy and that secure headers are consistently applied across all web properties.

Here is a list of Vulnerabilities Addressed by this Control:

- **Set-Cookie Headers Without 'SameSite' Attribute:** Without the SameSite attribute, cookies are potentially sent with requests initiated by third-party websites. This could allow attackers to leverage CSRF attacks, where unauthorized commands are transmitted from a user that the web application trusts. For an e-commerce giant, the impact of such attacks could be significant, potentially leading to unauthorized transactions or data breaches. By implementing the SameSite cookie attribute, we can significantly reduce the risk of CSRF attacks. The attribute ensures that cookies are not sent with cross-origin requests, thereby preventing attackers from leveraging eBay's cookies in unauthorized cross-site requests.

10.1.6 Enforcement of Access Controls and User Authentication

[Preventative Control][Technical]

This involves the implementation and maintenance of robust access controls and user authentication mechanisms within eBay's IT infrastructure. This includes requiring strong, multi-factor authentication for accessing sensitive systems and data, setting up strict role-based access controls that limit user permissions based on job responsibilities, and continuously monitoring and reviewing access logs to detect and respond to unauthorized access attempts[23]. This control is designed to ensure that only authorized personnel can access specific data and systems, which is crucial in a large, globally distributed organization like eBay.

Here is a list of Vulnerabilities Addressed by this Control:

- **Unauthorized Email Access:** Unauthorized email access can lead to data breaches, exposing sensitive corporate information or personal data of users and employees. Such breaches can result in financial loss, legal consequences, and damage to eBay's reputation. By enforcing strong user authentication, eBay ensures that access to email systems requires more than just a password, potentially incorporating elements like biometrics or security tokens. Access controls ensure that employees can only access the information necessary for their role, reducing the risk of information being accessed by someone inside the company who does not have a legitimate need for access.

- **Weak Network Access Controls:** Weak network access controls can allow attackers easy entry into the network, leading to potential manipulation or theft of sensitive data. This could compromise buyer and seller information, transaction details, and proprietary business data. he implementation of stringent access controls and authentication ensures that only authorized devices and users can connect to eBay's network.

- **Insider Threats:** Insider threats involve malicious actions by employees or contractors, such as theft or sabotage. Due to the nature of eBay's business, which includes handling large volumes of transactions and sensitive user data, insider threats can pose significant risks. Strong access controls limit the potential damage an insider could do by ensuring they can only access systems and data relevant to their job function.

10.1.7 Implementing Content Security Policy (CSP)

[Preventative Control][Technical]

Content Security Policy (CSP) is a security standard introduced to prevent common attacks such as cross-site scripting (XSS), clickjacking, and other code injection attacks originating from malicious content injected into trusted web pages.[24] eBay can implement CSP by specifying security policies in HTTP headers to dictate which dynamic resources are allowed to load, thereby minimizing the risk of XSS attacks and data leaks.

Here is a list of Vulnerabilities Addressed by this Control:

- **Information Disclosure in Server Header:** This vulnerability involves the potential for attackers to gain information about the backend systems of a web application from the HTTP headers. Such information could help attackers tailor further attacks. CSP helps mitigate this by restricting how and where resources can load, reducing the risk of information being inadvertently disclosed.

- **Cross-Site Scripting (XSS):** XSS attacks occur when malicious scripts are injected into otherwise benign and trusted websites, which can affect eBay users by executing scripts in the user's browser that can hijack user sessions or deface website interfaces. Implementing CSP on eBay reduces this risk by specifying which scripts are allowed to run and from where they can be loaded, preventing unauthorized scripts from executing.

10.1.8 Vendor Risk Management and Secure Procurement Processes

[Preventative Control][Non-Technical]

Vendor Risk Management and Secure Procurement Processes involve a comprehensive approach to assessing and mitigating risks presented by third-party vendors and suppliers. For eBay, this control is crucial due to its heavy reliance on various third-party services and plugins for operational functionality and marketplace services. Implementing stringent procurement processes ensures that all third-party services comply with eBay's security standards before integration. Here is a list of Vulnerabilities Addressed by this Control:

- **Vulnerabilities in Third-party Plugins/Services:** Third-party plugins/services can introduce vulnerabilities due to insufficient oversight or control over the security measures taken by the vendors. These vulnerabilities can expose eBay to data breaches, service disruptions, and other security incidents.

- **Supply Chain Vulnerabilities:** Supply chain vulnerabilities can similarly lead to significant disruptions and compromises in service integrity. eBay mitigates these risks by employing thorough vetting processes, regular security assessments, and enforcing strict security requirements for all suppliers and third-party services. This approach not only minimizes the risk of introducing vulnerabilities into eBay's ecosystem but also ensures compliance with industry security standards and regulations.

10.1.9 Patch Management Systems

[Preventative Control][Technical]

Patch Management Systems are vital for maintaining the security of software by ensuring that all systems are up-to-date with the latest security patches and updates[25]. At eBay, implementing a robust patch management system can automate the process of deploying patches across various technologies used by the company, thereby reducing the window of vulnerability and minimizing manual errors.

Here is a list of Vulnerabilities Addressed by this Control:

- **Security Configuration:** Misconfigurations can leave systems exposed to attacks. A patch management system ensures that configurations are updated alongside software patches, which often include enhancements to security settings. This proactive measure helps prevent potential breaches that exploit outdated configurations.

- **Vulnerabilities in Third-party Plugins/Services:** eBay relies on numerous third-party plugins and services, which can introduce vulnerabilities if not properly managed. Patch management systems ensure that these components are regularly updated, closing vulnerabilities that could be exploited by attackers and thus maintaining the integrity of service offerings.

- **Insecure Mobile APIs:** As eBay provides services accessible via mobile devices, securing APIs becomes crucial. Patch management systems play a critical role in applying security updates that fix vulnerabilities in the APIs. This is particularly important to protect against data leakage and unauthorized access through mobile platforms.

10.1.10 Secure Configuration Management

[Preventative Control][Technical]
Secure Configuration Management involves establishing and maintaining the security of systems and applications through rigorous configuration controls[22]. For eBay, this entails defining security settings and policies tailored to protect against specific threats, ensuring all systems are set up correctly, and that any changes are systematically managed to prevent security lapses.

Here is a list of Vulnerabilities Addressed by this Control:

- **Security Configuration:** Poor security configuration can expose the organization to a variety of threats including unauthorized access and data breaches. By implementing secure configuration management, we ensures that all systems are configured to the highest security standards, reducing the risk of exploitable vulnerabilities.

- **Inadequate Data Backup and Recovery Measures:** Without adequate data backup and recovery measures, eBay risks significant data loss in the event of system failures or cyber attacks, which could disrupt operations and erode user trust. Secure configuration management includes robust backup and recovery procedures, ensuring that data is regularly backed up and can be quickly restored, minimizing downtime and data loss.

- **Insider Data Theft:** Insider threats, including data theft by employees, are a critical security challenge. Such actions can lead to significant data breaches and financial loss. This control helps in setting up strict access controls and monitoring configurations, which limits access to sensitive data and alerts eBay to any unauthorized attempts to access or manipulate data internally.

10.1.11 Regular Penetration Testing and Vulnerability Scanning

[Detective Control][Technical]
Regular penetration testing and vulnerability scanning involve systematic checks to identify and fix security weaknesses in an organization's IT infrastructure. This means routinely scanning their web applications, servers, and network devices to discover vulnerabilities that could be exploited by attackers. This process not only identifies security weaknesses but also helps in validating the effectiveness of the existing security measures.

Here is a list of Vulnerabilities Addressed by this Control:

- **Set-Cookie Headers Without ‘SameSite’ Attribute:** Lack of the ’SameSite’ attribute in set-cookie headers can make eBay vulnerable to cross-site request forgery (CSRF) attacks, potentially leading to unauthorized actions on behalf of a logged-in user. Regular scans can identify and recommend the enforcement of ’SameSite’ attributes in cookies, thereby reducing the risk of CSRF attacks.

- **Transfer-Encoding - Chunked Information Disclosure:** This vulnerability could allow attackers to obtain sensitive information from eBay’s servers by exploiting how they process chunked transfer encoding. Through penetration testing, we can detect improper handling of chunked encoding and patch it to prevent information leakage.

- **DNSSEC Not Enabled:** Without DNSSEC, DNS responses could be susceptible to tampering, leading to redirected traffic and potentially exposing users to phishing sites. Regular scanning can highlight the lack of DNSSEC and facilitate its implementation to ensure DNS integrity and trustworthiness.

- **Open Ports/Services:** Unnecessary open ports can provide attackers with potential entry points to exploit vulnerabilities in the network services. Penetration testing can identify and recommend the closure or securing of open ports that are not needed for eBay’s business operations.

- **Vulnerabilities in Third-party Plugins/Services:** Third-party components can contain vulnerabilities that might compromise the security of eBay’s entire platform. Routine vulnerability scanning can detect outdated or vulnerable third-party plugins and services, prompting timely updates or replacements.

- **Vulnerable Systems/Services Identified by Shodan.io:** Systems identified by Shodan.io as vulnerable could be targeted by attackers. Regular scans can identify what is publicly exposed and vulnerable, allowing eBay to mitigate these risks by securing the systems.

- **Insecure Data Storage:** Inadequately secured data can lead to unauthorized access and data breaches. Penetration tests can help identify insecure data storage practices and suggest improvements to secure data effectively.

10.2 Highly Effective Controls

These controls provide a robust defense against a variety of common and potentially severe attacks but might not address the most critical vulnerabilities by themselves. They are vital for reinforcing the security framework and reducing the attack surface.

10.2.1 Email Filtering

[Preventative Control][Technical]
Email Filtering involves the use of automated software tools to inspect incoming emails to an organization’s mail servers, checking for signs of spam, phishing, spoofing, and other malicious content. This control can be utilized to inspect all incoming and outgoing emails to ensure they are from legitimate sources and do not contain harmful links or attachments. It uses criteria like sender reputation, keywords, and attachment scanning to block or flag suspicious emails.

Here is a list of Vulnerabilities Addressed by this Control:

- **Phishing Attacks:** Phishing attacks can deceive eBay employees into revealing sensitive information, such as login credentials or financial information, which could compromise both user accounts and internal systems. Email filtering systems at eBay can detect and quarantine emails that exhibit characteristics of phishing, such as deceptive links or suspicious sender addresses, before they reach the end user, thus reducing the likelihood of successful phishing attacks.
- **Email Spoofing:** Email spoofing could be used to impersonate eBay's branding to mislead customers or employees, potentially damaging eBay's reputation and trust. By implementing email filtering, we can prevent spoofed emails from being delivered by verifying the authenticity of the sender's domain using techniques like SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail).
- **Unauthorized Email Access:** Unauthorized access to email accounts can lead to data breaches, leaking sensitive corporate and customer data. Email filtering helps to detect unusual access patterns and potentially harmful content that could be used to exploit email account vulnerabilities, thereby protecting the integrity of email communications at eBay.

10.2.2 Implementation of Secure Backup and Recovery Solutions

[Preventative Control][Technical]
This control involves deploying robust solutions for backing up data and ensuring it can be effectively recovered in case of loss. At eBay, implementing secure backup and recovery solutions means maintaining continuity of service and safeguarding transactional data integrity. This is accomplished through regular backups of data, testing the recoverability of such data, and using secure and redundant storage locations to minimize the risk of data loss.

Here is a list of Vulnerabilities Addressed by this Control:

- **Inadequate Data Backup and Recovery Measures:** Without adequate backup and recovery measures, eBay risks losing critical operational and customer data in the event of system failures, cyber-attacks, or natural disasters. This vulnerability could disrupt operations, erode user trust, and potentially lead to significant financial and reputational damage. By implementing secure backup and recovery solutions, the organization ensures that data is not only backed up regularly but also recoverable in a secure and timely manner. This approach mitigates risks associated with data loss and supports business continuity and compliance with data protection regulations.

10.2.3 Intrusion Prevention Systems

[Preventative Control][Technical]
Intrusion Prevention Systems (IPS) are network security technologies that monitor network and system activities for malicious activity. An IPS operates by performing real-time packet inspection, deeply analyzing the contents and context of the network traffic. Upon detecting suspicious activity, the system can automatically block or prevent such activities by acting on predefined security policies. Here is a list of Vulnerabilities Addressed by this Control:

- **Cross-Site Scripting (XSS):** XSS can allow attackers to inject malicious scripts into eBay's web pages viewed by users, potentially leading to unauthorized access to user data and accounts. IPS systems on eBay can be configured to detect and block traffic that contains XSS attack signatures, preventing the execution of such scripts before they reach user browsers.

- **Open Ports/Services:** Open ports can act as entry points for attackers, possibly leading to unauthorized access or denial-of-service attacks. By monitoring and controlling the data that travels through these ports, IPS helps eBay in automatically detecting and blocking access attempts or traffic from suspicious sources, thus safeguarding against exploitation.

- **Insider Threats:** Employees with malicious intent or compromised accounts pose a significant risk, potentially leading to data theft or system sabotage. IPS can help mitigate this risk by monitoring and analyzing behavior patterns of network traffic, thus detecting and responding to abnormal activities that could indicate an insider threat.

- **Vulnerable Systems/Services Identified by Shodan.io:** Systems and services exposed and identified by tools like Shodan.io can be targeted by attackers. IPS can assist in mitigating these vulnerabilities by providing automated responses to recognized threats directed at these exposed systems, further enhancing the security posture of eBay against external scans and attacks.

10.2.4 Intrusion Detection Systems

[Detective Control][Technical]
Intrusion Detection Systems (IDS) are essential security tools that monitor network and system traffic for malicious activities and policy violations. An IDS can be strategically deployed to scrutinize all incoming and outgoing traffic. This system will be configured to alert security personnel of suspicious activities, allowing for immediate investigation and response, thus forming a critical layer of eBay's cyber defense strategy.

Here is a list of Vulnerabilities Addressed by this Control:

- **Cross-Site Scripting (XSS):** IDS at eBay could be configured to detect unusual outbound traffic or unauthorized data retrievals, which are indicators of XSS exploitation. By recognizing these patterns, the IDS can alert security teams to block these scripts and protect users' sessions.

- **Open Ports/Services:** IDS can continuously monitor and analyze network traffic to identify unexpected or unauthorized communications on open ports. This helps in quickly shutting down these vulnerabilities before they can be exploited.

- **Insider Threats:** Insiders, such as employees or contractors, might misuse their access rights, leading to data theft or system sabotage. The IDS at eBay would be crucial for detecting irregular access patterns or unusual data transmissions that might suggest insider threats, thereby enabling preemptive action to mitigate these risks.

- **Vulnerabilities in Third-party Plugins/Services:** By monitoring the behavior and traffic associated with third-party integrations, eBay's IDS can detect and alert on anomalies that may indicate exploitation of these vulnerabilities.

10.2.5 Enhanced Transaction Verification and Behavior Analysis

[Detective Control][Technical]
Enhanced Transaction Verification and Behavior Analysis involves using advanced techniques to verify the legitimacy of transactions and analyze behavior patterns for signs of fraud. This control can be implemented using machine learning models that evaluate each transaction in real-time, comparing it against known patterns of legitimate and fraudulent activities. eBay can integrate this

system into its transaction processing infrastructure to automatically flag or block transactions that show signs of fraud.

Here is a list of Vulnerabilities Addressed by this Control:

- **Payment Card Data Breaches:** Payment card data breaches can lead to unauthorized access to customer payment information, resulting in financial losses for customers and reputational damage for eBay. By using enhanced transaction verification, eBay can detect unusual transaction patterns that may indicate a breach. This proactive detection helps in minimizing the damage by identifying and addressing security breaches swiftly.

- **Fraudulent Transactions:** Fraudulent transactions can lead to direct financial losses for sellers and damage trust in eBay's marketplace. Behavior analysis helps eBay identify and prevent fraudulent transactions by recognizing abnormal purchasing behaviors, such as buying large quantities of high-value items in a short period. This control reduces the incidence of fraud by blocking suspicious transactions before they are completed.

10.2.6 Firewalls

[Preventative Control][Technical]
Firewalls act as a barrier between a trusted network and untrusted networks. A firewall can be hardware, software, or a combination of both. Its primary function is to control incoming and outgoing network traffic by analyzing data packets and determining whether they should be allowed through or not based on a predetermined security rule set.

Here is a list of Vulnerabilities Addressed by this Control:

- **Cross-Site Scripting (XSS):** XSS attacks can allow attackers to inject malicious scripts into eBay's webpages, which are then executed by the browser of any user viewing the webpage. This can lead to unauthorized access to user sessions and personal data. Although primarily a task for more specific web application firewalls (WAFs), these specialized firewalls can inspect HTML data and actively block suspicious content that may contain XSS scripts, thereby reducing the risk of such attacks.

- **Phishing Attacks:** Phishing attacks often involve deceptive emails or websites that mimic eBay's genuine interface to trick users into providing sensitive information. These attacks can lead to identity theft and financial fraud. Firewalls equipped with capabilities to scan and filter out potentially harmful inbound emails can reduce the incidence of phishing attacks by blocking malicious emails and links before they reach the users.

- **Open Ports/Services:** Unnecessary open ports and services on network devices can provide attackers with potential entry points into eBay's network, leading to unauthorized access and data breaches. Firewalls are configured to close all ports that are not required for the business operations of eBay, thereby minimizing the attack surface and enhancing the overall security posture of the network.

- **Vulnerabilities in Third-party Plugins/Services:** hird-party plugins and services can contain vulnerabilities that, if exploited, could compromise the security of eBay's platforms and data. These vulnerabilities can be a gateway for several types of cyber-attacks. Firewalls can restrict and monitor traffic between eBay's servers and third-party services. By enforcing strict security rules, firewalls can help prevent the exploitation of known vulnerabilities in these external components.

10.2.7 Network Segmentation

[Preventative Control][Technical]
Network segmentation involves dividing a computer network into subnetworks, each being a network segment or a subnet, to enhance security and performance[26]. For an e-commerce giant, network segmentation can be crucial for isolating critical infrastructure and sensitive data from less secure areas of the network. By implementing network segmentation, eBay can restrict access to important areas, ensuring that a breach in one segment doesn't compromise the entire network.

Here is a list of Vulnerabilities Addressed by this Control:

- **Open Ports/Services:** Network segmentation limits the exposure of open ports and services to unauthorized users. By segregating the network, we can ensure that only necessary ports and services are accessible within a segment and not exposed to the entire network, reducing the risk of exploitation from external threats and unauthorized access.
- **Weak Network Access Controls:** Implementing network segmentation strengthens network access controls by enforcing strict rules that govern inter-segment traffic. This approach will allow to enforce more granular control over who can access specific network resources, thereby tightening security and reducing the possibility of unauthorized access.
- **Insider Threats:** Segmentation of the network limits the access insiders have to sensitive information and critical infrastructure. By using network segmentation, eBay can effectively compartmentalize access to different parts of the network, ensuring that insiders can only reach the systems necessary for their role, which significantly mitigates the risk posed by insider threats.
- **Vulnerable Systems/Services Identified by Shodan.io:** Systems and services that are publicly identified as vulnerable on platforms like Shodan.io can be isolated within their network segments. This prevents potential attackers from exploiting these vulnerabilities to gain broader access to eBay's network. By keeping vulnerable systems contained within secure segments, eBay can also prioritize and manage security patches more effectively.

10.3 Moderately Effective Controls

These controls are crucial for ongoing security management and for addressing vulnerabilities that may not pose an immediate critical threat but are still essential to manage. They focus on detection and ongoing management of the security posture.

10.3.1 Regular Vulnerability Assessments

[Detective Control][Technical]
Regular Vulnerability Assessments involve a systematic review of eBay's security infrastructure to identify and prioritize vulnerabilities. By using automated tools and manual testing methods, eBay can regularly monitor its systems for any security discrepancies and newly emerging threats. This process will allow eBay to maintain a high security posture by proactively addressing potential security weaknesses before they can be exploited.

Here is a list of Vulnerabilities Addressed by this Control:

- **Security Configuration:** Regular assessments help ensure that all security configurations are up-to-date and configured according to the latest security best practices. This control is crucial for eBay, as it helps prevent unauthorized access and data breaches by continuously monitoring for misconfigurations or outdated security settings that could expose the company to cyber attacks.

- **Supply Chain Vulnerabilities:** This control helps mitigate risks associated with third-party vendors and suppliers by assessing their security practices and controls. Regular vulnerability assessments allow eBay to evaluate the security posture of its supply chain partners, ensuring that vulnerabilities in their systems do not compromise the overall security of eBay's operations.

10.3.2 Security Information and Event Management (SIEM)

[Detective Control][Technical]
Security Information and Event Management (SIEM) is a comprehensive security management tool that aggregates and analyzes activity from many different resources across your entire IT infrastructure. SIEM can be used to monitor, detect, and alert on potential security incidents by collecting and correlating logs from various parts of the network, such as email systems, network traffic, and transaction logs.

Here is a list of Vulnerabilities Addressed by this Control:

- **Unauthorized Email Access:** SIEM systems in eBay can be configured to monitor and analyze log data from email servers and clients for unusual access patterns, such as access from unauthorized locations or at unusual times. This can help in detecting and alerting security personnel about potential unauthorized email access attempts, enabling timely remediation actions to prevent data breaches.

- **Weak Network Access Controls:** By integrating SIEM with network access control systems, eBay can achieve enhanced visibility into network traffic and user behaviors. SIEM can identify and alert on anomalies or deviations from established network access policies, such as unauthorized access attempts to sensitive areas of the network, thus strengthening overall network security.

- **Insider Threats:** SIEM's ability to aggregate and analyze logs from all across eBay's IT infrastructure makes it an excellent tool for detecting potential insider threats. By setting up baselines of normal user activities, SIEM can flag unusual patterns such as large data transfers or access to sensitive data outside of normal working hours, which are indicators of insider threats.

- **Fraudulent Transactions:** SIEM can be particularly effective in identifying patterns that indicate fraudulent transactions. By continuously monitoring and analyzing transaction logs and correlating them with user account activities and external threat data, SIEM can help detect and prevent fraud by triggering alerts for transactions that deviate from typical user patterns or involve known fraudulent entities.

10.3.3 Implement and Enforce DNSSEC

[Preventative Control][Technical]
Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. eBay can implement and enforce DNSSEC to enhance security by ensuring that the DNS records such as IP addresses associated with domain names are authentic and have not been tampered with. DNSSEC operates by adding digital signatures to the data, allowing a DNS resolver to verify its validity. By enforcing DNSSEC, we can prevent

attackers from exploiting vulnerabilities related to DNS data, ensuring integrity and trust across its digital presence.

Here is a list of Vulnerabilities Addressed by this Control:

- **DNSSEC Not Enabled:** The primary vulnerability addressed by this control is the lack of DNSSEC (DNSSEC Not Enabled), which leaves DNS data susceptible to DNS spoofing and cache poisoning attacks. By enabling and enforcing DNSSEC, eBay mitigates these risks by validating the authenticity of the DNS data. This control helps protect users from being redirected to malicious sites, thereby safeguarding user data and maintaining service integrity.

10.3.4 Continuous Monitoring and Threat Intelligence

[Detective Control][Technical]
Continuous Monitoring and Threat Intelligence involves the ongoing observation and analysis of an organization's digital environment to detect, analyze, and respond to potential security threats. This means implementing systems that continuously scan for anomalies or signs of malicious activity across its network, systems, and applications. This control utilizes advanced algorithms and threat intelligence feeds to identify emerging threats or suspicious behavior in real time.

Here is a list of Vulnerabilities Addressed by this Control:

- **Unauthorized Email Access:** Continuous monitoring can detect unusual access patterns or locations, triggering alerts. eBay can use this control to quickly identify and respond to unauthorized email accesses, reducing the risk of information theft or leakage.

- **Open Ports/Services:** By continuously scanning for and identifying open ports or unnecessary services running on eBay's network, this control helps ensure that only essential ports are open, thereby minimizing the attack surface.

- **Weak Network Access Controls:** Continuous monitoring systems can evaluate the effectiveness of current network access controls and detect deviations from security policies or unexpected access attempts, facilitating immediate corrective actions.

- **Insider Threats:** This control can analyze user behaviors and access patterns within eBay to identify potential insider threats. Unusual file accesses, large data transfers, or other suspicious activities can be flagged for further investigation.

- **Vulnerabilities in Third-party Plugins/Services:** Continuous monitoring can be extended to third-party plugins and services integrated into eBay's environment. Regular checks ensure these external elements adhere to security standards and do not introduce vulnerabilities.

- **Brand Reputation Damage:** Monitoring social media, dark web, and other external platforms enables the organization to gather intelligence on potential threats or fraudulent activities that could harm its reputation. This proactive measure helps in managing and mitigating risks before they escalate.

- **Vulnerable Systems/Services Identified by Shodan.io:** Continuous scanning and intelligence tools can identify which of eBay's systems are visible on services like Shodan.io, and whether they appear vulnerable or misconfigured, allowing for prompt remediation.

- **Fraudulent Transactions:** Continuous monitoring of transaction patterns and behaviors can help detect and respond to anomalies that suggest fraudulent activities, reducing financial losses and protecting user trust.

- **Insecure Mobile APIs:** Regular scanning and assessment of eBay's mobile APIs can identify security gaps or vulnerabilities. Continuous monitoring ensures that any deviations from security baselines are quickly addressed.

- **Poor Session Management:** Monitoring session management practices in real-time allows us to detect and mitigate risks associated with session hijacking or token theft, enhancing the security of user sessions.

10.3.5 User and Entity Behavior Analytics (UEBA) systems

[Detective Control][Technical]
User and Entity Behavior Analytics (UEBA) systems leverage machine learning, algorithms, and statistical analyses to detect when there is anomalous behavior within an IT network that deviates from the norms of user activities. They are deployed to monitor user activity continuously, identify patterns of behavior, and highlight anomalies that might indicate potential security threats or breaches. Here is a list of Vulnerabilities Addressed by this Control:

- **Insider Data Theft:** UEBA systems are specifically tuned to mitigate the vulnerability of insider data theft, a significant risk for a platform like eBay. By establishing what constitutes normal behavior through baseline analytics. They can promptly identify unusual access patterns or data movements that deviate from the norm, suggesting potential insider threats. Automatically trigger alerts and initiate responses when suspicious activities are detected, thus preventing unauthorized data access or exfiltration.

10.4 Supportive & Procedural Controls

These controls focus on creating a secure environment through policies, procedures, and best practices. They are preventive by nature and aim to raise the overall security awareness and compliance within the organization.

10.4.1 Implementation of Security Policies and Training

[Preventative Control][Non-Technical]
The implementation of security policies and training at eBay involves developing, disseminating, and enforcing policies that outline secure practices for handling data and using technology systems. Additionally, this control includes comprehensive training programs for all employees, focusing on recognizing and responding to security threats effectively. This control is designed to create a security-aware culture within eBay, ensuring that all personnel understand their role in safeguarding the company's assets.

Here is a list of Vulnerabilities Addressed by this Control:

- **Security Configuration:** Security policies dictate secure configurations for all systems and devices. These policies help in establishing a baseline that guards against unauthorized changes and reduces the surface for potential attacks. Training ensures that employees understand the importance of adhering to these configurations, mitigating risks associated with misconfigurations.

- **Phishing Attacks:** Through regular training sessions, eBay's employees are educated on identifying and responding to phishing attempts. This training includes recognizing suspicious emails and websites, thus reducing the likelihood of falling prey to phishing schemes that could compromise sensitive information.

- **Email Spoofing:** Security policies include guidelines on verifying the authenticity of emails and handling unexpected requests. Training in recognizing email spoofing attempts helps employees to spot and report fraudulent activities, thereby preventing potential breaches that leverage spoofed emails.

- **Insider Threats:** Training programs at eBay emphasize the importance of security practices and the consequences of policy violations, which include potential legal actions. This approach helps deter malicious activities from within the organization and teaches employees how to report suspicious behavior.

- **Legal Issues:** Well-crafted security policies ensure compliance with relevant laws and regulations, reducing legal risks. Regular training on these legal obligations reinforces the importance of compliance and educates employees about the consequences of legal violations.

- **Brand Reputation Damage:** By implementing robust security policies and conducting regular training, eBay can maintain a strong security posture that protects its brand reputation. Training employees to handle data and security incidents properly minimizes the risk of incidents that could lead to negative public perceptions.

- **Insecure Data Storage:** Security policies at eBay set strict guidelines for data storage and encryption standards. Training ensures that employees are aware of these storage protocols and understand how to properly secure data, mitigating risks associated with data leakage or unauthorized access.

- **Insider Data Theft:** The combination of strict policies and comprehensive employee training helps to minimize the risk of insider data theft. Employees are educated on the secure handling of information and the serious implications of data theft, both for themselves and the organization.

10.4.2 Comprehensive Logging

[Forensic Control][Technical]
Comprehensive logging involves the detailed recording of events and transactions within an IT system to enable the tracking and analysis of actions performed, especially those related to security. A robust comprehensive logging system can be instrumental. It provides the ability to monitor and log all activities across its network, applications, and databases, which is crucial for an online marketplace with complex transactions and a high volume of user interactions.

Here is a list of Vulnerabilities Addressed by this Control:

- **Set-Cookie Headers Without 'SameSite' Attribute:** Logging all cookie operations and header settings can help identify and rectify instances where cookies are set without the 'SameSite' attribute, potentially reducing the risk of cross-site request forgery attacks.

- **Transfer-Encoding - Chunked:** By logging the details of how data packets are handled, eBay can monitor any irregularities or manipulations in the chunked transfer encoding process that might indicate an attempt to exploit the system.

- **Cross-Site Scripting (XSS):** Comprehensive logging will enable eBay to detect and respond to XSS attacks by logging input data and detecting malicious patterns. Analyzing logs helps to identify and patch XSS vulnerabilities promptly.

- **Unauthorized Email Access:** Logging access to email systems and recording login details such as IP addresses, access times, and access attempts can help eBay quickly identify unauthorized access and take appropriate security measures.
- **Open Ports/Services:** Regular logging and reviewing of open ports and services can reveal unnecessary or insecure open ports that might be used as entry points by attackers.
- **Weak Network Access Controls:** By logging attempts to access the network, eBay can analyze patterns that may indicate attempts to exploit weak network access controls, allowing them to strengthen their defenses.
- **Insider Threats:** Logging all user activities helps to detect unusual behaviors that might indicate insider threats. This is critical for eBay, given the vast amount of sensitive data they manage.
- **Vulnerabilities in Third-party Plugins/Services:** Logging interactions with third-party services can help eBay identify and mitigate risks associated with external plugins or services that might be compromised.
- **Vulnerable Systems/Services Identified by Shodan.io:** Logs can be used to verify alerts from tools like Shodan.io about vulnerable systems, enabling eBay to address these vulnerabilities more efficiently.
- **Payment Card Data Breaches:** Monitoring and logging all transactions involving payment data allows eBay to detect and respond to anomalies that may suggest a data breach.
- **Fraudulent Transactions:** By comprehensively logging transaction details, eBay can analyze patterns that help identify and prevent fraudulent activities.
- **Insecure Mobile APIs:** Logging API calls and responses is crucial for detecting security lapses in mobile applications, helping to prevent data leaks or unauthorized access.
- **Poor Session Management:** Logging session management processes enables eBay to detect and rectify issues such as inadequate session expiration and token reuse, enhancing user security.

10.4.3 Secure Storage and Handling of Logs and Evidence

[Forensic Control][Technical]
Secure Storage and Handling of Logs and Evidence is a critical forensic control designed to ensure that all digital logs and evidence are stored and handled in a manner that preserves their integrity and confidentiality. Implementing robust mechanisms for the secure storage and handling of logs is essential. This control involves the use of encrypted storage solutions, regular audits, and restricted access protocols to ensure that only authorized personnel can access log data. Additionally, eBay can employ automated tools to manage log data effectively, ensuring that all logs are collected, stored, and analyzed in a secure and compliant manner.

Here is a list of Vulnerabilities Addressed by this Control:

- **Information Disclosure in Server Header:** Secure storage and handling of logs help eBay to identify and mitigate instances where sensitive information might be inadvertently leaked through server headers. By analyzing logs securely, eBay can ensure that configurations do not expose sensitive data.

- **Insider Threats:** By securely logging and monitoring data access and handling, eBay can detect and respond to suspicious activities that might indicate insider threats. This control helps in tracing activities back to specific users, thereby deterring malicious insider activities and enabling prompt response to potential data breaches.
- **Legal Issues:** Proper log management and secure evidence handling ensure that eBay can comply with legal and regulatory requirements related to data retention and privacy. This control is essential for producing reliable logs that can serve as evidence in legal proceedings, thus protecting eBay from legal repercussions.
- **Brand Reputation Damage:** Secure handling of logs contributes to protecting eBay's brand reputation by preventing data breaches that can lead to loss of customer trust. Effective log management helps in early detection of security incidents, minimizing the impact and exposure of such events.
- **nsecure Data Storage:** Implementing secure storage practices for logs ensures that sensitive data, which could be exploited if exposed, is securely encrypted and handled. This minimizes the risk of data leaks and breaches that could occur due to insecure storage practices.

10.4.4 Audit Trails

[Forensic Control][Non-Technical]
Audit Trails are a crucial forensic control mechanism that involves systematically recording and storing actions taken by users or automated systems within an organization's IT environment. Implementing robust audit trails means tracking and logging every transaction, configuration change, data access, and other activities conducted on its platforms. This helps in ensuring accountability and provides a means to detect and investigate suspicious or unauthorized activities effectively.

Here is a list of Vulnerabilities Addressed by this Control:

- **Security Configuration:** Audit trails help mitigate security configuration vulnerabilities by providing a historical record of changes made to system configurations. This allows eBay to quickly review and audit configurations to ensure they comply with established security standards. Any unauthorized changes or misconfigurations can be identified and remedied promptly, thereby reducing the window of opportunity for attackers.
- **Inadequate Data Backup and Recovery Measures:** By maintaining comprehensive logs of data handling and backup operations, audit trails ensure that any data loss can be investigated and attributed to specific actions or shortcomings. This capability enables eBay to enhance its backup strategies and recovery processes, ensuring that data integrity and availability are maintained even in adverse conditions.
- **Insider Data Theft:** Audit trails are particularly effective against insider threats, as they provide detailed visibility into user activities, including access to sensitive data. For eBay, using audit trails means being able to detect unusual access patterns or unauthorized data exports, which are indicative of insider data theft. This allows for timely intervention and mitigation of potential data breaches from within the organization.
- **Supply Chain Vulnerabilities:** In the context of supply chain security, audit trails help eBay track and scrutinize the actions taken by third-party vendors within its systems. This ensures that any suspicious activity or deviation from agreed-upon protocols can be quickly identified and addressed. Moreover, audit trails help in the forensic investigation of incidents that may arise from supply chain vulnerabilities, thus strengthening overall supply chain security.

10.4.5 Incident Response and Investigation Procedures

[Forensic Control][Technical]
Incident Response and Investigation Procedures are critical forensic controls that eBay can employ to handle security incidents effectively and minimize potential damage. This control involves a predefined plan that outlines how to respond to various security breaches. It includes immediate actions upon detection, investigation to understand the breach's extent, and steps to prevent future incidents. By integrating these procedures, we ensures rapid containment and recovery from attacks, maintaining trust and operational continuity.

Here is a list of Vulnerabilities Addressed by this Control:

- **Phishing Attacks:** These procedures help eBay quickly identify and mitigate phishing attacks by analyzing suspicious emails or communication. This rapid response prevents broader distribution and reduces the risk of sensitive information being compromised.
- **Email Spoofing:** When email spoofing is detected, these procedures guide the response team on how to trace the source and block similar attacks. This helps protect eBay's communication channels from being exploited for fraud or misinformation.
- **Lack of Email Encryption:** If incidents occur due to unencrypted emails leading to data breaches, the incident response team investigates the breach's cause and scope, advising on corrective measures like enforcing encryption.
- **DNSSEC Not Enabled:** Should the organization face DNS-related attacks, the response procedures can identify and rectify the exploitation of this vulnerability, guiding the implementation of DNSSEC to enhance domain security.
- **Payment Card Data Breaches:** The procedures include immediate actions to secure affected systems, assess the data compromised, and comply with legal and regulatory reporting obligations, thus minimizing financial and reputational damage.
- **Fraudulent Transactions:** By following these procedures, eBay can quickly investigate fraudulent transactions, determine their origin, and take steps to reverse any unauthorized transactions and strengthen transaction monitoring systems.

10.4.6 Continuous Monitoring of Legal and Regulatory Changes

[Detective Control][Non-Technical]
Continuous Monitoring of Legal and Regulatory Changes involves systematic observation and review of the legal and regulatory landscape that impacts an organization's operations. This control is critical due to the diverse legal frameworks in different countries affecting e-commerce, data protection, consumer rights, and international trade. Implementing this control would require eBay to utilize dedicated legal and compliance teams, possibly supported by automated tools that alert changes in relevant laws and regulations. This proactive approach ensures eBay remains compliant and can adapt its policies and practices promptly to avoid legal pitfalls. Here is a list of Vulnerabilities Addressed by this Control:

- **Legal Issues:** This control directly addresses vulnerabilities related to legal non-compliance which could result in fines, sanctions, or business disruption. By continuously monitoring changes in laws and regulations, eBay can preemptively adjust its business practices to remain compliant with new legal requirements. This is especially important in areas like data privacy

(GDPR in Europe, CCPA in California), consumer protection laws, and anti-money laundering regulations. The effectiveness of this control can be measured by the decrease in legal violations and the speed at which new regulations are implemented into eBay's operational practices. Regular audits and reports on compliance status would help in maintaining transparency and accountability. Besides avoiding penalties, this control strengthens eBay's reputation as a trustworthy and law-abiding marketplace. It enhances consumer and stakeholder trust, which is crucial for maintaining and growing the user base in competitive global markets.

10.4.7 Document Classification and Handling Policies

[Preventative Control][Non-Technical]
Document Classification and Handling Policies are critical in establishing protocols for managing the sensitivity of company documents and determining who can access certain types of information. This control can be implemented by categorizing documents according to their confidentiality level and ensuring that handling procedures are strictly followed to protect sensitive data. This system not only helps in maintaining organized document storage and retrieval processes but also significantly mitigates the risk of information leaks.

Here is a list of Vulnerabilities Addressed by this Control:

- **Legal Issues:** Legal issues often arise from mishandling sensitive information, leading to compliance breaches and potential legal penalties. By implementing robust Document Classification and Handling Policies, eBay can ensure that all documents are handled according to their classification standards, thus preventing unauthorized access and disclosure. This control is particularly effective in maintaining compliance with data protection regulations like GDPR and HIPAA, which mandate strict handling and protection protocols for personal and sensitive information. Such policies are essential in training employees to recognize the importance of document security and in creating an audit trail for accessing sensitive information, thereby providing a legal defense mechanism should breaches occur.

10.5 Audit Controls

These controls are geared towards verification and compliance, ensuring that other security controls are effectively implemented and adhered to. They provide a mechanism for independent review and identification of lapses in the security posture.

10.5.1 IT Security Audits

[Audit Control][Technical]
IT Security Audits are a comprehensive evaluation of an organization's information system by measuring how well it conforms to a set of established criteria. These audits systematically assess the resilience of eBay's IT infrastructure against security breaches and compliance with international cybersecurity standards. The process includes reviewing security policies, system access controls, and the effectiveness of security measures in place.

Here is a list of Vulnerabilities Addressed by this Control:

- **Set-Cookie Headers & Security Configuration:** Audits identify misconfigurations like missing 'SameSite' attributes in cookies and other security headers, ensuring that security configurations align with best practices to prevent exploits.

- **Email Vulnerabilities (Spoofing, Lack of Encryption):** By auditing the email systems, eBay can ensure that adequate encryption is in place and that mechanisms to authenticate email sources are effective, reducing the risk of spoofing and unauthorized access.

- **Cross-Site Scripting (XSS) & Server Header Disclosures:** Security audits help discover vulnerabilities like XSS and information leakage through server headers by inspecting and evaluating the web applications and server configurations used by eBay.

- **Network Vulnerabilities (DNSSEC, Open Ports, Shodan.io Exposure):** Audits review network configurations and external service exposures to ensure that DNS security extensions are used and unnecessary ports are not open, thus safeguarding against service exploitation visible through platforms like Shodan.

- **Data Storage and API Security:** The audits extend to reviewing how data is stored and how APIs are secured, ensuring that any data at rest and in transit within eBay's infrastructure is adequately protected against breaches.

10.5.2 Operational Audits

[Audit Control][Non-Technical]
Operational audits involve a systematic review and analysis of organizational processes, controls, and guidelines to ensure compliance, effectiveness, and efficiency. Operational audits will be strategically used to scrutinize various aspects of the network and system operations, data handling practices, and internal policies. By examining these areas through audits, we can identify operational weaknesses and implement improvements, enhancing overall security posture and operational efficiency.

Here is a list of Vulnerabilities Addressed by this Control:

- **Weak Network Access Controls:** Operational audits would include an examination of existing network access controls. Auditors can assess the adequacy of authentication and authorization mechanisms, ensuring only authorized users have access to sensitive network segments. Recommendations can be made to strengthen these controls, thus reducing the risk of unauthorized access.

- **Insider Threats:** By reviewing user activities and access logs, operational audits help detect patterns or actions that might indicate malicious insider activities. These audits enable proactive management of potential insider threats by implementing stricter controls and monitoring systems based on audit findings.

- **Brand Reputation Damage:** Operational audits extend beyond technical measures to include evaluations of how data is handled and protected, as well as adherence to legal and ethical standards. Ensuring all processes align with best practices and regulatory requirements can mitigate incidents that might otherwise lead to reputation damage.

- **Inadequate Data Backup and Recovery Measures:** Through operational audits, we can verify the effectiveness and efficiency of its data backup and recovery procedures. Audits help ensure backups are performed as scheduled, stored securely, and can be quickly restored, thus maintaining business continuity in the event of data loss.

10.5.3 Third Party Audits

[Audit Control][Non-Technical]
Third Party Audits are an essential control measure that involves external auditors assessing the security and reliability of systems and services provided by third-party vendors[27]. eBay, relying significantly on various third-party plugins and services for its extensive online marketplace operations, needs to use these audits to verify the security measures implemented by these vendors, ensuring they comply with the organizations strict security standards.

Here is a list of Vulnerabilities Addressed by this Control:

- **Vulnerabilities in Third-party Plugins/Services:** Third Party Audits directly target vulnerabilities that may arise from third-party plugins and services. By conducting these audits, eBay can identify and address security weaknesses or compliance issues within these external services before they impact the platform. This proactive approach allows us to manage risks associated with external software integrations, which are crucial for its operation but could also serve as potential entry points for security breaches. Through the audits, we can ensure that third-party services adhere to the latest security practices and standards, reducing the likelihood of vulnerabilities such as unauthorized access, data leaks, or service disruptions. Regular auditing also pressures vendors to maintain high-security standards as a requirement for their continued collaboration with the organization, thus safeguarding the ecosystem from potential threats introduced via third-party systems.

10.5.4 Compliance Audits

[Audit Control][Non-Technical]
Compliance audits are systematic evaluations conducted to ascertain whether an organization adheres to regulatory guidelines. Compliance audits would involve rigorous checks to ensure that all business operations align with legal standards, payment card industry data security standards (PCI DSS), and other relevant regulations. These audits help identify non-compliance issues that could lead to legal actions, financial penalties, or breaches of customer trust.

Here is a list of Vulnerabilities Addressed by this Control:

- **Legal Issues:** Through regular compliance audits, the organization can ensure adherence to data protection laws, consumer protection laws, and other regulatory requirements. This proactive approach helps prevent legal entanglements that could arise from non-compliance, thus protecting eBay from potential fines and legal actions.

- **Payment Card Data Breaches:** Compliance audits help in the enforcement of PCI DSS compliance and other security standards that safeguard payment card data. Regular audits ensure that payment systems are secure and that any vulnerabilities are identified and addressed promptly, thus reducing the risk of data breaches.

- **Supply Chain Vulnerabilities:** Compliance audits extend to evaluating the security and compliance of third-party vendors and suppliers. By verifying that suppliers adhere to security standards, eBay can prevent breaches that originate from less secure elements in the supply chain.

10.5.5 Forensic Audits

[Audit Control][Non-Technical]
Forensic audits are comprehensive and systematic examinations of an organization's financial records,

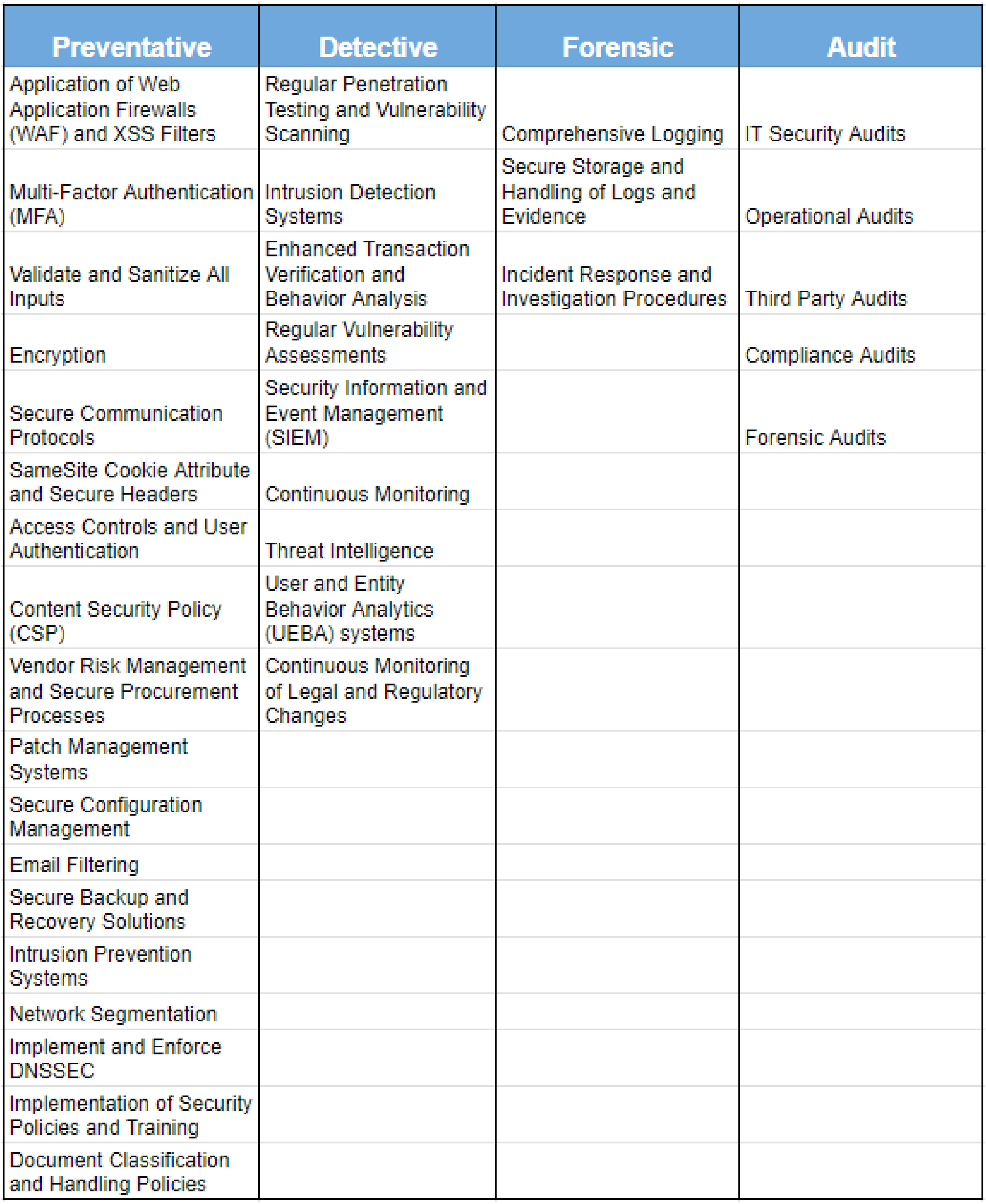
intended to uncover activities that might constitute fraud, theft, or misuse of the company's assets. At eBay, forensic audits can be employed as a specialized form of investigation following the detection of irregularities or suspicions of insider data theft. These audits would involve the meticulous review of digital trails left by employees or insiders who might have unauthorized access to sensitive data. Forensic tools and techniques would be used to reconstruct events, identify unauthorized actions, and gather evidence that can support disciplinary or legal actions.

Here is a list of Vulnerabilities Addressed by this Control:

- **Insider Data Theft:** This control is particularly effective in mitigating the risks associated with insider data theft. Forensic audits help identify and document instances where employees might be illegally copying, transferring, or using sensitive information for personal gain. The audit process can reveal hidden patterns and connections that are not obvious through regular monitoring and can help strengthen other security measures by providing insights into existing vulnerabilities. By doing so, forensic audits not only address the immediate concerns of data theft but also contribute to the overall strengthening of the organization's security posture against similar threats in the future.

11 CATEGORIZING CONTROLS

11.1 Preventative, Detective, Forensic & Audit



Preventative	Detective	Forensic	Audit
Application of Web Application Firewalls (WAF) and XSS Filters	Regular Penetration Testing and Vulnerability Scanning	Comprehensive Logging	IT Security Audits
Multi-Factor Authentication (MFA)	Intrusion Detection Systems	Secure Storage and Handling of Logs and Evidence	Operational Audits
Validate and Sanitize All Inputs	Enhanced Transaction Verification and Behavior Analysis	Incident Response and Investigation Procedures	Third Party Audits
Encryption	Regular Vulnerability Assessments		Compliance Audits
Secure Communication Protocols	Security Information and Event Management (SIEM)		Forensic Audits
SameSite Cookie Attribute and Secure Headers	Continuous Monitoring		
Access Controls and User Authentication	Threat Intelligence		
Content Security Policy (CSP)	User and Entity Behavior Analytics (UEBA) systems		
Vendor Risk Management and Secure Procurement Processes	Continuous Monitoring of Legal and Regulatory Changes		
Patch Management Systems			
Secure Configuration Management			
Email Filtering			
Secure Backup and Recovery Solutions			
Intrusion Prevention Systems			
Network Segmentation			
Implement and Enforce DNSSEC			
Implementation of Security Policies and Training			
Document Classification and Handling Policies			

Figure 5: Categorized in Subcategories

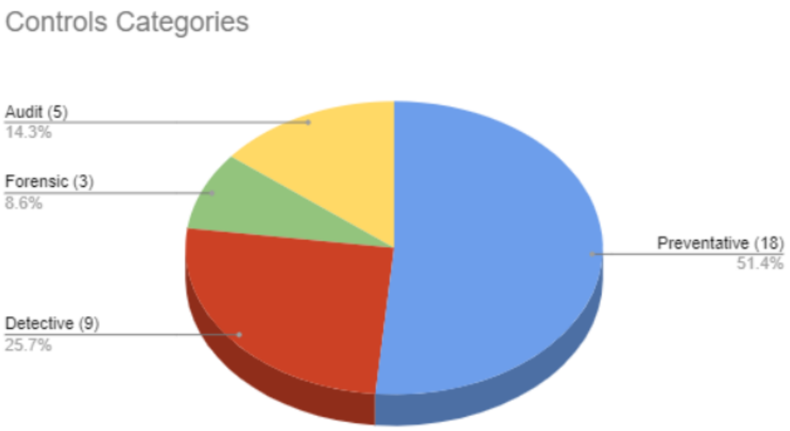


Figure 6: Control Category Chart

12 COST BREAKDOWN FOR ALL CONTROLS

eBay's security controls are structured to safeguard the platform's critical infrastructure, protect user data, ensure compliance with industry regulations, and respond effectively to threats. Each control has a unique cost structure, reflecting initial setup, ongoing maintenance, employee training, and operational impacts. The cost breakdown for all the controls is detailed in the Budget sheet[28]. For the purpose of understanding the budget sheet only includes the maximum cost calculated for each control. The approximate employee pay rate is assumed to be $40 to $55 per hour as found on Glassdoor[29]. These pay rates are used to estimate costs related to employee training, staffing, and other labor-intensive controls in the budget scenarios.

12.1 Most effective

12.1.1 Web Application Firewalls (WAF)

Implementing Web Application Firewalls (WAF) is a crucial security measure to protect eBay's digital infrastructure. The costs associated with this control vary significantly depending on the level of investment and scope of implementation as many services implement pay-as-you go pricing. eBay likely has a vast server infrastructure across multiple locations. Protecting all these points will likely requires complex WAF deployment. Further, maintaining a WAF for a large organization requires a dedicated security team and vendor support, which can be expensive[30].

- **Minimum Cost**
  Azure WAF v2 pricing details are not publicly available, it's safe to assume it's higher than v1's $0.448 per gateway-hour. Assuming a very low hourly rate of $0.5 and minimal runtime (8 hours/day), monthly cost would be $0.5 x 8 hours/day x 30 days = $120. Low consumption will have a monthly cost of $1,000 and yearly (1,000 x 12) = 12,000. Using the in-house IT team installation and configuration require 40 hours of labor, costing (40 x $40) = $1,800.

  Recurring costs for maintenance and updates are expected to be around $2,000/year, with an additional $3,000/year for subscription fees. Employee training is also a significant component, with one 8-hour session for 30 employees. This training, at a rate of $45/hour, results in a total cost of $10,800 for training.

Combining all these factors, the total annual cost for a minimum cost for WAF implementation is approximately $28,700.

- **Maximum Cost**
For an advanced WAF setup, the initial purchase with an high hourly rate of $1 and continuous operation (24/7), monthly cost would be $1.0 x 24 hours/day x 30 days = $720. Assuming high consumption with a monthly cost of $5,000 and yearly (5,000 x 12) = 60,000. The installation and configuration require 50 hours of labor, costing (50 x $40) = $2,250.

  Recurring costs for high-end maintenance and updates are estimated at $10,000/year, with premium subscription fees of $8,000/year. Employee training is more extensive, requiring three 8-hour sessions for 50 employees. At $40/hour, the training cost comes to $54,000.

  The total annual maximum cost for WAF implementation, including all advanced technology and extensive training, is approximately $135,400.

Description	Minimum Cost($)	Maximum Cost($)
Initial Setup Cost	12,000	60,000
Installation & Configuration Cost	1,800	2,250
Recurring Maintenance & Updates Cost	2,000	10,000
Recurring Subscription Fees	3,000	8,000
Employee Training Cost	10,800	54,000
Total Annual Cost	53,500	134,250

Table 12: Web Application Firewalls Cost Breakdown

12.1.2 Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a crucial control for enhancing security by requiring users to provide multiple verification factors to access systems. By requiring an extra layer of authentication, eBay can significantly reduce the risk of unauthorized access to employee accounts and protect sensitive data. The estimated costs assume an hourly wage of $40/hr for employees involved in the setup and operation of MFA[31].

- **Minimum Cost**
To implement MFA in a cost-effective manner, the initial setup cost includes hardware/software purchases. With 10% of the total workforce (1,060 out of 10,600 employees) requiring hardware tokens, at an estimated cost of $40/token, the total hardware cost is $42,400. The installation and configuration, involving minimal infrastructure changes, would require approximately $5,000 for basic software systems and light integration. Employee cost for installation, involving one system administrator and one security specialist working 20 hours each, is calculated to be $1,700 ($700 for the system administrator and $1,000 for the security specialist).

  Recurring costs consist of maintenance and updates, estimated at $1,000/year, and subscription fees for basic MFA software, costing $100/month or $1,200/year. Training sessions for system administrators and security specialists (4 hours) would cost $340 in total, with an additional $23,850 for employee training, given that each employee would attend a 1-hour training session at $40/hour.

  The total minimum annual cost for implementing MFA, including hardware, installation, maintenance, subscription fees, and employee training, is approximately $47,490.

- **Maximum Cost**
  For a premium MFA setup, the initial setup cost for hardware/software increases significantly. With a total of 10,600 employees requiring hardware tokens, at a cost of $40/token, the total hardware cost is $424,000. Using high-end contractors for installation and configuration, the cost is estimated at $30,000. Employee cost for installation, involving one system administrator and one security specialist working 40 hours each, is $3,400 ($1,400 for the system administrator and $2,000 for the security specialist).

  Recurring costs for maintenance and updates, with premium support, are estimated at $3,000/year, while subscription fees for advanced MFA software cost $500/month, totaling $6,000/year. Training sessions for system administrators and security specialists (4 hours) cost $340, with an additional $47,700 for employee training, assuming 1,060 employees require a 1-hour training session.

  The total maximum annual cost for implementing MFA, accounting for premium hardware, top-tier installation, maintenance, subscription fees, and extensive training, is approximately $163,640.

Description	Minimum Cost($)	Maximum Cost($)
Hardware/Software Purchase	42,400	424,000
Installation & Configuration Cost	1,700	3,400
Recurring Maintenance & Updates Cost	1,000	3,000
Recurring Subscription Fees	1,200	6,000
Employee Training Cost	23,850	47,700
Total Annual Cost	70,150	484,100

Table 13: Multi-Factor Authentication Cost Breakdown

12.1.3 Use of Encryption

Encryption is critical for online security, especially for e-commerce giants like eBay. It acts as a digital shield, scrambling sensitive information like financial details, personal data, and communication channels. By implementing robust encryption practices, eBay can fosters a secure environment where buyers and sellers can confidently interact, ultimately strengthening the foundation of trust that fuels their online marketplace.

- **Minimum Cost**
  For the minimum cost, the initial setup cost includes purchasing basic encryption software and SSL/TLS certificates. These costs are estimated at $100,000. The installation and configuration of encryption tools require $5,000 for setup, and the employee cost for installation, involving three employees working 40 hours each at a rate of $40/hr, totals $4,800.

  Recurring costs include maintenance and updates for encryption software, costing about $10,000/year, and basic subscription fees, estimated at $5,000/year. Training sessions for key employees involved in encryption implementation cost $500/session, with basic training estimated at $500 for one session. Employee training cost, assuming 50 employees requiring 8 hours of training at $40/hr, totals $16,000.

  The total annual cost for implementing encryption with a minimal budget, covering software, installation, maintenance, subscription fees, and training, is approximately $136,300.

- **Maximum Cost**
  The initial setup cost involves purchasing high-end encryption software, advanced encryption appliances, and enterprise-level security solutions, with a total estimate of $500,000. The installation and configuration cost, given more complex setup and high-end security configurations, is estimated at $50,000. Employee cost for installation, with 10 employees working 80 hours each at $40/hr, leads to a cost of $32,000.

  Recurring costs for maintenance and updates with advanced support are estimated at $50,000/year. High-end subscription-based encryption tools with premium features would cost around $50,000/year. Comprehensive training sessions by external experts are estimated at $25,000 for five sessions, with employee training for 200 employees requiring 16 hours each at $40/hr totaling $128,000.

  The total maximum annual cost for implementing encryption, considering advanced encryption solutions, installation, maintenance, premium subscriptions, and extensive training, is approximately $835,000.

Description	Minimum Cost($)	Maximum Cost($)
Hardware/Software Purchase	100,000	500,000
Installation & Configuration Cost	5,000	50,000
Employee Cost for Installation	4,800	32,000
Recurring Maintenance & Updates Cost	10,000	50,000
Recurring Subscription Fees	5,000	50,000
Training Session Cost	500	25,000
Employee Training Cost	16,000	128,000
Total Annual Cost	136,300	835,000

Table 14: Encryption Cost Breakdown

12.1.4 Enforcement of Access Controls and User Authentication

Access control and user authentication are critical components of any organization's security strategy. Access controls function like sophisticated security checkpoints, meticulously regulating who can enter specific areas and what actions they can take. Before granting access, users must verify their identity through a multi-layered authentication process.

- **Minimum Cost**
  The minimum cost focuses on a basic setup for enforcing access controls and user authentication, with an emphasis on cost-efficiency. Policy development is estimated to cost $10,000, covering the creation and implementation of access control policies, including roles and permissions. This might involve existing staff and basic tools.

  Employee training is another significant cost. With 10,600 employees needing 2 hours of basic training at an hourly rate of $40, the total training cost is $848,000. The training covers password management, multi-factor authentication, and secure access practices. Access control technology costs are estimated at $50,000 for basic hardware (smart card readers, biometric devices) and software licenses for user authentication. The recurring costs for maintenance and support are about $10,000/year. Implementation and configuration are estimated at $20,000, covering technical labor for the setup of access control systems.

  Ongoing maintenance is estimated at $15,000/year for patching and troubleshooting. Operational impact costs are minimal, with no significant downtime or reduced productivity factored into this budget scenario.

The total annual cost for enforcing access controls and user authentication, including policy development, training, technology, implementation, and ongoing maintenance, is approximately $953,000.

- **Maximum Cost**
  Policy development, including the use of external consultants to ensure best practices, is estimated to cost $30,000. Employee training in this scenario is more extensive. With 10,600 employees requiring 6 hours of training at an hourly rate of $40, the total training cost is $2,544,000. This training includes advanced security practices and technical sessions on specific tools.

  Access control technology costs are significantly higher, with hardware/software costs estimated at $150,000 for high-end equipment (biometric authentication, advanced user authentication systems, and secure identity management software). Recurring costs for maintenance and support are estimated at $30,000/year. Implementation and configuration, given the more complex systems, are estimated at $70,000.

  Ongoing maintenance and support are estimated at $40,000/year to ensure optimal performance and security. The operational impact costs could be significant due to extensive system changes, requiring contingency planning and backup systems. Reduced productivity costs are factored into the comprehensive training.

  The total annual cost for enforcing access controls and user authentication, accounting for extensive policy development, advanced training, high-end technology, and extensive support, is approximately $2,864,000.

Description	Minimum Cost($)	Maximum Cost($)
Policy Development	10,000	30,000
Employee Training Cost	848,000	2,544,000
Hardware/Software Cost	50,000	150,000
Implementation & Configuration Cost	20,000	70,000
Recurring Updates Cost	10,000	30,000
Recurring Maintenance Cost	15,000	40,000
Total Annual Cost	953,000	2,864,000

Table 15: Access Controls and User Authentication Cost Breakdown

12.1.5 Implementing Content Security Policy (CSP)

Content Security Policy (CSP) is a key web security feature that helps protect websites from various vulnerabilities, such as cross-site scripting (XSS) and clickjacking. A CSP acts as a set of security instructions that dictates what resources, such as scripts, images, and stylesheets, can be loaded on our webpages. This essentially allows us to create a whitelist of authorized sources, preventing any unauthorized content from infiltrating our platform.

- **Minimum Cost**
  Employee training cost assumes only a subset of employees requires CSP training—likely from IT, cybersecurity, and compliance teams—estimated at 5% of the total workforce. With 530 employees needing 8 hours of training at $45/hour, the total training cost is $339,200.

  Hardware and software costs are estimated at $15,000 for tools, with $10,000/year for updates and subscriptions. Implementation and configuration costs are expected to be relatively low, with internal staff handling the work. Assuming two full-time IT employees working for 80 hours each at $40/hour, the cost for implementation and configuration totals $6,400.

Policy development, involving three employees from a compliance or legal team working for 40 hours each at $40/hour, results in a cost of $4,800.

The total annual cost for implementing CSP, hardware/software, implementation, and policy development, is approximately $357,400.

- **Maximum Cost**
  Employee training is expanded to ensure compliance across the organization. With 20% of the total workforce (2,120 out of 10,600 employees) requiring 8 hours of training at $40/hour, the total training cost is $678,400.

  Hardware/software costs are higher, with $10,000 for high-end software tools and $5,000/year for updates and subscriptions. Implementation and configuration involve additional staff and expert consulting. Assuming four internal staff members working for 160 hours each at $40/hour, the cost for implementation and configuration is $25,600. Expert consulting for CSP best practices is estimated at $10,000.

  Policy development includes external legal consultation, estimated at $10,000, with an internal compliance team of five employees working for 80 hours each at $40/hour, totaling $16,000.

  Operational costs for additional staffing during implementation are minimal, with two employees working for 80 hours each at $40/hour, costing $6,400.

  The total annual cost for implementing CSP, including comprehensive training, high-end hardware/software, implementation with expert consulting, and policy development with legal consultation, is approximately $751,400.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	190,800	678,400
Hardware/Software Cost	15,000	10,000
Recurring Maintenance & Updates Cost	10,000	5,000
Implementation & Configuration Cost	6,400	25,600
Policy Development Cost	4,800	16,000
Expert Consulting	-	10,000
Operational Cost	-	6,400
Total Annual Cost	227,000	751,400

Table 16: Content Security Policy Cost Breakdown

12.1.6 Vendor Risk Management and Secure Procurement Processes

Vendor risk management and secure procurement processes are critical components of a comprehensive cybersecurity strategy. VRM acts as a comprehensive security screening process for our vendors. VRM meticulously assesses potential vendors to identify and mitigate potential risks[32].

- **Minimum Cost**
  The employee training cost involves a small team of 20 employees. Each employee receives 8 hours of training in vendor risk management and 8 hours in secure procurement processes, at $40/hr. The total training cost is $12,800 (20×(8+8)×40). Hardware/software costs are

assumed to be minimal, leveraging existing resources and open-source software to minimize expenses.

Implementation and configuration costs are kept low, with one individual working for 80 hours at $40/hr to establish vendor risk management processes and configure secure procurement systems. The total configuration cost is $3,200. Recurring costs for maintenance and updates are estimated at 40 hours/year at $40/hr, totaling $1,600. Policy development costs, considering 30 hours for creating and refining policies at $40/hr with 10 employees, result in $12,000. Operational costs, including administrative work for paperwork, meetings, and regular vendor evaluations, are estimated at 40 hours/year at $40/hr, adding $1600.

The total minimum annual cost for vendor risk management and secure procurement processes is approximately $31,200.

- **Maximum Cost**
  Employee training is more comprehensive, involving 100 employees receiving 16 hours of training (8 hours for vendor risk management and 8 hours for secure procurement). At $40/hr, the total training cost is $64,000 (100×(8+8)×40).

  Hardware/software costs increase, with an investment in specialized vendor risk management software and related tools, estimated at $10,000 for a year-long license. Implementation and configuration costs reflect a more extensive setup, with an expert team handling 160 hours of work at $40/hr, totaling $6,400. Recurring costs for maintenance and updates also increase, estimated at 80 hours/year at $40/hr, totaling $3,200.

  Policy development is more thorough, requiring detailed compliance checks and external expertise, with 40 hours at $40/hr and 20 employees, resulting in a cost of $32,000. Operational costs, including increased meetings, evaluations, and documentation, are estimated at 80 hours/year at $40/hr, adding another $3,200.

  The total maximum annual cost for vendor risk management and secure procurement processes, including extensive training, specialized hardware/software, comprehensive policy development, and increased operational support, is approximately $118,800.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	12,800	64,000
Hardware/Software Cost	-	10,000
Implementation & Configuration Cost	3,200	6,400
Recurring Maintenance & Updates Cost	1,600	3,200
Policy Development Cost	12,000	32,000
Operational Cost	1,600	3,200
Total Annual Cost	31,200	118,800

Table 17: Vendor Risk Management and Secure Procurement Processes Cost Breakdown

12.1.7 Patch Management Systems

Patch management systems are crucial for ensuring that all software and systems are updated with the latest security patches, reducing the risk of vulnerabilities and security breaches. A centralized PMS automates patch deployment processes, streamlining security updates and saving valuable IT resources. While there is an initial investment in a PMS, the cost savings it delivers through reduced downtime, improved security posture, and potential avoidance of regulatory fines can be significant[33].

- **Minimum Cost**
  The employee training cost involves training both IT staff and end-users. With IT staff, assume 10 professionals requiring 8 hours of training at \$60/hour, leading to a cost of \$4,800. For end-users, assume 10,600 employees require a 1-hour training session at \$40/hour, totaling \$371,000.

  Hardware/software costs for patch management systems consist of software licenses and potentially additional hardware. A basic patch management tool with a yearly license costs \$10,000. Additional hardware isn't required, as existing infrastructure can be used. Implementation and configuration involve setting up and testing the system. Assuming two IT professionals working for one week (40 hours each) at \$60/hour, the total cost is \$4,800.

  Recurring costs for maintenance and updates include a 20% maintenance fee based on the software license, totaling \$2,000/year. Additionally, one IT professional dedicated to maintenance costs approximately \$60,000/year. Policy development for patch management involves writing and maintaining policies, procedures, and guidelines. With three compliance officer working part-time, the estimated cost is \$90,000/year.

  The total annual cost for implementing patch management systems, including employee training, software licenses, implementation, maintenance, and policy development, is approximately \$542,600.

- **Maximum Cost**
  The employee training costs increase with more comprehensive training for IT staff and end-users. With 20 IT professionals needing 8 hours of training at \$60/hour, the cost is \$9,600. For end-users, assume 10,600 employees require 2 hours of training at \$40/hour, leading to a total cost of \$857,600. Hardware/software costs are significantly higher, with a more comprehensive patch management suite with advanced features costing \$50,000/year. Additional hardware for redundancy, such as servers and backup systems, adds \$30,000.

  Implementation and configuration costs increase due to a longer setup time and more IT professionals. Assuming four IT professionals working for two weeks (80 hours each) at \$60/hour, the total cost is \$19,200.

  Recurring costs for maintenance and updates are based on the higher software license fee, totaling \$10,000/year. With two IT professionals dedicated to maintenance, the cost is \$120,000/year. Policy development requires a dedicated team, with 5 compliance officers working full-time at \$60,000/year each, totaling \$300,000/year.

  The total annual cost for implementing patch management systems, considering extensive training, high-end hardware/software, more comprehensive implementation, and full-time policy development, is approximately \$1,386,800.

12.1.8 Secure Configuration Management

Secure configuration management involves maintaining systems and applications in a secure state through consistent configuration, ensuring they remain resistant to vulnerabilities and security breaches. Even minor misconfigurations in system settings can create security vulnerabilities. SCM helps prevent such errors by defining and enforcing the desired configuration for all systems across the platform.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	375,800	857,600
Hardware/Software Cost	10,000	80,000
Implementation & Configuration Cost	4,800	19,200
Recurring Maintenance & Updates Cost	62,000	130,000
Policy Development Cost	90,000	300,000
Total Annual Cost	542,600	1,386,800

Table 18: Patch Management Systems Cost Breakdown

- **Minimum Cost**
  The employee training costs are calculated for 10% of the workforce (1,060 employees) who require 8-hour training sessions on secure configuration management. With a software engineer salary of $120,000/year, the hourly wage is approximately $60. Thus, the training cost per employee is $480, leading to a total training cost of $508,800 (1,060 × $480).

  Hardware/software costs are minimized by using open-source or low-cost tools, with a one-time cost of $5,000 for software. Hardware costs are avoided by utilizing existing infrastructure. Implementation and configuration costs are kept low by using internal resources. Assuming two full-time employees (FTE) for two weeks (80 hours each) at $60/hour, the total cost is $9,600.

  Recurring costs involve basic maintenance and updates for software, estimated at $5,000/year, and low-cost licenses, estimated at $2,000/year. Policy development costs are minimized by using internal resources. Assume one FTE for two weeks (80 hours) at $60/hour, resulting in a cost of $4,800.

  The total annual cost for implementing secure configuration management, covering training, software, implementation, maintenance, and policy development, is approximately $530,200.

- **Maximum Cost**
  The employee training involves more comprehensive sessions for a larger group, with 20% of the workforce (2,120 employees) requiring 8-hour training. At an hourly wage of $60, the cost per employee is $480, resulting in a total training cost of $1,017,600 (2,120 × $480).

  Hardware/software costs increase with premium software and additional hardware for secure configuration management. Premium software is estimated at $30,000, while additional hardware costs around $20,000. Implementation and configuration involve external professional services, estimated at $30,000 for comprehensive setup and configuration.

  Recurring costs for maintenance and updates are estimated at $20,000/year for premium support, and high-end licenses for security software are estimated at $15,000/year. Policy development in this scenario involves external consultants for comprehensive policy development and regular audits, estimated at $20,000.

  The total annual cost for implementing secure configuration management, accounting for comprehensive training, premium hardware/software, professional implementation, advanced maintenance, and external policy development, is approximately $1,102,600.

12.1.9 Regular Penetration Testing and Vulnerability Scanning

Regular penetration testing and vulnerability scanning are essential for identifying and addressing security weaknesses in an organization's infrastructure. Penetration testing goes beyond what vul-

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	508,800	1,017,600
Hardware/Software Cost	5,000	50,000
Implementation & Configuration Cost	9,600	30,000
Recurring Maintenance & Updates Cost	7,000	35,000
Policy Development Cost	4,800	20,000
Total Annual Cost	530,200	1,102,600

Table 19: Secure Configuration Management Cost Breakdown

nerability scanners can detect. It uncovers previously unknown weaknesses in our defenses, allowing us to address them before they can be exploited by attackers[34].

- **Minimum Cost**
  The employee training costs focus on a smaller group of specialized employees. Assuming 3 security engineers require training at $1,000 each, the total training cost is $3,000.

  Hardware/software costs for penetration testing software like Nessus or OpenVAS are estimated at $3,000 per license per year. Assuming two licenses for redundancy and multi-project coverage, the total hardware/software cost is $6,000. Implementation and configuration involve setup and configuration by security engineers. Assuming 40 hours of labor at $60 per hour, the total cost is $2,400.

  Recurring costs include maintenance and updates for the software, estimated at 10% of the license cost, resulting in an additional $600. Ongoing labor costs for managing vulnerability scans and penetration tests, with 10 hours per week for 2 employees at $60 per hour, total $62,400 per year. Policy development for penetration testing and vulnerability scanning requires legal and compliance review. Assuming 20 hours of a legal advisor at $100 per hour, the cost is $2,000.

  The total annual cost for implementing regular penetration testing and vulnerability scanning, including training, hardware/software, implementation, recurring costs, and policy development, is approximately $76,400.

- **Maximum Cost**
  The employee training costs increase with a larger team and more comprehensive training. With 10 security engineers receiving training at $1,000 each, the total training cost is $10,000.

  Hardware/software costs increase significantly with high-end penetration testing software like Burp Suite Pro. At approximately $5,000 per license per year, and assuming five licenses for broad coverage, the total hardware/software cost is $25,000. Implementation and configuration become more complex with advanced tools. Assuming 80 hours for setup and configuration by security engineers at $100 per hour, the total cost is $8,000.

  Recurring costs for maintenance, support, and subscription services for premium software are estimated at 15% of the license cost, totaling $3,750. Ongoing labor costs for a larger team managing vulnerability scans and penetration tests, with 20 hours per week for 5 employees at $100 per hour, total $520,000 per year. Policy development is more extensive in this scenario, requiring 40 hours of legal review at $100 per hour, resulting in a cost of $4,000.

  The maximum total annual cost for implementing regular penetration testing and vulnerability scanning, including comprehensive training, high-end hardware/software, advanced implementation, recurring costs, and policy development, is approximately $570,750.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	3,000	10,000
Hardware/Software Cost	6,000	25,000
Implementation & Configuration Cost	2,400	8,000
Recurring Maintenance & Updates Cost	63,000	523,750
Policy Development Cost	2,000	4,000
Total Annual Cost	76,400	570,750

Table 20: Regular Penetration Testing and Vulnerability Scanning Cost Breakdown

12.2 Highly effective

12.2.1 Email Filtering

Email filtering is a critical measure to protect an organization from spam, phishing, and other email-based threats. Email filtering meticulously sorting through incoming emails and quarantining potential threats before they reach our inboxes. These filters analyze emails based on various criterias like Sender Reputation, Attachment Analysis, etc.[35]

- **Minimum Cost**
  The software cost for email filtering is calculated at a rate of $1 per user per month. With 10,600 employees, the annual software cost is $127,200 (10,600 x $1 x 12). Implementation and configuration costs for basic setup and configuration are estimated at $5,000. Maintenance and updates are typically 10% of the software cost, resulting in an annual cost of $12,720 (10% of $127,200).

  Employee training costs consist of training materials, sessions, and employee time. Using existing or low-cost materials, the training material cost is estimated at $1,000. Minimal training sessions using internal staff cost about $2,000 for trainers and logistics. The employee cost for training, with an average hourly rate of $30 and 1 hour of training per employee, totals $318,000 (10,600 x $30 x 1). Policy development is kept to a minimum, using existing templates with minor adjustments. This cost is estimated at $2,000.

  The total minimum annual cost for implementing email filtering, including software, implementation, maintenance, employee training, and policy development, is approximately $466,920.

- **Maximum Cost**
  Software costs for premium email filtering are higher, at a rate of $8 per user per month. With 10,600 employees, the annual software cost is $1,017,600 (10,600 x $8 x 12). Implementation and configuration costs involve advanced setup with expert consultants. This is estimated at $30,000.

  Maintenance and updates for premium software and support typically cost 15% of the software cost, totaling $152,640 (15% of $1,017,600). Employee training costs include customized training materials, professional trainers, and comprehensive sessions. Customised training material cost is estimated at $10,000, while higher-cost training sessions with professional trainers and logistics are estimated at $20,000. The employee time cost for a more extensive 3-hour training session per employee, with an average hourly rate of $30, totals $954,000 (10,600 x $30 x 3).

  Policy development in this scenario requires comprehensive policy development, including legal reviews and high-quality documentation, estimated at $10,000.

The maximum total annual cost for implementing email filtering, including premium software, advanced implementation, extensive maintenance, comprehensive training, and detailed policy development, is approximately $2,194,240.

Description	Minimum Cost($)	Maximum Cost($)
Software Cost	127,200	1,017,600
Implementation & Configuration Cost	5,000	30,000
Maintenance & Updates Cost	12,720	152,640
Employee Training Cost	321,000	984,000
Policy Development Cost	2,000	10,000
Total Annual Cost	466,920	2,194,240

Table 21: Email Filtering Cost Breakdown

12.2.2 Implementation of Secure Backup and Recovery Solutions

Secure backup and recovery solutions are essential to ensure data protection, disaster recovery, and business continuity. Safeguarding user data is paramount, and secure backup and recovery solutions form a critical line of defense.

- **Minimum Cost**
  The employee training costs are focused on System Administrators and IT employees. For System Administrators, the cost is based on 16 hours of training at $60/hour, totaling $960 per administrator. With 10 System Administrators, the total cost is $9,600 (10 x $960). For IT employees, each requires 4 hours of basic training at $50/hour, totaling $200 per employee. With 100 IT employees, the total cost is $20,000 (100 x $200).

  Hardware/software costs for basic cloud-based backup solutions, such as AWS S3 or Google Cloud Storage, are estimated at $1 per GB/month for 100 TB, resulting in an annual cost of $100,000. Implementation and configuration involve outsourced setup, estimated at a flat fee of $50,000. Recurring costs for software updates and routine maintenance are estimated at $10,000/year. Policy development is minimal, assumed to be handled internally with existing staff, resulting in negligible costs.

  The total annual cost for implementing secure backup and recovery solutions, including employee training, hardware/software, implementation, recurring costs, and policy development, is approximately $189,600.

- **Maximum Cost**
  The employee training costs increase with advanced courses and certifications for System Administrators, requiring 40 hours at $60/hour, totaling $2,400 per administrator. With 10 System Administrators, the total cost is $24,000 (10 x $2,400). For IT employees, the cost is $400 per employee for 8 hours of comprehensive training at $50/hour, resulting in a total of $40,000 (100 x $400).

  Hardware/software costs for high-end, enterprise-grade solutions with geo-redundancy, such as AWS Glacier, are estimated at $0.25 per GB/month for 500 TB, leading to an annual cost of $1,500,000. Implementation and configuration costs increase with comprehensive setup, including advanced security features and multi-region redundancy by expert consultants. This is estimated at $200,000. Recurring costs, which cover premium support contracts, frequent updates, and compliance checks, are estimated at $100,000/year.

Policy development involves external consultants to develop and review backup policies and ensure compliance with global data protection regulations, costing approximately $50,000.

The total annual cost for implementing secure backup and recovery solutions, including comprehensive training, high-end hardware/software, advanced implementation, premium recurring costs, and detailed policy development, is approximately $1,914,000.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	29,600	64,000
Hardware/Software Cost	100,000	1,500,000
Implementation & Configuration Cost	50,000	200,000
Recurring Maintenance & Updates Cost	10,000	100,000
Policy Development Cost	2,000	50,000
Total Annual Cost	189,600	1,914,000

Table 22: Secure Backup and Recovery Solutions Cost Breakdown

12.2.3 Intrusion Prevention Systems/ Intrusion Detection Systems

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are critical for identifying and preventing unauthorized access to an organization's network. IDS continuously monitors network traffic, system logs, and user behavior for anomalies that might indicate a potential attack. An IPS goes beyond simply detecting threats; it acts as a proactive security guard, actively preventing them from causing harm[36].

- **Minimum Cost**
  The employee training costs focus on key personnel involved in IPS/IDS operations. The total training cost is $7,560, with 5 security engineers requiring an 8-hour training session, costing $2,280, 3 network engineers costing $1,200, 2 system administrators costing $800, and 10 SOC personnel costing $3,280.

  Hardware/software costs for a basic IPS solution with a single unit and minimal hardware requirements are estimated at $10,000, with basic software licenses and support costing $2,500/year. The total hardware/software cost comes to $12,500. Implementation and configuration require minimal setups by existing IT staff, with two system administrators working a full day (8 hours), costing $800. Recurring costs for basic maintenance and periodic updates amount to $2,500/year. Policy development involves minor additional work by legal and IT personnel, estimated at 5 hours for each at $60/hour, totaling $600.

  The total annual cost for implementing IPS/IDS is approximately $23,960, encompassing employee training, hardware/software, implementation, recurring costs, and policy development.

- **Maximum Cost**
  The employee training costs increase with a larger group and more extensive training sessions, totaling $14,720. This includes 10 security engineers, costing $4,560, 5 network engineers costing $2,000, 4 system administrators costing $1,600, and 20 SOC personnel costing $6,560.

  Hardware/software costs for high-end IPS solutions with robust hardware requirements are estimated at $25,000 for a single unit. Comprehensive software licenses with premium features are estimated at $10,000/year, totaling $35,000. Implementation and configuration by specialized third-party teams for advanced setup cost around $10,000. Recurring costs for comprehensive maintenance and support, including on-site visits and premium support, total $15,000/year. Policy development, involving legal and compliance teams, requires 10 hours for each role at an average of $70/hour, totaling $1,400.

The total maximum annual cost for implementing IPS/IDS, covering comprehensive training, high-end hardware/software, advanced implementation, recurring costs, and detailed policy development, is approximately $76,120.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	7,560	14,720
Hardware/Software Cost	12,500	35,000
Implementation & Configuration Cost	800	10,000
Recurring Maintenance & Updates Cost	2,500	15,000
Policy Development Cost	600	1,400
Total Annual Cost	23,960	76,120

Table 23: IDS/IPS Cost Breakdown

12.2.4 Enhanced Transaction Verification and Behavior Analysis

Enhanced transaction verification and behavior analysis help detect and prevent fraudulent activities in online transactions. It employs advanced algorithms and data analysis techniques to scrutinize every transaction for potential anomalies.

- **Minimum Cost**
  The employee training costs are derived from sessions for various roles. With software engineers/developers, security specialists, data analysts, network engineers, compliance officers, and customer support representatives, the total employee training cost is $7,200. Software engineers and customer support representatives require an 8-hour session costing $200 per person. Security specialists and data analysts require similar training, with a total of $1,000 for each role. Network engineers and compliance officers have a total of $600 each.

  Hardware/software costs are calculated for a basic setup, with low-cost transaction verification software costing $10,000 and a basic server estimated at $5,000, totaling $15,000. Implementation and configuration costs are $8,000, with $5,000 for external consultants and $3,000 for internal labor from two engineers for one week.

  Recurring costs, which include software subscriptions and support, total $3,000 per year. Policy development is minimal, requiring only minor adjustments and compliance checks, estimated at $2,000.

  The total annual cost for implementing enhanced transaction verification and behavior analysis is approximately $35,200.

- **Maximum Cost**
  The employee training costs are higher due to more extensive training sessions. With software engineers/developers, security specialists, data analysts, network engineers, compliance officers, and customer support representatives, the total employee training cost is $27,000. Software engineers and customer support representatives require 8-hour sessions costing $300 per person. Security specialists, data analysts, network engineers, and compliance officers have varied costs, totaling $3,000, $3,000, $1,500, and $1,500, respectively.

Hardware/software costs involve high-end transaction verification software costing $50,000 and high-performance server infrastructure estimated at $20,000, totaling $70,000. Implementation and configuration costs increase, with high-end consultants costing $15,000 and internal labor involving a team of four engineers for one week, costing $12,000. The total implementation and configuration cost is $27,000.

Recurring costs for premium support and software subscriptions are higher, totaling $20,000 per year. Policy development costs increase due to extensive policy work and regulatory compliance, estimated at $10,000.

The total annual cost for implementing enhanced transaction verification and behavior analysis is approximately $154,000.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	7,200	27,000
Hardware/Software Cost	15,000	70,000
Implementation & Configuration Cost	8,000	27,000
Recurring Maintenance & Updates Cost	3,000	20,000
Policy Development Cost	2,000	10,000
Total Annual Cost	35,200	154,000

Table 24: Enhanced Transaction Verification and Behavior Analysis Cost Breakdown

12.2.5 Network Segmentation

Network segmentation is a critical security control that divides an organization's network into smaller, isolated segments. This approach enhances security by limiting unauthorized access and containing potential threats within specific areas of the network. It plays a key role in protecting sensitive data, ensuring compliance with industry regulations.

- **Minimum Cost**
  The employee training cost involves 10 employees, including 5 network engineers and 5 system administrators. Each requires 16 hours of training at an hourly wage of $62.50. The total training cost is $10,000 (10 x 16 x $62.50).

  Hardware/software costs for a basic setup rely on simple VLAN-capable switches and standard routers, with minor additions or upgrades to existing infrastructure. The estimated cost is $5,000. Implementation and configuration involve basic VLAN setup and minimal reconfiguration by a mid-level cybersecurity consulting firm, estimated at $25,000.

  Recurring costs for basic maintenance and updates require a small team to handle issues, costing $2,000 per year. Policy development is minimal, focusing on basic guidelines and simple access control policies, estimated at $3,000.

  The total annual cost for implementing network segmentation with a minimal budget is approximately $45,000.

- **Maximum Cost**
  Employee training costs are higher due to more comprehensive training sessions. With 20 employees, including 10 network engineers and 10 system administrators, each requiring 40 hours of training at $62.50/hour, the total training cost is $50,000 (20 x 40 x $62.50).

Hardware/software costs for an advanced setup involve high-end switches, routers, and security appliances, supporting sophisticated segmentation techniques like VXLAN and SDN. The estimated cost is $200,000. Implementation and configuration include complex network design and integration with top-tier cybersecurity consultants, costing $100,000.

Recurring costs for premium maintenance contracts and frequent updates are estimated at $10,000 per year. Policy development is more comprehensive, with detailed rules and extensive documentation involving legal and compliance teams, estimated at $10,000.

The total annual cost for implementing network segmentation is approximately $370,000.

Description	Minimum Cost($)	Maximum Cost($)
Employee Training Cost	10,000	50,000
Hardware/Software Cost	5,000	200,000
Implementation & Configuration Cost	25,000	100,000
Recurring Maintenance & Updates Cost	2,000	10,000
Policy Development Cost	3,000	10,000
Total Annual Cost	45,000	370,000

Table 25: Network Segmentation Cost Breakdown

12.3 Moderately effective

12.3.1 Regular Vulnerability Assessments

Regular vulnerability assessments help in maintaining a secure platform, protecting user data, and ensuring compliance with industry regulations. These assessments identify potential security vulnerabilities in eBay's infrastructure, applications, and processes, allowing the organization to address weaknesses before they are exploited.

- **Minimum Cost**
  Software tools primarily consist of open-source solutions, minimizing initial setup costs. If paid tools are used, a basic plan like Nessus Professional costs around $2,500/year for a single user.

  External consultants are employed sparingly, typically for annual audits or addressing significant vulnerabilities. The cost for these audits ranges from $5,000 to $10,000, depending on the scope and expertise required. Employee training costs are estimated for 10 employees, including security engineers and IT staff. If training costs $1,000 per employee, the total training cost is $10,000. For 8-hour training sessions, the hourly rate of employees is approximately $50/hour, leading to an additional employee cost of $4,000.

  Recurring costs involve maintenance and support for open-source tools, estimated at $500/year. Regular scans and monitoring can be handled internally, with a basic Security Information and Event Management (SIEM) setup costing around $2,000/year.

  The total annual cost for implementing regular vulnerability assessments, including software tools, external consultants, employee training, and recurring costs, is approximately $24,000 to $29,000.

- **Maximum Cost**
  Software tools encompass top-tier solutions like Tenable.io, starting at around $5,000/year for

5 users. To cover broader scopes, allocate $10,000 to $15,000/year for software licenses and advanced features.

External consultants are hired more frequently, with quarterly or bi-annual audits costing between $10,000 and $20,000 per audit. For quarterly audits, allocate between $40,000 and $80,000/year. Employee training costs are estimated for 20 employees, with each receiving advanced training. If training costs $2,000 per employee, the total training cost is $40,000. For 16-hour sessions, with an hourly rate of $75/hour, the additional employee cost is $24,000.

Recurring costs for advanced maintenance and support are allocated at $5,000/year. Ongoing monitoring with advanced systems requires between $10,000 and $20,000/year.

The total annual cost for implementing regular vulnerability assessments, covering advanced software tools, frequent external consultants, extensive employee training, and recurring costs, is approximately $129,000 to $184,000.

Description	Minimum Cost($)	Maximum Cost($)
Software Tools	2,500	15,000
External Consultants	10,000	80,000
Employee Training Cost	10,000	40,000
Employee Cost for Training	4,000	24,000
Recurring Costs	2,500	25,000
Total Annual Cost	29,000	184,000

Table 26: Regular Vulnerability Assessments Cost Breakdown

12.3.2 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) serves as a centralized platform to collect, analyze, and respond to security-related events and alerts across the organization's infrastructure. [37].

- **Minimum Cost**
  Open-source SIEM software like ELK (Elasticsearch, Logstash, Kibana) is used to reduce licensing costs. If existing hardware cannot be utilized, a basic server setup with adequate storage may be required, estimated at $10,000. Installation and configuration costs for technical labor to set up the SIEM are approximately $5,000.

  Employee training involves 20-25 personnel requiring an 8-hour training session at an average hourly wage of $40/hour. This totals $6,400 (40 x 8 x 20). Maintenance and updates are estimated at $2,000/year, with in-house technical staff performing these tasks. Recurring costs, including potential costs for third-party plugins or tools, are about $1,000/year.

  The total annual cost for implementing SIEM with a minimal budget, covering SIEM software, hardware, installation and configuration, training, maintenance, and recurring costs, is approximately $24,400.

- **Maximum Cost**
  Commercial SIEM software like Splunk is used, with licensing costs ranging from $10,000 to $100,000 depending on features and data volume. An estimated cost for mid-level commercial software is $50,000/year. Hardware costs for high-end servers with redundancy and high storage capacity are estimated at $25,000 for a dual-server setup.

Installation and configuration costs involve professional services for setup and integration, estimated at $15,000. Employee training is more comprehensive, with a 16-hour training session for 25 employees at a higher hourly wage of $60/hour, totaling $24,000 (60 x 16 x 25). Maintenance and updates for professional support and regular software updates cost around $10,000/year. Recurring costs for commercial software licenses and additional services are about $10,000/year.

The total annual cost for implementing SIEM with an unlimited budget, covering advanced software, high-end hardware, professional installation, comprehensive training, maintenance, and recurring costs, is approximately $144,000.

Description	Minimum Cost($)	Maximum Cost($)
Software Cost	-	50,000
Hardware Cost	10,000	25,000
Installation & Configuration Cost	5,000	15,000
Employee Training Cost	6,400	24,000
Maintenance & Updates Cost	2,000	10,000
Recurring Costs	1,000	10,000
Total Annual Cost	24,400	134,000

Table 27: SIEM Cost Breakdown

12.3.3 Continuous Monitoring

Continuous monitoring is essential for maintaining visibility over a network's security posture, detecting anomalies, and responding to incidents in real time.

- **Minimum Cost**
  Open-source monitoring solutions like Nagios are used to reduce costs while providing basic network and server monitoring capabilities. Since Nagios is open-source, there are no licensing costs. The hardware cost for a basic server setup to host Nagios is estimated at $2,000. Installation and configuration by internal IT staff cost around $5,000.

  Employee training costs involve 40 employees, each undergoing 8 hours of training at $25/hour, totaling $8,000. Training material development is estimated at $1,500, and external consultation, if needed, might cost around $3,000. Operational costs consist of maintenance, estimated at $500/year (10% of the setup cost), and monitoring staff salaries, requiring one staff member at an estimated salary of $60,000/year. Policy development involves minimal adjustments, costing around $1,000.

  The total minimum annual cost for implementing continuous monitoring, including software, hardware, installation, training, operational costs, and policy development, is approximately $80,000.

- **Maximum Cost**
  Commercial monitoring platforms like Splunk are used for advanced analytics and big data capabilities. The software cost for a Splunk Enterprise license with a data volume of up to 100 GB/day is around $75,000/year. Installation and configuration require advanced setup, costing about $10,000, and the hardware cost for high-end servers is estimated at $10,000.

  Employee training costs are higher due to advanced training sessions, involving 60 employees with 16 hours of training at $50/hour, totaling $48,000. Training material development and purchase cost about $5,000. External consultation to optimize Splunk might cost around $15,000. Operational costs consist of Splunk maintenance and support fees, which are typically 20% of the license cost, amounting to $15,000/year. Monitoring staff costs increase with two staff members at $80,000/year each, totaling $160,000. Policy development for Splunk requires more extensive work, estimated at $5,000.

The total maximum annual cost for implementing continuous monitoring, including software, hardware, installation, training, operational costs, and policy development, is approximately $343,000.

Description	Minimum Cost($)	Maximum Cost($)
Software Cost	-	75,000
Hardware Cost	2,000	10,000
Installation & Configuration Cost	5,000	10,000
Employee Training Cost	8,000	48,000
External Consultation	4,500	20,000
Operational Costs	60,500	175,000
Policy Development Cost	1,000	5,000
Total Annual Cost	80,000	343,000

Table 28: Continuous Monitoring Cost Breakdown

12.3.4 Threat Intelligence

Threat intelligence involves gathering and analyzing information about potential security threats to proactively protect an organization's assets. It provides valuable insights into the tactics, techniques, and procedures used by cybercriminals and allows eBay to proactively defend against security risks.

- **Minimum Cost**
  Threat intelligence subscriptions focus on basic services. Recorded Future offers basic threat feeds and intelligence reports, with an annual subscription cost of $50,000. This package may include community-based threat sharing and access to online threat databases.

  Employee training costs involve training sessions for 30 employees, each requiring 8 hours of training at an average hourly wage of $44.29. The total training cost is approximately $10,629.60 (30 x 8 x $44.29). External consultation and policy development costs for security consultants providing basic setup and policy development are estimated at 40 hours at $200/hour, totaling $8,000.

  Infrastructure and miscellaneous costs for software setup involve an estimated $10,000 for basic software tools. Assumptions include using existing infrastructure, minimizing additional hardware costs.

  The total annual cost for implementing threat intelligence, including threat intelligence subscriptions, employee training, external consultation, and software setup, is approximately $78,629.60.

- **Maximum Cost**
  FireEye Threat Intelligence provides in-depth threat intelligence with extensive coverage, with an annual subscription cost of $150,000. This covers advanced threat feeds, detailed intelligence reports, and additional threat hunting capabilities.

Employee training costs increase with 50 employees, each requiring 8 hours of training. At the same hourly wage of $44.29, the total training cost is approximately $17,716.32 (50 x 8 x $44.29). External consultation and policy development costs are estimated for 80 hours of premium consultation at $300/hour, totaling $24,000. This covers advanced setup, threat intelligence strategy, and policy development.

Infrastructure and miscellaneous costs are higher, involving advanced software tools estimated at $30,000 and specialized hardware or high-end servers, estimated at $40,000.

The total annual cost for implementing threat intelligence, covering advanced threat intelligence subscriptions, comprehensive employee training, premium external consultation, and advanced infrastructure, is approximately $261,716.32.

Description	Minimum Cost($)	Maximum Cost($)
Subscription Cost	50,000	150,000
Employee Training Cost	10,629	17,716
External Consultation	8,000	24,000
Software Cost	10,000	30,000
Hardware Cost	-	40,000
Total Annual Cost	78,629	261,716

Table 29: Threat Intelligence Cost Breakdown

12.3.5 User and Entity Behavior Analytics (UEBA) systems

User and Entity Behavior Analytics (UEBA) systems help detect abnormal user behavior and potential security threats within an organization[38]. UEBA systems use advanced analytics, machine learning, and big data techniques to detect unusual patterns in user and entity activity, providing valuable insights into potential security incidents.

- **Minimum Cost**
  The hardware/software costs are kept low by using open-source or lower-cost UEBA solutions. A typical low-cost UEBA system costs between $10,000 and $15,000 per year. Hardware costs are minimized by operating on existing infrastructure.

  Employee training costs involve training 10 employees, with an hourly rate of about $45 (based on a $90,000/year salary). For an 8-hour training session, the total cost is $3,600 (10 x 8 x $45). Policy development involves senior-level personnel, with 20 hours at $80/hour, resulting in a cost of $1,600. Maintenance costs for minimal UEBA are focused on software updates and basic monitoring, estimated at $1,000/year. Miscellaneous costs for smaller updates or contingency are estimated at $500.

  The total annual cost for implementing UEBA systems, including hardware/software costs, employee training, policy development, maintenance, and miscellaneous costs, is approximately $21,700/year.

- **Maximum Cost**
  The hardware/software costs are higher due to investment in high-end UEBA systems with advanced features and robust support. High-end UEBA solutions can cost between $50,000 and $100,000 per year. The hardware costs for a high-end server setup are around $15,000.

Employee training costs increase with 20 employees requiring 8 hours of training, totaling $7,200 (20 x 8 x $45). Policy development requires a broader implementation, estimated at 20 hours at $100/hour, resulting in $2,000. Maintenance costs for advanced support and 24/7 assistance are about $10,000/year. Miscellaneous costs for additional software, backup hardware, or extra resources are estimated at $5,000.

The total annual cost for implementing UEBA systems, covering high-end software, advanced hardware, extensive employee training, comprehensive policy development, maintenance, and miscellaneous costs, is approximately $114,200/year.

Description	Minimum Cost($)	Maximum Cost($)
Software Cost	15,000	75,000
Hardware Cost	-	15,000
Employee Training Cost	3,600	7,200
Policy Development Cost	1,600	2,000
Maintenance Cost	1,000	10,000
Miscellaneous Costs	500	5,000
Total Annual Cost	21,700	114,200

Table 30: UEBA System Cost Breakdown

12.4 Supportive and procedural

12.4.1 Implementation of Security Policies and Training

Security policies and training are fundamental to eBay's security framework, ensuring that employees understand their roles and responsibilities in maintaining a secure environment. Effective policies provide a clear set of guidelines, while comprehensive training ensures that employees are equipped to follow these policies.

- **Minimum Cost**
  The employee time costs are calculated for 6,603 IT employees, each undergoing two 4-hour training sessions per year. With an average hourly wage of $40/hour, the annual cost for each employee is $320 (40 x 4 x 2). The total employee time cost for all employees is $2,112,960 (320 x 6,603).

  Training materials for a minimal budget are $10 per employee per session, resulting in $20 per year for each employee. The total cost for training materials for all employees is $132,060 (20 x 6,603). Trainer fees are calculated at $1,000 per session, with 150 sessions required for all employees, totaling $150,000 (1,000 x 150).

  The total annual cost for implementing security policies and training, including employee time, training materials, trainer fees, and administrative overheads, is approximately $10,176,000.

- **Maximum Cost**
  The employee time costs remain the same as the minimal budget, totaling $2,112,960 (320 x 6,603). However, training materials cost more, at $20 per employee per session, resulting in $40 per year for each employee. The total cost for all employees is $264,120 (40 x 6,603).

  Trainer fees for high-quality trainers are estimated at $5,000 per session, with the same number of sessions (150), totaling $750,000 (5,000 x 150).

The total annual cost for implementing security policies and training, including employee time, training materials, trainer fees, and administrative overheads, is approximately $13,992,000.

Description	Minimum Cost($)	Maximum Cost($)
Employee Time Cost	2,112,960	2,112,960
Training Materials Cost	132,060	264,120
Trainer Fees	150,000	750,000
Total Annual Cost	2,395,020	3,127,080

Table 31: Implementation of Security Policies and Training Cost Breakdown

12.4.2 Secure Storage and Handling of Logs and Evidence

Secure storage and handling of logs and evidence are critical for maintaining data integrity and ensuring compliance with regulatory requirements. It ensures that sensitive information, logs, and evidence related to security incidents are properly protected, stored, and accessible for audits or investigations.

- **Minimum Cost**
  Policy development costs are calculated for 40 hours of work by a mid-level compliance officer, costing $3,000 (75 x 40). Employee training involves key personnel (10 people), each requiring 8 hours of training at $50/hour, totaling $4,000 (10 x 8 x 50).

  Storage infrastructure uses a basic cloud-based storage service with encryption, costing $50/month per terabyte. With 5 terabytes of storage, the yearly cost is $3,000 (5 x 50 x 12). Additional security measures include basic encryption and secure access control, totaling $3,000 (2,000 for encryption + 1,000 for access control). Maintenance and monitoring involve minimal upkeep, with 2 hours of maintenance monthly, costing $1,200 (50 x 2 x 12), and monitoring software costing $1,000/year.

  The total annual cost for implementing secure storage and handling of logs and evidence, including policy development, employee training, storage infrastructure, additional security, maintenance, and monitoring, is approximately $15,200.

- **Maximum Cost**
  Policy development costs are calculated for 80 hours of work by higher-level compliance officers at $150/hour, resulting in a total cost of $12,000 (150 x 80). Employee training involves 100 personnel across different departments, each requiring 16 hours of training at $100/hour, totaling $160,000 (100 x 16 x 100).

  Storage infrastructure uses a high-end secure cloud storage solution with extensive encryption and redundancy features, costing $200/month per terabyte. With 10 terabytes of storage, the yearly cost is $24,000 (10 x 200 x 12). Advanced security measures involve advanced encryption costing $10,000/year and biometric access control setup costing $15,000, with an additional $5,000/year for maintenance.

  Maintenance and monitoring require a dedicated team. Assuming two full-time staff dedicated to this task, each at $100,000/year, the total maintenance cost is $200,000. Additional monitoring software with sophisticated features costs $10,000/year.

  The total annual cost for implementing secure storage and handling of logs and evidence, including policy development, extensive training, advanced storage infrastructure, high-end security, and dedicated maintenance and monitoring, is approximately $431,000.

Description	Minimum Cost($)	Maximum Cost($)
Policy Development Cost	3,000	12,000
Employee Training Cost	4,000	160,000
Storage Infrastructure Cost	3,000	24,000
Additional Security Cost	3,000	25,000
Maintenance & Monitoring Cost	2,200	210,000
Total Annual Cost	15,200	431,000

Table 32: Secure Storage and Handling of Logs and Evidence Cost Breakdown

12.4.3 Incident Response

Incident response involves a coordinated approach to addressing and mitigating security incidents. It involves detecting, analyzing, containing, eradicating, and recovering from security breaches or incidents to minimize damage and restore normal operations swiftly.

- **Minimum Cost**
  Policy development is estimated at 40 hours at $75/hour, costing $3,000. Employee training involves training sessions for 50 employees, with 10 hours of training at $60/hour, totaling $30,000. Drills and exercises require 2 drills/year, with 10 hours per drill, costing $60,000 (10 x 60 x 50). Training facilitators cost $10,000 per session, totaling $20,000 for 2 sessions.

  The incident response team has 3-4 dedicated team members, with an annual salary of $120,000 each, totaling $480,000. Equipment and tools for the team are estimated at $10,000, using open-source software. Software and tools include additional training (250 hours at $60/hour) costing $15,000, and hiring 1 additional technician for support at $100,000/year.

  Incident response plan development costs $10,000 with external consultants, and annual updates and revisions for 4 team members cost about $5,000. Additional costs for miscellaneous expenses and emergencies are estimated at $5,000.

  The total annual cost for implementing incident response, including policy development, employee training, incident response team, software and tools, and additional costs, is approximately $735,000.

- **Maximum Cost**
  Policy development involves 80 hours at $150/hour, costing $12,000. Employee training for 60 employees, with 20 hours of training at $60/hour, totals $72,000. Drills and exercises require 4 drills/year, with 15 hours per drill, costing $216,000 (15 x 60 x 60). Training facilitators cost $20,000 per session, totaling $80,000 for 4 sessions.

  The incident response team has 6-8 dedicated team members, with salaries totaling $960,000 (8 x 120,000). Premium equipment and tools cost $50,000. Software and tools involve premium incident response tools with annual licensing costs of $150,000, and hiring 2 experienced technicians at $150,000 each, totaling $300,000.

  Incident response plan development with premium external consultants costs $50,000, and annual updates and revisions cost about $10,000 for 8 team members. Additional costs for miscellaneous expenses are estimated at $20,000.

  The total annual cost for implementing incident response, including policy development, employee training, incident response team, software and tools, and additional costs, is approximately $1,908,000.

Description	Minimum Cost($)	Maximum Cost($)
Policy Development Cost	3,000	12,000
Employee Training Cost	90,000	288,000
Trainer Fees Cost	20,000	80,000
Incident Response Team Cost	490,000	1,010,000
Software and Tools Cost	115,000	450,000
Additional Costs	5,000	20,000
Total Annual Cost	735,000	1,860,000

Table 33: Incident Response Cost Breakdown

12.4.4 Continuous Monitoring of Legal and Regulatory Changes

Continuous monitoring of legal and regulatory changes is essential to ensure compliance with evolving laws, regulations, and industry standards. This process involves staying updated with legal developments and integrating them into eBay's operations and security practices.

- **Minimum Cost**
  Compliance software costs around $10,000/year, offering basic monitoring of legal and regulatory changes. The compliance team comprises 15 employees at a mid-level salary of $80,000/year per employee, totaling $1,200,000/year. Training costs are calculated at $25/hour for 16 hours, resulting in $10,000 (25 x 25 x 16).

  Documentation and reporting tools are estimated at $5,000/year, providing basic capabilities. Consultants/legal experts are engaged on a limited basis, costing $15,000/year. Operational impact is minimal due to the implementation of basic controls.

  The total annual cost for continuous monitoring of legal and regulatory changes, including compliance software, compliance team, training, documentation and reporting tools, consultants/legal experts, and operational impact, is approximately $2,540,000.

- **Maximum Cost**
  Advanced compliance software with extensive features costs around $50,000/year, providing real-time monitoring and comprehensive support. Keeping the same employee cost as the above.

  Advanced training programs are calculated at $50/hour for 16 hours, resulting in $20,000 (25 x 50 x 16). Advanced documentation and reporting tools are estimated at $20,000/year, offering robust reporting features. Consultants/legal experts are extensively engaged, costing around $50,000/year. The operational impact is significant due to the extensive implementation and training required.

  The total annual cost for continuous monitoring of legal and regulatory changes, including advanced compliance software, expanded compliance team, advanced training programs, comprehensive documentation and reporting tools, extensive consultants/legal experts, and operational impact, is approximately $3,890,000.

12.4.5 Document Classification and Handling Policies

Document classification and handling policies are crucial for ensuring that sensitive information is properly managed and protected. These policies dictate how documents are classified, stored, accessed, and shared within the organization, ensuring compliance with data protection regulations and reducing the risk of unauthorized access or data breaches.

Description	Minimum Cost($)	Maximum Cost($)
Compliance Software Cost	10,000	50,000
Compliance Team Cost	1,200,000	1,200,000
Training Cost	10,000	20,000
Documentation and Reporting Tools Cost	5,000	20,000
Total Annual Cost	1,225,000	1,290,000

Table 34: Continuous Monitoring of Legal and Regulatory Changes Cost Breakdown

- **Minimum Cost**
  Policy development costs are calculated for 40 hours at a rate of $50/hour, totaling $2,000. Employee training involves training sessions for 10,600 employees, each requiring 2 hours of training at $50/hour, totaling $1,060,000 (10,600 x 2 x 50). The cost for training material development and internal trainers is estimated at $10,000.

  Security tools for a minimal budget include a basic Data Loss Prevention (DLP) software license costing $50,000/year. Monitoring and auditing for internal audits require 60 hours at a rate of $50/hour, totaling $3,000. Additional costs for miscellaneous expenses or unexpected resources are estimated at $5,000.

  The total annual cost for implementing document classification and handling policies, including policy development, training, security tools, monitoring, auditing, and additional costs, is approximately $1,150,000.

- **Maximum Cost**
  Policy development involves 40 hours at a rate of $100/hour, totaling $4,000. External consultants are hired for expert consultation, costing $20,000. Employee training costs increase due to 2 hours of training for 10,600 employees at $100/hour, totaling $2,120,000. High-quality training materials and external trainers cost about $50,000.

  Security tools for a premium DLP solution with advanced features are estimated at $200,000/year. Additional software tools to support document classification and compliance cost about $50,000. Monitoring and auditing involve 60 hours at $100/hour for internal audits, costing $6,000, and premium external audit services costing $50,000. Additional costs for miscellaneous expenses or luxury resources are estimated at $20,000.

  The total annual cost for implementing document classification and handling policies, including advanced policy development, comprehensive training, high-end security tools, monitoring, auditing, and additional costs, is approximately $2,520,000.

12.5 Audit

12.5.1 IT Security Audits

SOC Type 2 IT security audits evaluate how well a company's controls function over a specified period, typically three to 12 months. These audits assess both the design of controls and their operating effectiveness. The cost of a Type 2 audit for large organizations can typically range from $30,000 to $100,000[39].

- **Minimum Cost**
  Assuming a minimal budget, the cost is estimated at $30,000. Audit tools for basic software

Description	Minimum Cost($)	Maximum Cost($)
Policy Development Cost	2,000	4,000
External Consultant Cost	-	20,000
Employee Training Cost	1,060,000	2,120,000
Training Material & External Trainers Cost	10,000	50,000
Security Tools Cost	50,000	200,000
Additional Software Cost	-	50,000
Internal Audit Cost	3,000	6,000
External Audit Cost	-	50,000
Miscellaneous Costs	5,000	20,000
Total Annual Cost	1,150,000	2,520,000

Table 35: Document Classification and Handling Policies Cost Breakdown

are estimated at $10,000, providing the necessary resources for effective audits. Travel and miscellaneous expenses for local audits require minimal travel, costing around $10,000.

Employee time for audits assumes 10 employees at different levels, with an hourly rate of $45. Given that a Type 2 audit requires a more extensive evaluation, let's assume 40 hours per employee, resulting in a total employee cost of $18,000 (10 x 40 x 45).

The total annual cost for implementing Type 2 IT security audits, including external auditors, audit tools, travel and miscellaneous expenses, and employee time for audits, is approximately $68,000.

- **Maximum Cost**
  External auditors can be hired from top-tier auditing firms with specialized skills. The cost for a premium audit firm conducting a Type 2 audit can range from $30,000 to $100,000. Assuming an unlimited budget, the cost is estimated at $100,000.

  Audit tools for high-end software with more features are estimated at $50,000, providing advanced capabilities for comprehensive audits. Travel and miscellaneous expenses for global audits require more extensive travel, costing around $50,000.

  Employee time for audits assumes 15 employees at higher levels, with an hourly rate of $60. If each audit requires 40 hours, the total employee cost is $36,000 (15 x 40 x 60).

  The total annual cost for implementing Type 2 IT security audits, covering premium external auditors, high-end audit tools, extensive travel and miscellaneous expenses, and employee time for audits, is approximately $236,000.

Description	Minimum Cost($)	Maximum Cost($)
External Auditors Cost	30,000	100,000
Audit Tools Cost	10,000	50,000
Miscellaneous Expenses	10,000	50,000
Employee Time Cost	18,000	36,000
Total Annual Cost	68,000	236,000

Table 36: IT Security Audits Cost Breakdown

12.5.2 Third Party Audits

Third-party audits provide an external perspective on the platform's security posture, compliance, and risk management practices. These audits involve independent organizations or experts assessing security controls, policies, and operations to ensure they meet industry standards and regulatory requirements.

- **Minimum Cost**
  These audits are basic, focusing on general compliance checks. The scope is limited, covering a smaller number of vendors or focusing on specific areas of concern, requiring fewer resources and less time.

  External auditor fees, if required, range from $100 to $200 per hour, with total costs influenced by the number of audits and the duration. Internal audits rely on existing security personnel, reducing costs. Travel expenses are minimal since audits can be conducted remotely or in centralized locations. Additional costs, including minor expenses, training, and materials, contribute to the total cost.

  The estimated cost for this scenario is derived from auditor fees of $30,000, internal staff costs of $40,000, travel expenses of $10,000, and miscellaneous costs of $10,000.

- **Maximum Cost**
  Here the audits are comprehensive, with in-depth assessments and extensive use of external auditors. The scope covers a wide range of vendors, with detailed security checks, requiring more resources and time.

  External auditor fees range from $200 to $500 per hour, with costs influenced by the level of specialization and audit duration. Internal staff costs are higher due to dedicated internal personnel for coordination and support, potentially requiring additional hires. Travel expenses are significant due to external auditors visiting multiple vendor locations. Additional costs include training, audit-related software, and consultants for complex processes.

  The estimated cost range for this scenario includes auditor fees of $100,000, internal staff costs of $70,000, travel expenses of $50,000, and additional costs of $50,000.

Description	Minimum Cost($)	Maximum Cost($)
Auditor Fees	30,000	100,000
Internal Staff Costs	40,000	70,000
Travel Expenses	5,000	50,000
Additional Costs	10,000	50,000
Total Annual Cost	85,000	300,000

Table 37: Third Party Audits Cost Breakdown

12.5.3 Compliance Audits

Compliance audits involve a thorough review of the organization's policies, procedures, and practices to ensure adherence to legal and regulatory requirements. These audits are important for protecting against legal liabilities, and promoting best practices in security and governance..

- **Minimum Cost**
  Assuming External compliance officers conduct the audits, with each compliance officer costing

around $20,000/employee (including salary and benefits). Assuming 5 compliance officers, the total cost is $100,000 (20,000 x 5).

Audit tools are basic, with an estimated cost of $10,000 for compliance tracking tools. Travel and miscellaneous expenses are minimal, focusing on local audits, costing around $10,000. Employee time for audits involves 6 employees assisting in compliance checks, with an hourly rate of $45. Assuming 20 hours per audit, the total employee cost is $5,400 (6 x 20 x 45).

The total annual cost for compliance audits, including internal auditors, audit tools, travel, and employee time, is approximately $295,400.

- **Maximum Cost**
  External auditors from premium compliance auditing firms are used. The cost for a premium audit firm is approximately $100,000 per audit. Assuming 2 audits a year, the total cost is $200,000 (150,000 x 2).

  Audit tools are high-end, with premium compliance management software costing about $30,000. Travel and miscellaneous expenses are higher due to global audits requiring extensive travel, costing around $20,000. Employee time for audits involves 10 senior-level employees, with an hourly rate of $60. Assuming 30 hours per audit, the total employee cost is $18,000 (10 x 30 x 60).

  The total annual cost for compliance audits with an unlimited budget, including premium external auditors, high-end audit tools, extensive travel, and senior-level employee time, is approximately $708,000.

Description	Minimum Cost($)	Maximum Cost($)
Auditors Cost	100,000	200,000
Audit Tools Cost	10,000	30,000
Travel and Miscellaneous Expenses	10,000	20,000
Employee Time Cost	5,400	18,000
Total Annual Cost	125,400	268,000

Table 38: Compliance Audits Cost Breakdown

13 CATEGORIZING CONTROLS IN GROUPS

The following grouping organizes the list of security controls into coherent sets, each addressing specific aspects of an overall security strategy. The overall cost for each group is calculated considering only the desired control sets. The grouping considers how certain controls can address multiple risks, while others have a narrower focus.

1. **NETWORK & INFRASTRUCTURE SECURITY**
   This group addresses the core infrastructure that underpins eBay's network. Controls in this group focus on establishing and maintaining a secure network architecture, including segmenting networks, enforcing secure configurations, and implementing protective systems like Web Application Firewalls (WAF). This group is critical to prevent unauthorized access, ensure network resilience, and maintain a robust defense against external threats.

   - Multi-Factor Authentication (MFA)

- Network Segmentation
- Secure Configuration Management
- Patch Management Systems
- Intrusion Prevention Systems (IPS)
- Intrusion Detection Systems (IDS)
- Web Application Firewalls (WAF)
- Secure Backup and Recovery Solutions

2. **DATA PROTECTION & ENCRYPTION**
   This group encompasses controls that safeguard data throughout its lifecycle. The controls aim to ensure secure communication, enforce encryption standards, and handle sensitive data with care. This group covers everything from encrypted communication protocols to secure handling of logs and sensitive information. It plays a pivotal role in protecting customer data and ensuring compliance with data protection regulations.

   - Encryption
   - Secure Storage and Handling of Logs and Evidence
   - Email Filtering
   - Content Security Policy (CSP)

3. **TRAINING, COMPLIANCE & POLICY ENFORCEMENT**
   Controls in this group are focused on maintaining compliance with industry standards and regulations. This group includes implementing and enforcing security policies, conducting various audits to ensure compliance, and providing security training to employees. The objective is to maintain a culture of compliance and ensure that eBay meets all legal and regulatory requirements.

   - Enforcement of Access Controls and User Authentication
   - Implementation of Security Policies and Training
   - Continuous Monitoring of Legal and Regulatory Changes
   - Compliance Audits
   - IT Security Audits

4. **THREAT DETECTION & RESPONSE**
   This group is dedicated to identifying and responding to security threats. Controls include Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), regular penetration testing, and robust incident response procedures. The goal is to detect threats early and respond quickly to minimize damage, ensuring eBay's systems are monitored and secure against internal and external threats.

   - Security Information and Event Management (SIEM)
   - Enhanced Transaction Verification and Behavior Analysis
   - Regular Penetration Testing and Vulnerability Scanning
   - User and Entity Behavior Analytics (UEBA) systems
   - Incident Response

5. **VENDOR & THIRD-PARTY RISK MANAGEMENT**
   This group focuses on managing the risks associated with vendors and third-party entities. The controls ensure that eBay's relationships with external parties are secure and compliant with security policies. This involves assessing vendor risk, implementing secure procurement processes, and conducting third-party audits to ensure that external entities meet eBay's security standards.

   - Vendor Risk Management and Secure Procurement Processes
   - Third Party Audits

6. **LOGGING, MONITORING & ANALYTICS**
   This group is dedicated to continuous monitoring and analysis of security data. Controls in this group ensure that logs are handled securely, incidents are tracked, and threat intelligence is continuously monitored. The objective is to maintain situational awareness and ensure that eBay has the tools and practices needed to detect and respond to emerging threats.

   - Continuous Monitoring
   - Threat Intelligence

Control	Total Group Cost ($)
Network & Infrastructure Security	5,517,870
Data Protection & Encryption	4,211,640
Training, Compliance & Policy	7,715,080
Threat Detection & Response	2,832,950
Vendor & Third Party Management	418,800
Logging, Monitoring & Analysis	604,716
Total Cost	21,301,056

Table 39: Categorized Cost Breakdown

14 BUDGET SCENARIO

These budgets demonstrate varying levels of security, from a minimal cost that focuses on the most critical controls, to a practical cost that balances between minimal and unlimited, to a budget with no restrictions, covering all potential security risks. Each budget profile comes with certain risks and trade-offs based on the level of security provided.

14.1 Minimal Cost Budget

The minimal budget scenario for eBay addresses the most critical security controls, focusing on the most pressing risks. This budget profile is designed to maintain a basic level of security while minimizing costs. It doesn't aim for comprehensive security but provides a baseline solution to protect essential assets and ensure some compliance with regulatory requirements. Considering only the lower end of the cost for essential controls for minimal budget calculation. Most of the controls use open-source software or cloud based implementation, hence reducing the hardware and software cost.

1. Network & Infrastructure Security:
    - Multi-Factor Authentication (MFA): $70,150
    - Network Segmentation: $45,000
    - Secure Backup and Recovery Solutions: $189,600
2. Data Protection & Encryption:
    - Encryption: $136,300
    - Content Security Policy (CSP): $227,000
3. Training, Compliance & Policy Enforcement:
    - Access Controls and User Authentication: $953,000
    - Compliance Audits: $125,400
4. Threat Detection & Response:
    - Security Information and Event Management (SIEM): $24,400
    - Regular Penetration Testing and Vulnerability Scanning: $76,400
5. Vendor & Third-Party Risk Management:
    - Vendor Risk Management and Secure Procurement Processes: $31,200
6. Logging, Monitoring & Analytics:
    - Continuous Monitoring: $80,000

Total = $304,750 + $363,300 + $1,078,400 + $100,800 + $31,200 + $80,000 = $1,958,450

Unaddressed Risk and Trade-offs: This budget lacks comprehensive incident response and investigation procedures, leading to a delayed response to security incidents. The use of basic Security Information and Event Management (SIEM) and minimal regular penetration testing may not capture all potential threats. With limited focus on compliance audits and policy enforcement, this budget might face risks from non-compliance with regulatory requirements. Limited attention to vendor risk management and secure procurement processes increases the risk of third-party vulnerabilities. While this budget is cost-effective, it compromises on certain critical security controls. The minimal budget might not have backup or redundancy for essential systems, leading to higher risks during failure or attack. This budget relies on basic controls, which may not offer the same level of protection as more advanced systems.

Comparing the budget to similar marketplace organizations, this budget might be seen in more smaller or risk tolerant organizations that have fundamental security measures in place but give more priority to low cost.

14.2 Practical Budget

The practical budget for eBay's security controls aims to balance security and cost. It addresses critical risks with a reasonable level of security while avoiding excessive expenditure. This budget scenario includes controls that provide comprehensive coverage for essential security aspects, offering a practical approach to managing risks.

1. Network & Infrastructure Security:
   - Multi-Factor Authentication (MFA): $484,100
   - Network Segmentation: $300,000
   - Secure Configuration Management: $1,102,600
   - Patch Management Systems: $542,600
   - Secure Backup and Recovery Solutions: $1,914,000
2. Data Protection & Encryption:
   - Encryption: $835,000
   - Secure Storage and Handling of Logs and Evidence: $431,000
   - Email Filtering: $2,194,240
3. Training, Compliance & Policy Enforcement:
   - Access Controls and User Authentication: $953,000
   - Implementation of Security Policies and Training: $2,395,020
   - Continuous Monitoring of Legal and Regulatory Changes: $1,225,000
4. Threat Detection & Response:
   - Security Information and Event Management (SIEM): $134,000
   - Enhanced Transaction Verification and Behavior Analysis: $154,000
   - Regular Penetration Testing and Vulnerability Scanning: $570,750
   - Incident Response: $1,860,000
5. Vendor & Third-Party Risk Management:
   - Vendor Risk Management and Secure Procurement Processes: $118,800
   - Third Party Audits: $300,000
6. Logging, Monitoring & Analytics:
   - Continuous Monitoring: $343,000
   - Threat Intelligence: $261,716

Total = $4,343,400 + $3,460,240 + $4,572,020 + $2,718,750 + $418,800 + $604,716 = $16,117,926

Unaddressed Risk and Trade-offs: This budget includes incident response but may lack the robustness and flexibility to respond to large-scale or complex incidents. Although it includes regular penetration testing and more advanced SIEM, this budget might not cover all potential threat vectors. The practical budget covers compliance but might not fully address all audit requirements or legal regulations. The budget might still have limited resources for extensive third-party audits or vendor risk assessments. This budget balances security with cost, but it might not provide comprehensive security coverage. his budget may lack extensive redundancy and backup, which could increase risks during system failures or attacks. While providing more security controls, this budget could lead to higher maintenance and support costs.

E-commerce businesses like Shopify and Walmart might lean towards a practical budget focusing on a balanced range of security controls that provide substantial protection without the extensive costs associated with the highest tier of security spending.

14.3 Money No Object Budget

The "money no object" budget scenario involves implementing a comprehensive security framework, focusing on achieving the highest level of security without financial constraints. For this we can assume all the high end cost for each of the controls described. These controls are meticulously designed and encompassing, aiming to mitigate a wide array of risks with utmost efficiency and effectiveness.

Total = $5,517,870 + $4,211,640 + $7,785,080 + $2,832,950 + $418,800 + $604,716 = $21,371,056

Unaddressed Risk and Trade-offs: The comprehensive nature of this budget might lead to high system complexity, increasing the risk of configuration errors and security gaps. Even with extensive controls, some risks, such as zero-day vulnerabilities or insider threats, cannot be completely mitigated. This budget is the most expensive, which could impact the company's overall financial performance. The extensive use of resources and personnel might lead to operational inefficiencies or over staffing.

Large world-wide enterprises like Amazon would likely invest in securiyt at a level comparable to eBay's "Money No Object" budget. As these companies require utmost security measures due to their massive scale, high transaction volume, and the sensitive nature of the data they handle.

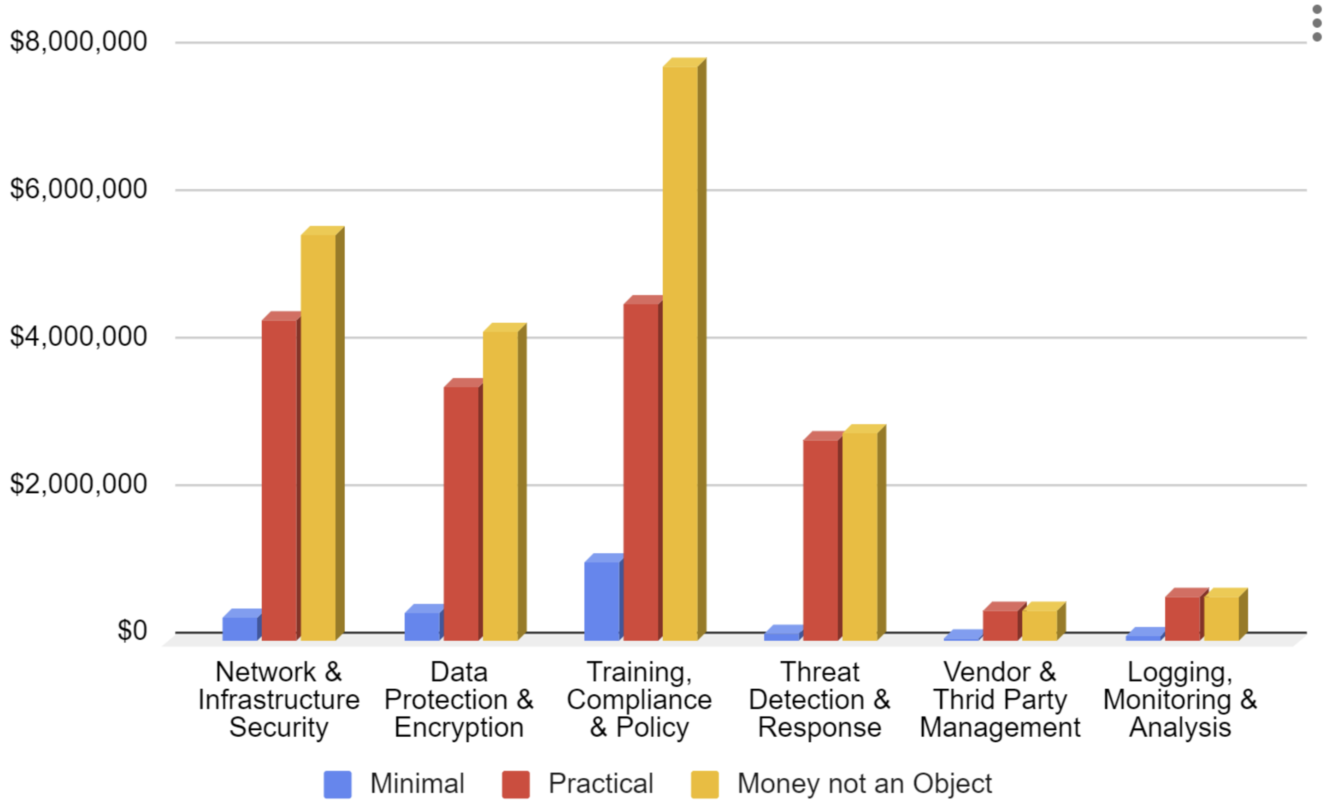


Figure 7: Three Budget Scenario

References

[1] Organization for Economic Co-operation and Development .

[2] International Finance Corporation - Interpretation Note on Small and Medium Enterprises and Environmental and Social Risk Management .

[3] Corporate Finance Institue - Small and Medium-sized Enterprises (SMEs).

[4] Gartner - Small And Midsize Business (SMB).

[5] Investopedia - What Is a Business? Understanding Different Types and Company Sizes.

[6] Digital Resources - Small, Medium, or Large: Does Business Size Matter?

[7] Vocalcom - Key Differences Between the SMB, SME and Large Enterprise .

[8] Cubeler - What's the Difference Between an SMB vs. an SME?

[9] CustomerGlu - zoominfo .

[10] CustomerGlu - crunchbase .

[11] UniSwap - zoominfo .

[12] UniSwap - growjo .

[13] UniSwap - crunchbase .

[14] UniSwap - zoominfo .

[15] UpGuard Security Report .

[16] Aeroleads email search .

[17] Shodan.io-1 .

[18] Shodan.io-2 .

[19] Controls List with addressed Vulnerabilities Sheet .

[20] Vulnerability List with all types of controls Sheet .

[21] What does MFA cost to implement and maintain?

[22] Best Practices in Web Development.

[23] What is Access Control?

[24] Content Security Policy (CSP) - HTTP: MDN.

[25] Patch Management: Benefits and Best Practices.

[26] What Is Network Segmentation?

[27] Budgeting for SOC 2: How Much Does a SOC 2 Audit Cost?

[28] Budget sheet on yearly bases .

[29] Glassdoor - Ebay Salaries .

[30] Top 12 Web Application Firewall (WAF) Solutions.

[31] What is MFA and how does it work?

[32] List of Top Vendor Risk Management Software 2024.

[33] How Much Does Patch Management Software Cost?

[34] How Much Does Penetration Testing Cost? 11 Pricing Factors.

[35] How Much Does Email Security Cost? Common Email Protection Fees Expenses.

[36] 6 Best Intrusion Detection & Prevention Systems for 2024.

[37] How Much is Your SIEM Solution Costing You?

[38] Best User and Entity Behavior Analytics (UEBA) Software.

[39] Different Audit Types.