# The Challenges Posed by CybersecurityRoles in Adopting Digital Transformation

## التحديات التي تفرضها أدوار الأمن السيبراني في تبني التحول الرقمي

**Benabed Radouan[1], Amer Abderrahmen[2]**
[1] Mascara University, benabedredouane6@gmail.com,
[2]Oran 2 University, amereabderrahmen@gmail.com,
Received on: 30/12/2024 Accepted on:06/05/2026 published on: 31/05/2026

***Abstract***:
The integration of technology and digital practices within economic institutions has brought forth a paradigm shift in the way these entities operate, communicate, and safeguard their assets. This academic abstract provides an overview of the intersection between technology, digital practices, and cybersecurity in the context of economic institutions. It explores the critical role of cybersecurity in protecting sensitive financial data, customer information, and critical infrastructure within these institutions. Furthermore, the abstract highlights the evolving threat landscape, characterized by sophisticated cyberattacks and nation-state actors, and emphasizes the importance of robust cybersecurity measures, compliance frameworks, and ethical considerations. As economic institutions navigate this dynamic digital landscape, they must recognize cybersecurity as an integral component of their operations, essential for preserving trust, privacy, and financial stability in an interconnected world,vital for maintaining financial stability, trust, and privacy in a linked society

***Keys words***: **Digital Practices,Cyber-Security Workforce, Digital Environments**
***JEL classification codes***:L86;G21; K42; O33.

**ملخص**:أدى دمج التكنولوجيا والممارسات الرقمية في المؤسسات الاقتصادية إلى حدوث تحول جذري في طريقة عمل هذه الكيانات وتواصلها وحماية أصولها. يقدم هذا الملخص الأكاديمي نظرة عامة على التقاطع بين التكنولوجيا والممارسات الرقمية والأمن السيبراني في سياق المؤسسات الاقتصادية. ويستكشف الدور الحاسم للأمن السيبراني في حماية البيانات المالية الحساسة ومعلومات العملاء والبنية التحتية الحيوية داخل هذه المؤسسات. علاوة على ذلك، يسلط المقال الضوء على المشهد المتطور للتهديدات، المتعلقة بهجمات إلكترونية متطورة وأطراف فاعلة من أطرافقومية، ويؤكد على أهمية تدابير الأمن السيبراني القوية وأطر الامتثال والاعتبارات الأخلاقية. بينما تتنقل المؤسسات الاقتصادية في هذا المشهد الرقمي الديناميكي، يجب عليها أن تدرك أن الأمن السيبراني هو جزء لا يتجزأ من عملياتها، وهو ضروري للحفاظ على الثقة والخصوصية والاستقرار المالي في عالم مترابط، وهو أمر حيوي للحفاظ على الاستقرار المالي والثقة والخصوصية في مجتمع مترابط.

**الكلمات المفتاحية**:**الممارسات الرقمية، القوى العاملة في مجال الأمن السيبراني، البيئات الرقمية.**
**تصنيف JEL**: L86، G21، K42، O33.

***Corresponding author***: **Amer Abderrahmen**, ***e-mail:***amereabderrahmen@gmail.com

## 1-Introduction

Economic institutions, including banks, financial markets, government agencies, and corporations, have historically played pivotal roles in the global economy. However, the advent of technology and the widespread adoption of digital practices have ushered in a new era for these institutions. This paper aims to elucidate the multifaceted influence of technology and digitalization on economic institutions and their functions.

The emergence of digital technology has fundamentally transformed the traditional banking and financial services landscape. Digital banking, often referred to as "online banking" or "e-banking," is a contemporary manifestation of this transformation. It encompasses a wide range of banking activities and services conducted electronically, facilitated by the internet and mobile devices.

E-commerce, short for electronic commerce, has emerged as a transformative force in the retail industry, altering consumer behavior, supply chain dynamics, and business models. This paper provides an academic analysis of e-commerce's impact on the retail sector, exploring the evolution of online shopping, its key drivers, advantages, and challenges. Additionally, it discusses the implications of e-commerce for traditional brick-and-mortar retailers and the regulatory considerations associated with this digital transformation.

Blockchain technology and cryptocurrencies have emerged as groundbreaking innovations in the realm of finance and beyond. This academic paper provides an in-depth analysis of blockchain technology and its application in cryptocurrencies, examining the underlying principles, benefits, challenges, and the wider implications for various industries.

The advent of the digital age has brought about an unprecedented deluge of data. In this era of information abundance, the role of data analytics in aiding decision-making processes has gained paramount importance. This academic paper delves into the significance of data analytics, its methodologies, applications, and the transformative impact it has on decision-making in various domains.

In today's interconnected digital landscape, cybersecurity is a critical concern for individuals, organizations, and governments alike. This academic paper explores the multifaceted challenges that the field of cybersecurity faces. It delves into the evolving threat landscape, the complexities of securing digital environments, and the implications for privacy, national security, and the global economy.

## 2- Digital Banking and Financial Services

The emergence of digital banking has redefined how financial institutions operate and interact with customers. Online banking, mobile apps, and digital payment platforms have not only made banking more convenient but have also lowered operational costs for financial institutions. Moreover, artificial intelligence (AI) and machine learning are enhancing risk assessment, fraud detection, and customer service, providing more tailored financial solutions.

As of 2021, Varonis reports that financial services employees have access to about 11 million company files on average, including files with sensitive personal and financial information. That number is nearly doubled for employees of large businesses, who have access to about 20 million files each(Max, 2022).

Financial institutions already face extraordinary risks if even a single employee's security becomes compromised, but the risk of social engineering, malware, ransom ware and noncompliance have multiplied since the sudden and widespread adoption of remote work. In 2020, financial institutions took an average of 233 days (approximately eight months) to detect and address data breaches affecting their systems. While crimes committed in person (such as robbing a store) are usually noticed immediately, skilled cybercriminals have the advantage of remaining undetected for months while they take their time to steal their target's valuable information(Luís & Rodrigues, 2023)

### 2.1. Evolution of Digital Banking

Digital banking has evolved significantly since its inception. Initially, it focused on providing basic online services such as checking balances and transferring funds. However, it has since expanded to encompass a broader array of services, including mobile banking apps, digital wallets, peer-to-peer (P2P) payments, and even crypto-currency services.

### 2.2. Key Features of Digital Banking

Digital banking is characterized by several key features:

**Accessibility**: Customers can access their accounts and conduct transactions at any time and from anywhere with an internet connection.

**Convenience**: The ability to perform various banking tasks through user-friendly mobile apps or websites makes banking more convenient for consumers.

**Cost-Efficiency**: Digital banks often have lower operating costs than traditional banks, allowing them to offer competitive fees and interest rates.

**Personalization**: Data analytics and artificial intelligence enable digital banks to provide personalized financial advice and tailored product recommendations.

### 2.3. Benefits of Digital Banking

Digital banking offers several advantages:

**Enhanced Convenience**: Customers can manage their finances without visiting physical bank branches, saving time and effort.

**Lower Costs**: Reduced overhead costs for digital banks can translate into lower fees and better interest rates for customers.

**Financial Inclusion**: Digital banking can extend financial services to underserved populations who lack access to traditional banks.

**Innovation**: Digital banks are at the forefront of financial technology innovation, driving the industry forward.

### 2.4. Challenges and Concerns

Despite its advantages, digital banking faces challenges and concerns:
**Cyber-security**: The digital realm is susceptible to cyber threats, necessitating robust security measures.
**Data Privacy**: The collection and use of customer data for personalization raise concerns about data privacy and security.
**Regulatory Compliance**: Compliance with evolving financial regulations is crucial but can be complex for digital banks operating across borders.

**2.5. Financial Inclusion**

Digital banking has the potential to foster financial inclusion by providing banking services to unbanked or under-banked populations. Mobile banking and digital wallets offer accessible and affordable options for these individuals to manage their finances and access credit.

Digital banking represents a transformative force in the financial services industry. Its evolution from basic online services to a comprehensive suite of financial products and the potential for financial inclusion make it a pivotal aspect of modern finance. While digital banking offers numerous benefits, addressing challenges such as cyber-security and regulatory compliance is imperative to sustain its growth and ensure its continued positive impact on the financial landscape.

**3. E-commerce and Retail**

The evolution of e-commerce can be traced back to the early days of the internet, primarily as a platform for information exchange. However, as technology advanced, online retailing began to take shape. Amazon's pioneering efforts in the mid-1990s paved the way for e-commerce to become a mainstream consumer activity.

**3.1.Key Drivers of E-commerce**

Several key drivers have propelled the growth of e-commerce:
**Internet Penetration**: The increasing global access to the internet has expanded the potential customer base for e-commerce platforms.
**Mobile Technology**: The proliferation of smartphones and mobile apps has made it easier for consumers to shop online from anywhere.
**Payment Solutions**: Secure online payment gateways and digital wallets have facilitated seamless transactions.
**Logistics and Delivery**: Efficient logistics and last-mile delivery solutions have reduced shipping times and costs.
**User Experience**: E-commerce platforms invest heavily in user-friendly interfaces, personalization, and customer service.

**3.2.Advantages of E-commerce**

E-commerce offers several advantages to consumers and businesses:
**Convenience**: Shoppers can browse, select, and purchase products or services 24/7, eliminating the need to adhere to store hours.
**Product Variety**: E-commerce platforms often feature a wider range of products than physical stores, enabling consumers to access a broader selection.

**Price Comparison**: Online shoppers can easily compare prices and reviews, promoting price transparency and informed decision-making.
**Global Reach**: E-commerce transcends geographical boundaries, allowing businesses to reach a global customer base.
**Data-Driven Insights**: E-commerce platforms gather data on customer preferences, enabling businesses to tailor their offerings and marketing strategies.

## 4. Block-chain Technology and Crypto-currencies

Block-chain technology has introduced decentralization and transparency to economic transactions. Crypto-currencies, despite their volatility, have emerged as alternative assets and investment opportunities. Economic institutions are exploring block-chain for secure record-keeping, supply chain management, and even central bank digital currencies (CBDCs)(Prakash, V.S, & S, 2022).

### 4.1.Block-chain Technology: Foundations and Mechanisms

Block-chain, at its core, is a decentralized and distributed digital ledger that records transactions across a network of computers. Its key features include:
**Decentralization**: Unlike traditional centralized systems, blockchain operates on a peer-to-peer network, reducing the need for intermediaries.
**Immutability**: Once a transaction is recorded on the blockchain, it is nearly impossible to alter, enhancing security and trust.
**Transparency**: Transactions on the blockchain are visible to all network participants, promoting transparency and accountability.
**Security**: Cryptographic algorithms and consensus mechanisms safeguard the integrity of the blockchain.

### 4.2.Cryptocurrencies: The Application of Blockchain

Cryptocurrencies are digital or virtual currencies that rely on blockchain technology for secure and transparent transactions. The most renowned cryptocurrency, Bitcoin, introduced the concept of digital currencies. Key aspects of cryptocurrencies include:
**Decentralization**: Cryptocurrencies operate without central authorities, such as banks or governments, allowing for borderless transactions.
**Cryptography**: Advanced cryptographic techniques secure transactions and control the creation of new units.
**Digital Wallets**: Users store their cryptocurrencies in digital wallets, which are secured with cryptographic keys.
**Volatility**: Cryptocurrency prices can be highly volatile, influenced by factors such as market sentiment, regulatory developments, and macroeconomic conditions.

### 4.3. Benefits of Blockchain and Cryptocurrencies

Blockchain technology and cryptocurrencies offer several advantages:

**Security**: The blockchain's cryptographic nature ensures the security and immutability of transactions.
**Transparency**: Blockchain's transparency reduces fraud and enhances trust among users.
**Efficiency**: Digital transactions are faster and more cost-effective than traditional banking systems, especially for cross-border transfers.
**Financial Inclusion**: Crypto currencies provide access to financial services for unbanked and under banked populations.
**Innovation**: Block chain's versatility has led to innovations in various sectors, from supply chain management to healthcare.

**5. Data Analytics and Decision-Making**

Data analytics tools have empowered economic institutions to harness the vast amount of data at their disposal. Predictive analytics, driven by big data and machine learning, assist in risk assessment, investment strategies, and policy formulation. Ethical considerations, data privacy, and regulatory compliance, however, are ongoing concerns(Vladimir, Sergey, & Yuri, 2019).

**5.1.Data Analytics: Foundations and Methodologies**

Data analytics is the process of examining, cleaning, transforming, and interpreting data to extract meaningful insights. It encompasses several key methodologies:
**Descriptive Analytics**: This involves summarizing historical data to understand past trends and patterns, providing a foundation for further analysis.
**Diagnostic Analytics**: Diagnostic analytics aims to determine why certain events or trends occurred by examining causal relationships in data.
**Predictive Analytics**: Predictive analytics leverages statistical models and machine learning algorithms to forecast future outcomes based on historical data.
**Prescriptive Analytics**: Building upon predictive analytics, prescriptive analytics suggests actions to optimize outcomes, offering decision-makers actionable insights.

**5.2.Applications of Data Analytics**

Data analytics finds applications across a wide spectrum of industries:
**Business and Marketing**: Organizations use data analytics to enhance customer segmentation, personalize marketing strategies, and optimize pricing.
**Healthcare**: Data analytics aids in patient diagnosis, drug discovery, and hospital resource allocation.
**Finance**: In the financial sector, analytics underpins risk assessment, fraud detection, and algorithmic trading.
**Supply Chain Management**: Analytics optimizes inventory management, demand forecasting, and logistics.
**Government and Public Policy**: Governments employ data analytics for policy formulation, resource allocation, and performance measurement.

**5.3.The Role of Data in Decision-Making**

Data analytics revolutionizes decision-making in several ways:
**Informed Decision-Making**: Data-driven decisions are based on evidence and insights rather than intuition or gut feeling, reducing the risk of errors.
**Precision and Personalization**: Analytics allows for highly targeted decisions, tailoring solutions to specific contexts, individuals, or markets.
**Improved Efficiency:** Automation of data processing and analysis expedites decision-making processes.
**Risk Mitigation**: Predictive analytics can identify potential risks or anomalies, enabling proactive measures.

## 6. Cyber security Challenges

The digital transformation of economic institutions has rendered them vulnerable to cyber threats. Robust cyber security measures are imperative to protect sensitive financial data, customer information, and critical infrastructure. Continuous investments in cyber-security are essential to mitigate these risks effectively(Chen, 2021).

### 6.1.Evolving Threat Landscape

The cybersecurity landscape is in a state of perpetual evolution. Several key challenges contribute to this dynamic environment:
**Sophisticated Cyberattacks**: Malicious actors employ increasingly sophisticated techniques, including advanced persistent threats (APTs), ransomware, and zero-day exploits, to breach digital defenses.
**Nation-State Actors**: Nation-state-sponsored cyberattacks pose significant threats to critical infrastructure, government institutions, and international stability.
**Evolving Attack Vectors**: As technology advances, new attack vectors emerge, such as IoT vulnerabilities, supply chain attacks, and attacks on cloud infrastructure.
**Insider Threats**: Insider threats, whether intentional or unintentional, remain a significant challenge for organizations, necessitating robust internal security measures.

### 6.2.Complexities of Securing Digital Environments

Securing digital environments is a complex undertaking with several inherent challenges:
**Data Protection**: Ensuring the confidentiality, integrity, and availability of data is paramount, requiring encryption, access controls, and robust data management.
**Vulnerability Management**: The proliferation of software and devices demands effective vulnerability management to identify and patch weaknesses promptly.
**Identity and Access Management**: Verifying user identities and managing access rights across complex networks and cloud environments is challenging yet crucial.

**Compliance and Regulations**: Navigating a web of ever-evolving cybersecurity regulations and standards demands significant resources and expertise.

**6.3.National Security and Global Implications**

The consequences of cybersecurity breaches extend beyond individual organizations:

**National Security**: Cyberattacks targeting critical infrastructure, military systems, and government agencies can have profound implications for national security.

**Global Economy**: Cyberattacks can disrupt supply chains, financial systems, and international trade, impacting the global economy.

**Geopolitical Tensions**: Cyber espionage and cyberattacks are becoming integral components of modern geopolitical conflicts.

**7. Method and Empirical Study:**

**7.1. Database**

Cyber Security Job Salaries Dataset contains 11 columns and 1247 Rows :

**1. work_year :** The year when salary was recorded.
**2. experience_level :** The experience level in the job during the year.
**3. employment_type :** The type of employment for the role.
**4. job_title :** The role worked in during the year.
**5. salary :** The total gross salary amount paid.
**6. salary_currency :** The currency of the salary paid as an ISO 4217 currency code.
**7. salary_in_usd :** The salary in USD
**8. employee_residence :** Employee's primary country of residence.
**9. remote_ratio :** The overall amount of work done remotely
**10. company_location :** The country of the employer's main office.
**11. company_size :** The median number of people that worked for the company during the year.

**7.2. Data analysis**

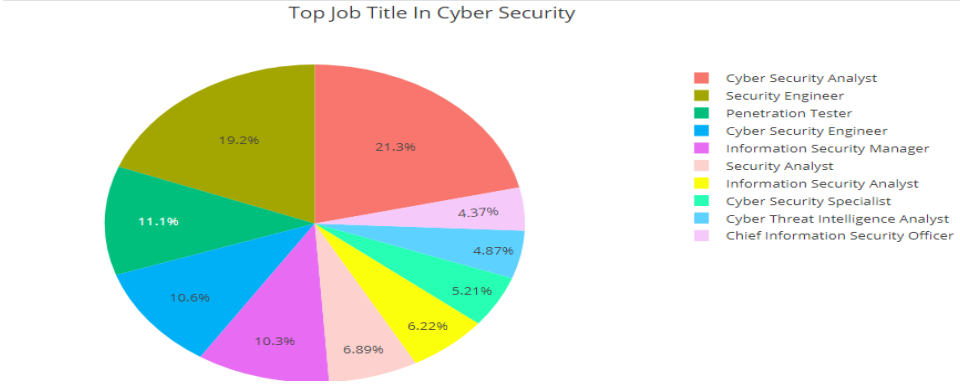
A cyber security job is a role that allows you to protect online data and information from hackers and other security threats. Over the last 20 years, people across the globe have started relying on technology more throughout their daily lives.From content management systems to e-readers and phones, smart devices and software have become progressively more prominent. Most of the public uses platforms like social media applications and mobile devices that store their personal data within security systems. With this popularization, users have become more interested in how companies are handling and accessing their private information.Companies often utilize extensive resources to protect consumer data. Cybersecurity is now a large and lucrative industry with the potential for enormous growth over the coming years. While there are various roles to choose from within the industry, cybersecurity positions often pay six figures or more because of the industry's importance. If you're interested in

joining the field, you may want to narrow your search by considering the top-paying roles.

**7.3. Results & Discussion:**

Some cyber security roles reflect similar or identical responsibilities, but may be more or less appealing to candidates based on the importance that the title projects. A "Cyber Security Manager" title may sit better with candidates than a "Cyber Security Team Lead" for example. According to job board Indeed.com, Information Security Analysts make an average of $83,264 per year, compared to IT Security Specialists who bring in $113,024 . While many employers may treat this difference in title as a nuance of company policy, the job title can have a serious impact on candidate salary expectations and willingness to apply for the role. By the same token, if the complexity of a role isn't conveyed by a job title that accurately portrays the responsibilities of the position, an employee may become discouraged and eventually less productive. A professional with an analyst role that begins to take on managerial or supervisory tasks will eventually demand a raise, promotion or begin to resent the lack of recognition for their efforts. In the case of talented cyber security professionals with highly marketable skills, a lack of recognition, through job titles that match skill sets and contributions to the company's success, will make them more difficult to find, hire and retain.

**Fig01**: Top job title in cyber security




**Source** : Outputs Researcher

Demand for cybersecurity specialists has soared in the last decade due to increasing rates of cybercrime. As a result, careers in cybersecurity bring numerous benefits, including job security and a relatively high income. In this article, we'll highlight the average cybersecurity salary, including income differences by position and state.

The U.S. Bureau of Labor Statistics (BLS) reports that the median annual salary for information security analysts is $102,600. This salary is more than double the national median earnings of workers across all industries ($45,760). Cybersecurity salary potential tends to be so high due to the delicate nature of the job and the increasing economic demand for cybersecurity professionals.

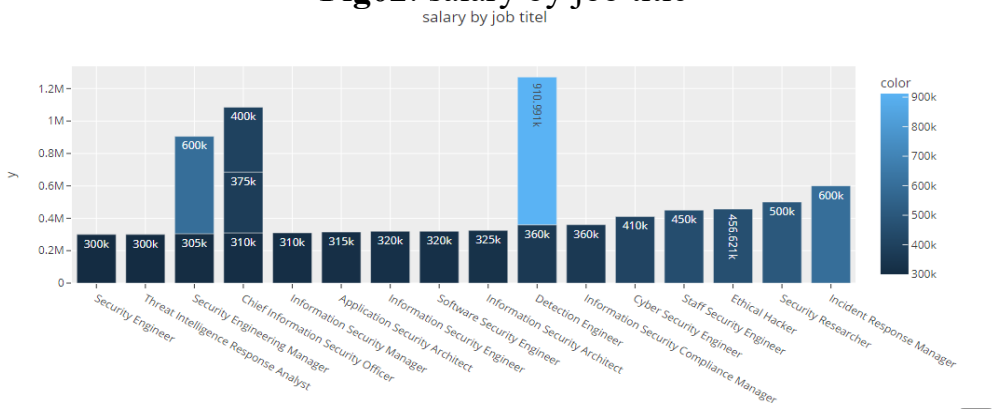
**Salary by Industry**

An upside of working as a cybersecurity specialist is getting to choose from a variety of industries. As a cybersecurity professional, the specific industry you work for plays a major role in determining your annual income.

Let's look at some top-paying industries where experts in cybersecurity are in demand, according to the BLS.

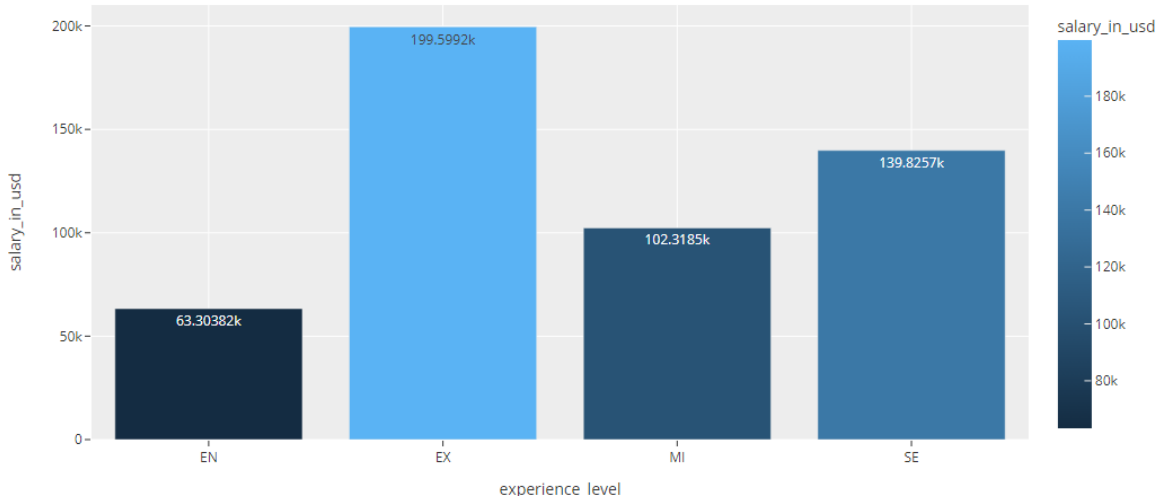
- **Remediation and other waste management services**. Information security analysts in this sector earn an average annual wage of $173,250.
- **Other information services**. This IT subsector pays an average of $149,540 to cybersecurity experts.
- **Computer and peripheral equipment manufacturing**. Cybersecurity professionals in this field earn an average of $144,040.
- **Securities and other financial investment sectors**. These fields pay an average cybersecurity salary of $142,070.
- **Motion picture and video industries**. This entertainment subsector pays information security analysts an average annual wage of $141,070.

**Fig02**: salary by job title




**Source** : Outputs Researcher

**Fig03**: Experience level

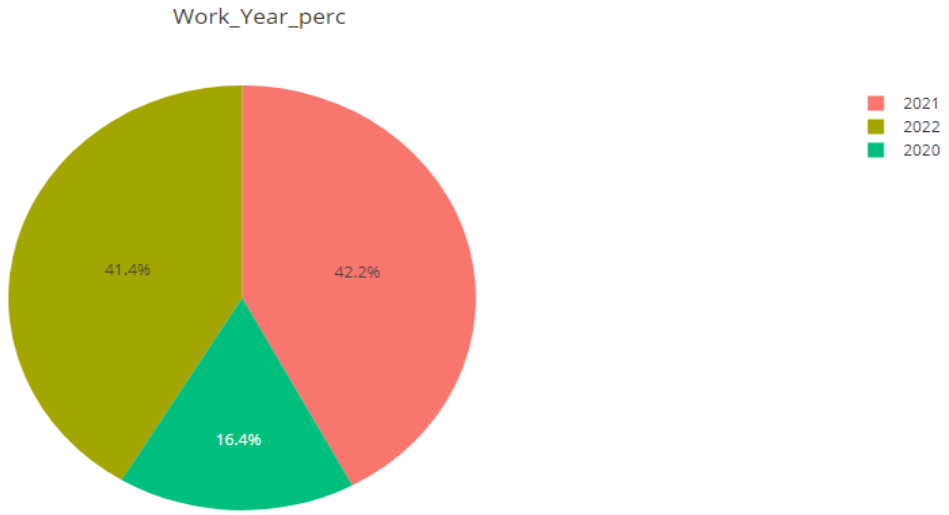



**Source** : Outputs Researcher

As we explore cybersecurity careers, we take a look at some of the highest-paid roles:

- Malware analyst: Earning an average annual salary of $165,000, malware analysts work to identify, examine, and understand various forms of malicious software and their delivery methods. Malware may include all the diverse forms of adware, bots, bugs, rootkits, spyware, ransomware, Trojan horses, viruses, and worms.
- Security architect: The primary role of a security architect is to assess organizations' systems for weaknesses. Security architects conduct penetration tests, risk analyses, and ethical hacks on local area networks, wide area networks, and virtual private networks. Theyearn an averageannualsalary of $128,000.
- Cybersecurity engineer: With an average annual salary ranging from $120,000 to $133,000, cybersecurity engineers create and manage hardware, software, and security policies to protect systems, networks, and data. Cyber engineers incorporate electrical engineering and computer science to understand cyberspace.
- Cybersecurity manager/administrator: A cybersecurity manager/administrator acts as the cybersecurity team's point person and is generally responsible for installing, administering, and troubleshooting an organization's security solutions. Earning an average annual salary of $90,120, cybersecurity managers also write up security policies and training documents about security procedures for colleagues and are responsible for the system overall, rather than specific parts.
- Penetration tester: A penetration tester for an organization earns an average annual salary of $87,000 and conducts a cybersecurity technique known as a penetration test, also called a "pen test" or "ethical hacking." This specific technique sees the professional using data to identify, test, and highlight vulnerabilities in the organization's security posture(Paul, 2023).

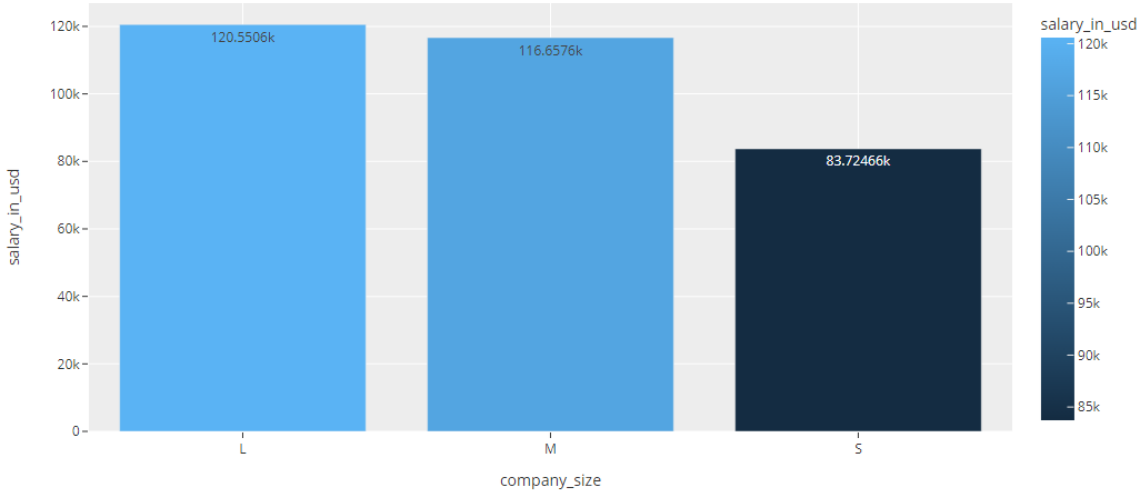
**Fig04**: Work year perc




**Source** : Outputs Researcher

According to the US Bureau of Labor and Services, there were 163,000 Information Security Analysts in 2021, with just 300 of these self-employed. Additionally, there was an almost unheard-of 100 percent employment rate in this sector. In fact, the BLS expects demand to increase by nearly 35 percent by 2031 – that's an additional 56,500 positions to be filled. In 2021, cybersecurity staff made, on average, five percent more than the year previous, with an average salary of $113,270 per year. That said, *where* you are located makes a huge difference: workers in California average $135,200 annually while those in Puerto Rico make just $51,600(IAN, 2023).

**Fig05**: company size



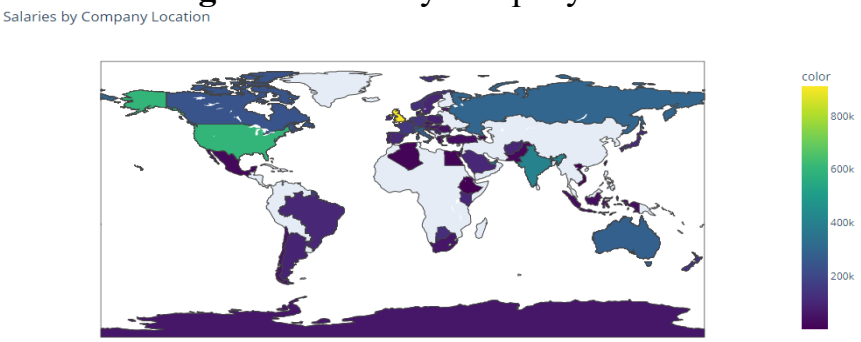

**Source** : Outputs Researcher

Skills and achievements are associated with higher pay grades, says a new cybersecurity salary report from Cynet.According to the report:

- Geolocation matters: Security analysts in North America get significantly higher salary than in EMEA and APAC, with more than 80% earning between US $71K and $110K. In contrast, less than 35% in EMEA and 21% in APAC earn equivalent salaries.
- A degree does not guarantee higher compensation: All analyzed positions feature similar salary range distribution for both employees with or without a degree in computer science or a related engineering field.
- Banking and finance provide the highest salaries in the industry: This holds true for both strategic management and tactical positions.
- Quality beats experience: Individuals were analyzed across all positions and those quality professionals with little experience were at the top of the payment curve, while seasoned veterans were at the bottom.
- Pivoting pays: Individuals that pivoted from an IT occupation to a cybersecurity position earned more than their peers that started out in cybersecurity.

- Bonuses are common practice: With the exception of security analysts, all other positions included periodic bonuses with annual rates ranging between one and ten percent.
- Women are hard to find: There is a significant shortage of women in security positions. The highest percentage is in the 20-29 age group with 6% in overall positions.
- Women in management: Within the five analyzed positions, the highest percentage of women were found in the security director/manager position at a rate of 10%.

**Fig05**: Salaries by company location




**Source** : Outputs Researcher

According to the survey, Washington, D.C. is the greatest location for cybersecurity jobs because of the abundance of job opportunities and the high average compensation for these positions. Singapore has the most job openings for cybersecurity specialists, while Luxembourg provides the best salary to cybersecurity professionals.

The list of the best countries and cities and the average salaries given are as below :

- Washington D.C, United States: GBP 84,628.38
- Singapore, Singapore - GBP 55,576.66
- Berlin, Germany- GBP 70,141.64
- Luxembourg, Luxembourg- GBP 110,768.11
- Brussels, Belgium- GBP 75,563.59
- Ottawa, Canada- GBP 70,060.75
- Vienna, Austria- GBP 72,339.79
- London, United Kingdom- GBP 74,416.00
- Riyadh, Saudi Arabia- GBP 43,280.91
- Tokyo, Japan- GBP 84,915.14

It's no wonder that Washington, D.C., is at the top of the list; the city is home to a number of federal departments that employ a large number of cybersecurity professionals. With a high average income of £84,628 and a second-place ranking for job availability in the cybersecurity market, the city is a strong candidate for individuals seeking employment in the field. Out of all the places studied, the city in Southeast Asia has the most job openings. However, the low living costs of £3,267 and the average wage of £55,577 bring it down.

Singapore has the highest number of cybersecurity job openings. Recent grads and anyone looking for a new job might improve their chances of landing a job by browsing for cities with the most job opportunities. Luxembourg has the highest pay for cybersecurity experts. Cybersecurity is a burgeoning field with enormous potential. In order to get all the value for the money in this market, you must also take into account the cost of residing. Variations in the living costs can quickly devour any pay rise.

## 9. Conclusion

In conclusion, technology and digital practices have reshaped economic institutions in profound ways, altering the nature of financial services, trade, transparency, and data-driven decision-making. While presenting immense opportunities for efficiency and growth, this digital transformation also raises critical issues, including regulatory compliance and cyber-security. Economic institutions must continue to adapt to this evolving landscape, embracing digitalization while remaining vigilant in safeguarding the economic well-being of individuals and nations.

Digital banking represents a transformative force in the financial services industry. Its evolution from basic online services to a comprehensive suite of financial products and the potential for financial inclusion make it a pivotal aspect of modern finance. While digital banking offers numerous benefits, addressing challenges such as cybersecurity and regulatory compliance is imperative to sustain its growth and ensure its continued positive impact on the financial landscape.

E-commerce has become an integral part of the modern retail landscape, reshaping how consumers shop and how businesses operate. Understanding the drivers, advantages, challenges, and regulatory considerations associated with e-commerce is essential for both consumers and retailers to navigate this dynamic and evolving sector effectively. E-commerce has disrupted traditional retail, altering consumer behavior and supply chain dynamics. Economic institutions have had to adapt by providing secure payment gateways, e-commerce financing, and digital marketplaces. The global reach of e-commerce has also necessitated a rethinking of cross-border trade regulations and tax policies.

Blockchain technology and cryptocurrencies represent a transformative force in finance and beyond. Understanding their fundamental principles, benefits, challenges, and broader implications is essential for businesses, policymakers, and individuals alike as they navigate this rapidly evolving digital landscape. While blockchain and cryptocurrencies offer immense potential, addressing their challenges and regulatory considerations is imperative to unlock their full benefits responsibly.

Data analytics has become an indispensable tool for informed and effective decision-making across various domains. Its methodologies, ranging from descriptive to prescriptive analytics, empower organizations and

individuals to harness the power of data. While data analytics offers immense potential, addressing challenges related to privacy, security, and data quality is essential to maximize its benefits responsibly. In an era where data is often considered the new currency, understanding and leveraging data analytics is paramount for success in the modern world(Max, 2022).

Cyber-security challenges are multifaceted and ever-evolving, driven by a dynamic threat landscape, complex digital environments, and global implications. The field of cyber-security is indispensable for protecting digital assets, ensuring privacy, and safeguarding national security and the global economy. Addressing these challenges necessitates a holistic approach, combining technological advancements, legal frameworks, ethical considerations, and a well-trained cyber-security workforce. As our digital dependence continues to grow, so too will the importance of effectively addressing these challenges.

# Bibliographie

Chen, M. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports* , 7999–8012.

IAN, G. (2023). *Cybersecurity job statistics (2021-2023 edition).* Comparitech .

Luís, F. R., & Rodrigues, &. a. (2023). Technology management has a significant impact on digital transformation in the banking sector. *International Review of Economics and Finance* .

Max, P. (2022). Top Cyber Security Statistics, Facts & Trends in 2023. *Cloudward* .

Paul, B. (2023). Cybersecurity Salary: Where Can You Go? *Western Governors University* .

Prakash, R., V.S, A., & S, A. (2022). Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights, 2* (100112).

Vladimir, K., Sergey, S., & Y. ,. (2019). Informational and analytical support of decision-making for ensuring the data safety in distributed systems . *Procedia Computer Science* , 19–27 .