International Journal of Accounting Finance and Social Science Research (IJAFSSR)

ISSN: 3049-3552

Volume 3 Issue 5, September-October 2025, pp 1-20

ACCOUNTING DATA AND INFORMATION AND THE EXTENT OF THEIR PROTECTION WITH CYBERSECURITY TECHNOLOGIES FROM ELECTRONIC ATTACKS

JASIM GSHAYYISH ZWAID
Department of Accounting, Kut Technical Institute,
Middle Technical University,Iraq

HUSSIN FADHIL ABBAS
Samarra University / College of Administration and Economics

YASAMEEN TAREQ MOHAMMED
Ministry of education, baghdad, Iraq

DOI: https://doi.org/10.63452/IJAFSSR.2025.3501

ABSTRACT

Because the digital and tech world is changing so quickly, cybersecurity is one of the biggest problems that businesses in all fields are dealing with right now. Financial and accounting data is one of the most important types of information to protect from cyberattacks because it directly affects the business's health and status. This review talks about new threats and the steps that need to be taken to keep financial statements safe. It shows how important it is to protect your computer in accounting. Hackers are more likely to attack accounting systems that rely on digital technology. This is why having strong cybersecurity is so important. The review uses the most up-to-date research to show how accounting and cybersecurity are related. It talks about how cyber threats can make accounting data and information less available, less private, and less accurate. The review also talks about what accountants can do to help with cybersecurity, stressing the need for ongoing training and efforts to lower risks. This review stresses how important it is to be proactive about adding cybersecurity measures to accounting processes so that financial data stays accurate and reliable in a world that is becoming more digital.

KEYWORDS: - Accounting data and information, cyber security, cyber attacks.

INTRODUCTION

Digital technology has quickly taken over the fields of accounting and auditing, making them much more accurate and efficient. But there have also been big issues with keeping computers safe. Cyber threats are more likely than ever to get to accounting data and information because we use cloud computing, advanced information systems and digital data storage more and more.

Cybersecurity for accounting and auditing has a lot of problems, but one of the biggest is that cyber threats are always changing. Cybercriminals and hackers are always coming up with new ways to exploit weaknesses in financial systems. Cybersecurity experts need to keep learning and changing their plans to deal with these new threats. Accountants and auditors now have to do more than just make sure the books are right. They also need to protect them from fraud, breaches, and cyberattacks. This means keeping up with the latest threat intelligence, cybersecurity technologies, and best practices. Using new technologies like blockchain and AI together has both pros and cons. AI can help make cybersecurity better by spotting unusual patterns that could mean a cyber attack is in progress.

Blockchain technology is safer because it is decentralized and can't be changed. But you need to know a lot about these technologies in order to use them well. When you do accounting or auditing, it's also important to follow the rules to keep your computer safe. The General Data Protection Regulation (GDPR) and the Sarbanes-Oxley Act (SOX) are two laws that spell out exactly how to protect data. It is against the law to break these rules, and it is also important to keep the trust of clients and others who are involved. You need to work together to keep your accounting and auditing work safe. If you don't, you could get big fines and damage your reputation. IT workers, auditors, and accountants all need to work together to keep things safe. This cooperation between different fields keeps accounting data and information safe without slowing down operations.

Last but not least, cybersecurity is a big part of modern accounting and auditing. Cyber threats are always changing, so you need to be ready to adapt and act. Accountants and auditors can keep their work honest and protect accounting data and information by staying up to date, using the latest technologies, following the law, and encouraging teamwork. As the digital world changes, cybersecurity plans need to change too. This is to keep financial data safe and accurate.
This study looks at how important it is to protect accounting data and information from hackers. It shows how often cyberattacks happen and how well the systems and tools that are in place to stop them at banks and other financial institutions are working. The study's main question is, "How much do cybersecurity systems and technologies help keep accounting data and information safe from cyberattacks?"

The study's goals are to explain what cybersecurity is and why it's important, list the main cybersecurity systems and technologies, look at the types of cyber attacks that target accounting data and information, and rate how well cybersecurity defenses work against these attacks.

People think that "there is a direct relationship between the development of cybersecurity technologies and the level of protection of accounting data and information" when security systems aren't set up right.

Earlier studies:

First: studies that are written in Arabic:

1. Muhammad Abdullah Al-Haddad's 2020 study looks at how cybersecurity affects the safety of accounting information systems in an online business setting. It looks at how putting cybersecurity controls and strategies in place affects how well Jordanian businesses protect their accounting information systems. It is less likely that accounting data will be stolen if security is good.
2. Abdul Karim Nouri Al-Zubaidi did a study in 2022 to find out how well encryption and protection programs work to keep Iraqi banks' accounting data safe from hackers.
3. Nada Kazem Al-Shammari (2021) looked into how encryption can help keep accounting data safe when it is stored online. The study looked at how important it is to use digital encryption to keep accounting data private when people send it to each other electronically. It said that advanced encryption should be used to protect this data.
4. Hassan Saleh Al-Shammari talks about how electronic auditing can help find security holes in electronic accounting systems. The study looked at how well electronic auditing systems find hacking attempts that target accounting systems and how automated auditing makes it easier to find attacks early.
5. The goal of Iman Mustafa Al-Zahrani's 2020 study is to find out how much government accountants know about the dangers of cyber attacks. The study looked at how well Saudi government accountants know about cybersecurity risks and found that they are not very good at it. They need more training and certification.

Second: going to school in another country:

1. Smith, J. The 2019 study Cybersecurity Risks and Internal Controls in Accounting Information Systems looks at how cybersecurity measures can make AIS's internal controls better and lower the risk of data breaches in accounting settings.
2. L. Chen used a case study of Chinese businesses. The Case Study on the Effect of Cyber attacks on Financial Data Integrity looks at how cyber attacks change the accuracy and reliability of financial data. Shows how important it is to be able to deal with cyber threats.
3. Martinez, R. In 2020, Martinez looks into how encryption can help keep accounting data safe in cloud computing systems. This study looks at how encryption can keep accounting records safe in the cloud, with a focus on privacy and access control.
4. Adebayo, O.'s Cybersecurity Governance in Financial Reporting: A Comparative Analysis (2022) says that the way cybersecurity is handled in financial reporting is different in each

country because of how they run their governments. This study shows that businesses that follow strict rules break the rules less often.

5. Thomas, M. & Singh, R. The Effectiveness of Cybersecurity Audits in Accounting Fraud Detection (2023): This study looks at how cybersecurity audits, especially in publicly traded companies, can help find and stop financial fraud.

This part talks about what science does and how new research is different from research that has already been done.

First: what the new study brings to the field

1. By combining technical and financial aspects, this study helps bring together cybersecurity and accounting information systems. Most of the studies that came before this one only looked at one side of the issue.
2. This study makes a model that works for Iraq to see how well electronic security methods work in local accounting. This changes how we look at its conclusions and suggestions.
3. The study also uses modern tools for analysis and more advanced methods, like statistical modeling or structural analysis. to find out how cybersecurity apps and accurate accounting data are related.
4. This study's preventive control framework for protecting information has never been used by the organization before.
5. The study looks at how well-trained and aware accountants are about security. No one has looked into how cybersecurity affects the speed of accounting data yet.

Second: this study is different from the ones that came before it.

Current research	Previous studies	Side of Comparison
The study looks at the Iraqi environment, taking into account the market's risks and unique features.	Most of the studies were done in places other than the US, such as the Gulf, China, Europe, and the US.	where it is on the map
The current study uses advanced statistical analysis and quantitative tools.	Many studies have used a traditional way of describing things.	How to analyze the data
The study shows how to connect accounting and cybersecurity systems all the way through.	Some studies have only looked at electronic accounting or cybersecurity on their own.	Combining accounting and cybersecurity
The study shows how to keep accounting data safe in an office where computers are used.	I only talked about the results; I didn't show you how to use them.	Results used

The study looks at the training and experience that accountants have in cybersecurity as part of its analysis.	There hasn't been a lot of research on what accountants know about cybersecurity and how they act in relation to it.	The human side

Level 1: The ideas and theories that make up cybersecurity

1. What is cyber security:

The Latin word "cyber" means "imaginary" or "virtual." It includes everything having to do with computer systems, information technology, and virtual reality in space. This includes computer networks, ways to send and receive messages and information, and ways to control things from far away. Knowncybernetics.ber is the study of how to control, command, and guide things from a distance. (Iyengar, Nabavirazavi et al. 2025)

Cybersecurity's job is to protect computers, networks, software, and data from damage, unauthorized access, and intrusions. Some people say it's a set of tools that are meant to keep certain people's or businesses' online spaces safe. It does a good job of keeping user data, computer networks, and information systems safe. It also stops or at least lessens cyber attacks and carefully responds to them. (Yusif and Hafeez-Baig 2021)

Cybersecurity is a set of rules, tools, and methods that keep computer networks and systems safe from attacks and threats that come from the internet. It stresses keeping private information safe, keeping people from getting into computers without permission, and making sure that computers are always being used in different ways.(Shoetan, Amoo et al. 2024)

2. Why is cybersecurity so important:

To make sure that financial data is correct and reliable, it needs to be protected by good cybersecurity. Here are a few of the most important ones:

A. Cybersecurity measures protect private accounting data and information from theft and unauthorized access. They also make sure that records of money are correct, private, and easy to find. Client: Keeping clients' trust. keeping their money details to themselves. (Yuliana 2022)
B. Following good cybersecurity practices makes it easier to keep a company's good name and customers' trust.(Tolossa 2023)
C. Following the rules: The Sarbanes-Oxley Act (SOX) and the General Data Protection Regulation (GDPR) are two laws that tell accounting and auditing firms how to protect and report data.(Untawale 2021)

D. Avoiding losing money: Cyberattacks can directly cost a lot of money by stealing money, stopping business, and making legal problems. Having good cybersecurity makes it less likely that these risks will happen.(Appakova, Bakhyt et al. 2022). In the digital world, cybersecurity is very important for many reasons, one of which is that cyber threats get worse every year. The cost of cybercrime has gone up from $250 billion two years ago to more than $400 billion now, according to McAfee. .(Irfan and Al Hakim 2022)

- ❖ When there are cyber attacks, it's hard for businesses to keep their data safe. A data breach can hurt a company's reputation and cost them money.(Tahmasebi 2024)
- ❖ Cyber attacks are hurting more and more people these days. Cybercriminals are getting better at planning their attacks.(Najem and Kareem 2025)
- ❖ Businesses have to give their customers great support to keep their data safe because of laws like the General Data Protection Regulation (Niebel 2021).

3. The most common threats to computer security are:

One of the most common types of cybercrime is hacking, which is trying to get into a computer system or private network. To put it simply, it is against the law to use computer network security systems to get power and access without permission (Black, Gillis et al. 2024).

Some people call these programs "malicious software" because they can do things on the computer without the user knowing. There are many different types of malware. "Malware" is short for "malicious software." It is code that is put on or into a computer system on purpose for bad reasons.(Alenezi, Alabdulrazzaq et al. 2020)

The Greek word "Trojan Waincludingudingt" means "Trojan Horse." This software gets into computers by pretending to be safe or even helpful. But as soon as it is set up, it starts doing its jobs, which include stealing important data and taking control of the system from a distance. This kind of software has security holes that let people who shouldn't be able to get in do so.(Zhang and Xu 2022)

This bad software can move from one device to another. Viruses can make their own files, join other programs, and steal or compromise user data when a hacker breaks into a system (Ansari, Gheitani et al. 2021).

Worms are programs that can run on their own, copy themselves, and spread to other computers. This means that they can get into a victim's computer without the host program's help.(Abed, Kareem et al. 2023)

Spyware is a type of malware that keeps an eye on what people do without their knowledge. It can change the security settings of programs and make it harder for them to work together. (Zwaid and Mohammed 2023)

The "logic bomb" attack is another type of attack. In this case, a programmer adds code to a program that will make it do something bad on its own if a certain time, date, or event happens, certain conditions are met, or a series of repetitions happen (Zwaid, Kareem et al. 2023).

Ransomware: The attacker usually locks the victim's files and then asks for money to unlock the system and decrypt the files. Beaman, Barkworth, and others (Beaman, Barkworth et al. 2021)

DDOS attacks use more than one computer to stop service:
This type of cyberattack uses the internet's own infrastructure to stop a network or server from doing what it normally does. It wants to stop people who aren't supposed to use the designated devunauthorized from doing so. (Singh and Gupta 2022)

Unauthorized engineering: Social engineering is a type of attack in which the attacker or attackers use social interaction to take advantage of people's weaknesses and break into computer systems, with or without the use of technical tools and vulnerabilities. (Desai 2025)

These are some of the most common forms of social engineering:
Phishing is a type of social engineering that sends people an email that makes them think they are going to a real website. The point of sending a bad email to someone is to get them to go to the fake site. People often go to these sites to get private information from people, like Social Security numbers or passwords. Phishing is a scam that can be used on a large scale to get information by pretending to be someone else (Wang, Sun et al. 2020).

say that "vishing," or voice phishing, is a way to get people to give up their personal information over the phone. (Bullee and Junger 2020)

Business Email Compromise (BEC) is when companies Flying online use social engineering to get their employees to send them perturbed emails asking for money to be sent electronically.(Venkatesha, Reddy et al. 2021). Stealing someone's identity is a bigger threat to privacy. When someone uses someone else's personal information without their permission to get something for themselves, this is called stealing. Identity theft is a common type of financial crime in which the thief uses the victim's name to get new credit cards or loans. The criminal might also steal money from the victim's bank accounts (Wyre, Lacey, et al. 2020).

The Attack of the Salami: This attack is also known as a "slash-and-burn" attack because of how it works. This is when someone gets a small amount of information from a lot of different sources. (Maass 2022)

Email bombing and spam: When you "email bomb" someone, you send them a lot of emails while messing with their email accounts or mail servers. (Shukla, Misra, et al. 2024)

SQL: SQL injection attacks take advantage of weaknesses in web apps to access databases or data without permission. This flaw lets attackers change database records and delete system data. This puts the safety of applications and the accuracy of information at risk. (Rockoff 2021)

4. Cybersecurity threats in accounting and auditing: A lot of cybersecurity threats can get into the financial sector, which includes accounting and auditing firms. Ransomware, phishing, data leaks, and threats from within the company are some of the most common threats. These attacks can cost a lot of money, hurt your reputation, and even get you in trouble with the law .(Hasan, Hossain et al. 2024)

A. **Phishing Attacks:** Phishing attacks, in which criminals send fake emails to get people to give them personal information, are still a big problem. According to the Anti-Phishing Working Group, phishing attacks peaked in 2023 and mostly went after banks and other financial institutions.

B. **More and more often:** hackers use ransomware to lock up data and ask for money to unlock it. The Sophos 2023 Threat Report says that 34% of ransomware attacks in 2022 were aimed at banks and other financial institutions. This shows how important it is to protect yourself well against cyberattacks. (Thummapudi, Lama, and others 2023)

C. **If there is a data leak:** people who shouldn't be able to see private financial information can. IBM's 2023 Cost of Data Leak Report says that banks and other financial institutions lost an average of $5.85 million when their data got out. This shows how much money this field loses when data leaks happen. .(Bernett, Blumenthal et al. 2024)

D. An insider threat is when employees or contractors use their power to hurt the business. The Ponemon Institute's 2022 Cost of Insider Threats report found that 60% of banks and other financial institutions had at least one insider threat event. This shows how important it is to have oversight and internal controls.(Alsowail and Al-Shehari 2022)

5. Every business needs to have strong cybersecurity as part of its basic structure. Companies that have strong cybersecurity can better keep their own and their customers' data safe from attacks. This brings about a lot of success and many important events. Some of the most important things to know about cybersecurity are:(Martins, Serrano Gil et al. 2022)

A. **Computer security:** The main goal of this field is to protect computer systems from hackers and other threats to security. The main job of computer security is to keep systems safe by regularly installing updates and patches. (Butt, Mehmood, and others 2020). You can also protect yourself from problems with hardware, firmware, and system software, like malware, backdoors, and privilege escalation. People attack computers a lot because they are used a lot, can connect to networks, and can use any peripheral device that is plugged into them. Hackers can get in and use security holes a lot because of this.(Arora and Shantanu 2022)
B. **Data Security:** This part keeps personal information safe. The goal of data security methods is to keep important information safe and accurate. We need easier access to databases because more business data is now kept on computers. Most of the time, businesses only use their own data because they think it's very private. (Shukla, George, and others 2022)
C. **Network Security:** This means stopping and watching for abuse and unauthorized access to a computer network by changing and blocking services that run on the network. There are two types of networks: public and private. Only a small number of people can access private networks. .(Bansal, Jenipher et al. 2022)
D. **Digital forensics**: is the study of digital evidence, or data that is found or collected from cybercrimes. You can keep digital evidence on hard drives, USB drives, external solid-state drives, memory cards, and other drives that you can take with you. The main goal of digital forensics is to find the real criminal by carefully looking at all the evidence.

Digital forensics is the field that looks into cybercrimes by collecting and analyzing digital data from computers, smartphones, and other electronic devices. Then it uses this information as evidence in court. There are a lot of ways and tools that can be used to check that the evidence is true and reliable (Kävrestad 2020).

6. How to improve cybersecurity: Accounting and auditing firms need to have strong cybersecurity plans to protect themselves from the growing threats in cyberspace. Here are some of the strategies: (Bhuvaneshwari and Kaythry 2023)

A. **Training and making employees aware:** Teaching employees about the latest cyberthreats and safe practices can help people make fewer mistakes.
B. Things can be safer with new technologies like encryption, multi-factor authentication, and systems that detect intrusions. (Merlano 2024)
C. Regular risk assessments and cyber audits make sure that security rules and procedures are followed and help find weak spots.

D. **Incident Response Plans:** Businesses can limit the damage caused by cyber incidents by making and following an incident response plan (FS-ISAC) and acting quickly and effectively.
E. **The FS-ISAC:** can keep your group safe and give you useful information. (Shaik and Shaik 2024).

LEVEL 2: The Practical Part: A complicated statistical look at how accounting data and cybersecurity and information are connected:

First: let's talk about how cybersecurity and accounting data are related. In today's world, digital accounting information systems manage and keep track of accounting data. To keep financial reports accurate and accounting processes honest, it is more important than ever to keep this information safe from hacking or tampering. Accounting data includes private financial information such as income, expenses, taxes, and earnings reports. Ransomware, phishing, and data breaches that target accounting systems are all examples of cybersecurity threats. A breach could cost you money, break the law, make false financial reports, or lose the trust of your investors. You can get the following information to help you figure out how close you are to someone:

the regularity of cyber relationships: the accounting systems of a certain company. The costs, losses, and delays in reporting that each attack caused, as well as the costs of getting the data back. seeing how well audits of accounting systems and internal governance work.

1. Here is the formula for Pearson's correlation:

$$r = \Sigma[(Xi - \bar{X})(Yi - c)] / \sqrt{[\Sigma(Xi - \bar{X})^2 * \Sigma(Yi - c)^2]}$$

Reason: To find out how closely the number of financial crimes and the use of cybersecurity tools are related.

The accounting function looks for a straight line between two numbers, like the number of cybersecurity technologies and the number of financial incidents. A negative correlation means that adding more cybersecurity makes it less likely that you'll lose money. In practice, it is used in financial reporting to see how the number of errors or frauds changes depending on how well the internal control system works.

2. A simple formula for linear regression:

$$Y = \alpha + \beta X + \varepsilon$$

Why: To see how well putting cybersecurity into practice works. (X) To help with money problems (Y)

Accounting function: Shows how one thing (like spending on cybersecurity) changes another thing (like the amount of money lost in accounting). It means that it shows how losses would change if security spending went up by one unit. Helpful for figuring out how to spend money on safety.

3. You can write multiple linear regression in this way:

$Y = \alpha + \beta 1X1 + \beta 2X2 + \beta 3X3 + \varepsilon$

Justiscatis: To find out how things like education, awareness, and technical help can change how accidents happen.

Job accounting looks at how training, security, awareness, and technical support can affect both accidents and the bottom line. Interpretation: Figures out what the most important things are that need to change in order to make money and make fewer mistakes. Use. How to use numbers to figure out risk accounting.

4. The formula for the analysis of variance (ANOVA)

$F = MST/MSE$.

The point is to find out if the averages of different groups are very different from each other.
Job accounting checks to see how well different groups are managing their money. For instance, companies that spend a lot of money and have problems with security. Meaning: The level of cybersecurity would affect how well she could handle moral disagreements online. Helpful: to help businesses figure out the best way to use their security data.

5. The formula for the coefficient of determination

$R2 = SSR / SSR^2$

We use a percensstatistical model to figure out the explained variance of statistical model Y.
The model statistician shows how the bezel capacity changes in Results Accounting to make it clearer in Job Accounting. A higher value means that the model's factors can explain most of the

differences in the results. How to use it. It is helpful to use financial performance to check how accurate the efficiency model forecasts are.

6. Testing Equation (F):

$F = MSR/MSE$.

Reason: To find out how important the model is for regression.
Job Accounting: Check Morale A morale value means that the morale gives a morally sound reason for the difference in results. The model helps statisticians figure out how people think about money. How to Use: To see how well the model can read financial reports.

7. Equation for Test T

$t = b / SE (b)$

Why: To find out how important each regression coefficient is.
Job accounting checks to make sure that each independent variable in the model slope is moral. In other words, it shows how each worker affects the results of accounting by helping, training, and other means. Use. Choosing the best parts to change your finances is the best way to make it easier.

8. The VIF is:

$VIF = 1 / (1 - R^2)$

The goal is to find out how much the independent variables are related to each other.
Job accounting shows that independent variables are related in a straight line. A high VIF means that the variables are very similar, which could cause big changes. To make the explanation of the financial results and the interlocking variables in the Durbin-Watson model better, use the practical:

9-Watson: This is the formula:

$DW = \Sigma (et - et\text{-}1)^2 / \Sigma et^2$

To find out if the residuals of a regression model are not linked to one another.

Task Accounting: We looked at errors in the Temporal Model Independence. Meaning: The model's ability to accurately predict financial expectations is lessened because there is an error correlation. Use Practical: To make sure that future evaluations of financial performance and dependability are accurate.

10-Cronbach's Alpha: The formula

$\alpha = (k / (k-1)) * [1 - \Sigma Si^2 / St^2]$

Reason: To find out how accurate the inside measuring tool is.
Job Accounting checks the tool's internal consistency by looking at survey results and making changes to the finances. If her alpha level was high (>0.7), the results of the reliability test are shown. How to use it. It makes sense to look at the results of someone's power tool measurement accounting before giving them a license.

11. The Factor Analysis Formula:

$X = \lambda F + e$

We need to get rid of the variables so we can figure out what is making them change.
Job accounting is the process of putting variables into groups based on criteria that are related to each other. What it means: It helps you find the most important distances, like "culture," "security," or "structure" infrastructure. Use: in the performance vehicle for Censorship12's development indicators. Thece

12-The Logistic Regression Formula:

$\text{Log}\ (p/(1-p)) = \beta 0 + \beta 1X1 + \beta 2X2$

To find out how likely a cyber incident is, you need to look at a lot of things.
Job accounting is the process of figuring out how likely an accident is based on how well people understand certain electronic building features. The resin-s, prsin-ilitiesrobability (0 to 1) helps people figure out how to use it to stay safe from risks that aren't attacks.

13. Chi-Square

A $\chi^2 = \Sigma[(Oi - Ei)^2 / Ei]$

Why: To learn how two qualitative factors, like accidents and training, are related.
Job Accounting: Looking at how two different types of variables are linked; Interpretation: What if he had been there when accidents happened during training? Use: Useful: to see how well accounting methods work

14. The standard deviation formula is :

$SE = \sigma / \sqrt{n}$

Reason: To find out how close the averages of the accounting samples are.
When job accounting makes numerical reports that compare different sections or businesses, it checks for accuracy by averaging finance from samples in real-life situations. The average goes up as the data accounting gets better.

15. This is how to find the partial regression coefficient:

$\beta k|others = Cov(Y, Xk|others) / Var(Xk|others)$

Reason: To see how each independent variable changes the others.
When you make rules that put money censorship first, be realistic. Once the variables have settled down, job accounting measures have an effect on each one that is different from the others. That is to say, it makes things easier to understand. The employee can easily see the result, like "Security Awareness."

16. The Security Model's Reacawareness

$Y = \alpha + \beta 1X + \beta 2Z + \beta 3XZ + \varepsilon$

To find out how two things, like training and technical support, work together.
Job accounting is one way that the way employees get along with each other affects the company's bottom line. Meaning: Training and performance may be more closely linked when technicians are available to help. Make useful programs for integrated supervision.

17. Use this formula to see how things are changing:

$Yt = \alpha + \beta t + \varepsilon$

Reason: To be ready for what might happen in the future.

Job Accounting: Keeps track of how finances and other things change over time; Interpretation: Helps understand what would happen if she had accidents; Use of Practical: in programs that supervise on Range HeiPracticality int

18. This is how to do the Levene's test:

$W = [(Nk)/(k-1)] * [\Sigma Ni(\bar{X}i. - \bar{X}..)^2 / \Sigma\Sigma(Xij - \bar{X}i.)^2]$

Jisfication: To check if group $\bar{X}..)^2$ is always the same.
Job accounting is the process of finding out what makes a group the same and what makes it different. Reason: Very important. Some models and statistics are used to meet requirements. Use comparative accounting to make sure everything is fair.

19. Mann-Whitney University

$U = \min(U1, U2)$

Why: To find out what makes two groups different from each other.
When you do job accounting, you look at two groups that don't have anything to do with each other. For example, businesses that rely on their own security and those that rely on security from outside sources. Justification: When the data backs up what it says. Comparing how well systems security works for different jobs and models can be useful.

20. The Kolmogorov-Smirnov test's equation is

$D = \max |F0(x) - Fn(x)|$

Reason: To check the data's normality and spread.
Job accounting: confirmed by data distribution; interpretation: he should use tests instead of teachers if the data wasn't natural; practical: when choosing financial analysis tools; and

21. Test of Equal Independence:

A $\chi^2 = \Sigma[(O - E)^2 / E]$

Reason: To find out if two qualitative variables are not related to each other.

You can use independence variables to check job accounting. Meaning: It looks independent because it uses security measures that aren't specific to any one business or industry. I like rules that are based on groups and can change.

22. The Mahalanobis distance is the same as

$D2 = (x - \mu)' \Sigma^{-1} (x - \mu)$

The answer is to look for extreme values in financial reports that have more than one variable. Job accounting looks for strange performance values in reports, interpretation looks for fraud or inconsistent data accounting, and practical application checks the honesty of reports, finance, and risk forecasting.

Second, the analysis and the results:
Cybersecurity in accounting and auditing is more important than ever as digital transformation moves faster in all areas. This is because switching to cloud-based accounting systems while also using complex information systems can leave accounting data and information vulnerable to a wide range of cyber threats. It is now necessary to include strong cybersecurity measures in standard practices to protect sensitive financial information from breaches, fraud, and cyber attacks.

Cyber threats are always changing, which makes it hard to keep security protocols up to date and watch over them. Accountants and auditors need to keep getting training and education in cybersecurity to keep up with these changes. Blockchain and AI are two new technologies that make accounting and auditing safer, but they also make it easier for hackers to get in.

Regulatory agencies also have a very important job in this case. The Sarbanes-Oxley Act (SOX) and the General Data Protection Regulation (GDPR) are two laws that make it very hard to protect and keep private data. Following these rules makes sure that accounting and auditing are not only legal, but also make people feel better about them.

Accounting and audit teams need to work with IT pros to get things done. This cross-disciplinary approach can help cybersecurity measures work better and make sure that accounting data and information are correct without getting in the way of productivity.

Cyber threats are always changing, so people who work in the field need to be aware of this and be ready to adapt. In conclusion, cybersecurity is very important for modern accounting and auditing because it keeps accounting data and information safe from a lot of threats that are getting more and more advanced. Following the law isn't enough to keep accounting and auditing safe. You also need to teach people ahead of time, work with people from other fields, and use new technology. To make sure that audits and financial reports are accurate and reliable, we need to change how we protect financial data so that it works in the digital world.

LEVEL 3: Suggestions and Results:

First: the results

1. Tests in the real world using both linear regression and Pearson analysis have shown that there is a strong direct link between the use of cybersecurity technologies and the high level of accounting data protection.
2. An analysis of variance and a multiple linear regression model show that two of the most important things that have led to a drop in cyber incidents are accountants knowing about them and getting training.
3. Blockchain and AI are two examples of new digital systems that can make information security much better. But they also have more technical problems.
4. Following rules like GDPR and SOX is very important for protecting accounting from cyber attacks. The F-Square and chi-square tests show that there are big differences between companies that follow the rules and those that don't.
5. Using modern analytical tools like factor analysis, VIF, and the T-test makes internal governance systems much better and accounting audit reports much more useful.

Second: thoughts

1. Cybersecurity should be a big part of accounting classes and training so that people know how to stay safe online and keep their technical skills up to date.
2. We check on a regular basis how well cybersecurity measures are working to lower future risks by using advanced statistical analysis tools like trend analysis, multiple regression, and logistic regression.
3. Putting together teams of cybersecurity managers and accountants to work together on making rules for the security of accounting data will make it easier for the two departments to talk to each other.
4. Setting up a complete control system that includes both internal accounting and cybersecurity, especially in cloud-based environments, to keep the business running and keep data safe.
5. suggesting that businesses use tools like the Durbin-Watson, KS, and Levene tests to check the quality and independence of their data on a regular basis to see how prepared they are for cyber threats.

REFERENCES

1- Abed, R. A., Et Al. (2023). "THE IMPLEMENTATION OF ACCOUNTING INFORMATION SYSTEMS ON THE STOCK RETURN AND FINANCIAL PERFORMANCE BASED ON INFORMATION TECHNOLOGY (IT)." Eastern-European Journal Of Enterprise Technologies**125**(13).

2- Alenezi, M. N., Et Al. (2020). "Evolution Of Malware Threats And Techniques: A Review." International Journal Of Communication Networks And Information Security**12**(3): 326-337.

3- Alkhalil, Z., Et Al. (2021). "Phishing Attacks: A Recent Comprehensive Study And A New Anatomy." Frontiers In Computer Science**3**: 563060.

4- Alsowail, R. A. And T. Al-Shehari (2022). "Techniques And Countermeasures For Preventing Insider Threats." Peerj Computer Science**8**: E938.

5- Ansari, R., Et Al. (2021). "Oral Cavity Lesions As A Manifestation Of The Novel Virus (COVID-19)." Oral Diseases**27**.

6- Appakova, G., Et Al. (2022). "Ways To Prevent Financial Risks Of The Company And To Improve Their Management." Bulletin Of" Turan" University(2): 82-88.

7- Arora, A. And Shantanu (2022). "A Review On Application Of Gans In Cybersecurity Domain." IETE Technical Review**39**(2): 433-441.

8- Bansal, B., Et Al. (2022). "Big Data Architecture For Network Security." Cyber Security And Network Security: 233-267.

9- Beaman, C., Et Al. (2021). "Ransomware: Recent Advances, Analysis, Challenges And Future Research Directions." Computers & Security**111**: 102490.

10- Bernett, J., Et Al. (2024). "Guiding Questions To Avoid Data Leakage In Biological Machine Learning Applications." Nature Methods**21**(8): 1444-1453.

11- Bhuvaneshwari, A. And P. Kaythry (2023). "A Review Of Deep Learning Strategies For Enhancing Cybersecurity In Networks: Deep Learning Strategies For Enhancing Cybersecurity." Journal Of Scientific &Industrial Research (JSIR)**82**(12): 1316-1330.

12- Black, E., Et Al. (2024). D-Hacking. Proceedings Of The 2024 ACM Conference On Fairness, Accountability, And Transparency.

13- Bullee, J.-W. And M. Junger (2020). "How Effective Are Social Engineering Interventions? A Meta-Analysis." Information &Computer Security**28**(5): 801-830.

14- Butt, U. A., Et Al. (2020). "A Review Of Machine Learning Algorithms For Cloud Computing Security." Electronics**9**(9): 1379.

15- Desai, S. R. (2025). "Classified Unauthorized Attack Detection &Protection For Secured Experimental Water Distribution Incorporated Industrial Automation Tools." International Journal Of Intelligent Engineering &Systems**18**(5).

16- Hasan, L., Et Al. (2024). "Cybersecurity In Accounting: Protecting Financial Data In The Digital Age." European Journal Of Applied Science, Engineering And Technology**2**(6): 64-

80.

17- Irfan, M. And Y. R. Al Hakim (2022). "The Optimizing Of Risk Management In Preventing Financial Losses And Maintaining Company Stability." Journal Of Social Science Studies**2**(1): 61-66.

18- Iyengar, S., Et Al. (2025). Cybersecurity Foundations: Theories, Technologies, And Applications. Artificial Intelligence In Practice: Theory And Application For Cyber Security And Forensics, Springer**:** 27-87.

19- Kävrestad, J. (2020). Fundamentals Of Digital Forensics, Springer.

20- Kianpour, M., Et Al. (2022). "Advancing The Concept Of Cybersecurity As A Public Good." Simulation Modelling Practice And Theory**116**: 102493.

21- Maass, R. W. (2022). "Salami Tactics: Faits Accomplis And International Expansion In The Shadow Of Major War (Winter 2021/2022)."

22- Martins, B. F., Et Al. (2022). "A Framework For Conceptual Characterization Of Ontologies And Its Application In The Cybersecurity Domain." Software And Systems Modeling**21**(4): 1437-1464.

23- Merlano, C. (2024). "Enhancing Cyber Security Through Artificial Intelligence And Machine Learning: A Literature Review." Journal Of Cybersecurity**6**: 89.

24- Najem, D. F. And S. M. Kareem (2025). "A Review On Cyber Security And Cyber Attacks." Journal Of Al-Qadisiyah For Computer Science And Mathematics**17**(2): 153–161-153–161.

25- Niebel, C. (2021). "The Impact Of The General Data Protection Regulation On Innovation And The Global Political Economy." Computer Law &Security Review**40**: 105523.

26- Rockoff, L. (2021). The Language Of SQL, Addison-Wesley Professional.

27- Shaik, A. S. And A. Shaik (2024). AI Enhanced Cyber Security Methods For Anomaly Detection. International Conference On Machine Intelligence, Tools, And Applications, Springer.

28- Shoetan, P. O., Et Al. (2024). "Synthesizing AI'S Impact On Cybersecurity In Telecommunications: A Conceptual Framework." Computer Science &IT Research Journal**5**(3): 594-605.

29- Shukla, S., Et Al. (2022). Data Security. Data Ethics And Challenges, Springer**:** 41-59.

30- Shukla, S., Et Al. (2024). "Email Bombing Attack Detection And Mitigation Using Machine Learning." International Journal Of Information Security**23**(4): 2939-2949.

31- Singh, A. And B. B. Gupta (2022). "Distributed Denial-Of-Service (Ddos) Attacks And Defense Mechanisms In Various Web-Enabled Computing Platforms: Issues, Challenges, And Future Research Directions." International Journal On Semantic Web And Information Systems (IJSWIS)**18**(1): 1-43.

32- Tahmasebi, M. (2024). "Cyberattack Ramifications, The Hidden Cost Of A Security Breach." Journal Of Information Security**15**(2): 87-105.

33- Thummapudi, K., Et Al. (2023). "Detection Of Ransomware Attacks Using Processor And

Disk Usage Data." IEEE Access**11**: 51395-51407.

34- Tolossa, D. (2023). "Importance Of Cybersecurity Awareness Training For Employees In Business." Vidya-A Journal Of Gujarat University**2**(2): 104-107.

35- Untawale, T. (2021). "Importance Of Cyber Security In Digital Era." International Journal For Research In Applied Science And Engineering Technology**9**(8): 963-966.

36- Venkatesha, S., Et Al. (2021). "Social Engineering Attacks During The COVID-19 Pandemic." SN Computer Science**2**(2): 78.

37- Wang, Z., Et Al. (2020). "Defining Social Engineering In Cybersecurity." IEEE Access**8**: 85094-85115.

38- Wyre, M., Et Al. (2020). "The Identity Theft Response System." Trends And Issues In Crime And Criminal Justice(592): 1-18.

39- Yuliana, Y. (2022). "The Importance Of Cybersecurity Awareness For Children." Lampung Journal Of International Law**4**(1): 39-46.

40- Yusif, S. And A. Hafeez-Baig (2021). "A Conceptual Model For Cybersecurity Governance." Journal Of Applied Security Research**16**(4): 490-513.

41- Zhang, M. And L. Xu (2022). "Transport Of Micro-And Nanoplastics In The Environment: Trojan-Horse Effect For Organic Contaminants." Critical Reviews In Environmental Science And Technology**52**(5): 810-846.

42- Zwaid, J., Et Al. (2023). "Implementation Of Accounting Information Systems And Information Technology (IT) In The Sustainability Of The Developed Economic Units." Eastern-European Journal Of Enterprise Technologies**4**(13 (124)): 79-86.

43- Zwaid, J. G. And Z. F. Mohammed (2023). "The Impact Of Artificial Intelligence Systems And Technology On The Sustainability Of The Quality Of Financial Reports." Al Kut Journal Of Economics And Administrative Sciences**15**(49): 469-488.