LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS5052NI - Professional Issues Ethics and Computer Law

Assessment Weightage & Type

60% Individual Coursework

Year and Semester

2022-Spring

Student Name: Punam Thapa Magar

London Met ID: 20048968

College ID: np01cp4s210273

Assignment Due Date:12th May 2022

Assignment Submission Date:12th May 2022

Title: Elastic Server and Data Breach

Word Count: 3500

Table of Contents

List of figures

Introduction

In today's world, playing online casinos and poker online is the difficult and sometimes daunting task of choosing the best online casino for our game needs. We must look at a variety of things to decide on the online casino of their choice. Unlike Las Vegas, where even if people have 50 casinos land on a strip of about 1 km on the Internet, there are thousands of online casinos to choose from in a matter of minutes. Each casino has a variety of games, promotions, graphics, software, and games to try to encourage them to make a deposit and start playing for gold (Admin, 2010). Ever since the first online casino was launched in the year 1996, the online gambling industry has grown tremendously over the years and contributed a significant portion to the entire gambling activity that happens throughout the world today. Online gaming has grown to be a billion-dollar industry and is only going to grow more in the future (localhistories, 2021)

Online Casinos are an online net model of ordinary land-based casinos. They empower players to play as well as bet on the liked games over the web. They normally have conceivable outcomes and pay-out costs indistinguishable from land-based gambling establishments. Most of these publish payment cost reviews consistently to woo more clients. The garden is numerous and reasonable sites have emerged over the last three years. A number of these starter information exchange motivating forces to very first-time clients when they make their first down payment.

Figure 1: Free real money online casino games

Many have gaming software applications made through presumed providers to improve their reliability like Microgaming, Realtime Gaming, and Playtech. There are commonly three forms of gambling enterprises on the web: web-casino sites, reside casino sites as well as downloaded-bases gambling enterprises. Some of them additionally offer various point-of-interface games. Online ones are for most of the past founded on a streak as well as java innovations providing high-quality gambling information alongside brilliant graphics, which show up as well as animation. Be that as it may, live gambling establishments permit players to play over the web in a genuine casino environment. By and large, online casino gives plenty of casino activities comprising online poker, baccarat, craps, online port video games, blackjack, and roulettes. Most websites furnish users with choices to play for the sake of entertainment or play for genuine cash. Some sites might expect users to enter a username before playing on the web, and most services are free, yet the user should pay in if they play for genuine cash. The interest in online casino games and the competition between betting platforms brought about the introduction of the new age casino games, many of which were developed by Microgaming.

The online world is an amazing universe that guarantees instant connectivity and instant access to whatever you want from the comfort of your home. Log in and get instant access to whatever you need – goods, movies, and online casino games. And therein lies the biggest threat – when we log in, we provide personal data. And that data can be easily accessed by skilled hackers regardless of the level of security surrounding the repositories where they are

stored. Data breaching is the stuff of new age science fiction and nightmarish reality. If we are someone with evil intentions and the right skillsets, all we must do is hack into systems that store data and manipulate or sell it to those who need it. There have been quite a few instances of major data (supanet, 2019).

Background of the Scandal

Other than the adaptability and commonality of the Elasticsearch server, it is generally near the news titles for its off-base reasons and lack of regard. There is generally insight about data breaches and information being uncovered. While digging further that why there is a general information break it was observed that it is an open-source examination component and data set to store information. Moreover, it has billions of snippets of data and gives the chance of looking at information through a colossal measure of information inside an extremely brief time frame. In addition, the Elasticsearch server gives a cloud-based help, in any case, associations connected with it can utilize another cloud offering or can utilize Elastic-search locally. This inconsequential association utilizes the program to gather the total information in their assortments/vaults which can likewise be known as pails. These assortments incorporate messages, records, crude information, social media, etc.

In January 2019, an online casino group has leaked information on over 108 million bets, including details about customers' personal information, deposits, and withdrawals, which was reported by ZDNet. However, the overall information from the online casino was leaked from an Elasticsearch server (a portable, high-grade search engine that companies install to improve their web apps' data indexing and search capabilities). Such servers are usually installed on internal networks and are not meant to be left exposed online, as they usually handle a company's most sensitive information. The data leaked from an Elasticsearch server that was left exposed online without a password, Justin Paine, the security researcher who discovered the server, told ZDNet. Paine came across one such Elasticsearch instance that had been left unsecured online with no authentication to protect its sensitive content. From a first look, it was clear to Mr. Paine that the server contained data from an online being portal (Cimpanu, 2019)

Regardless of being one server, the Elasticsearch instance took care of an enormous wrap of data that was aggregated from numerous web domains, probably from some sort of affiliate scheme, or a larger company operating a betting portal. After an analysis of the URLs spotted in the server's data, Paine and ZDNet reasoned that all domains were running online casinos where users could put down wagers on exemplary cards and slot games yet in addition to other non-standard betting games. Some of the domains that Paine saw in the defective server included kahunacasino.com, azur-casino.com, easybet.com, and viproomcasino.net, just to name a few. After some digging around, a portion of the domains was claimed by a comparative company, yet others were possessed by a company situated in a similar building at a location in Limassol, Cyprus, or were operating under the same eGaming permit number issued by the public authority of Curacao –a small island in the Caribbean – purposing that they were likely operated by the same entity.

Justin Paine found the user information that spilled from this common Elasticsearch server incorporated a ton of sensitive information, such as real names, home addresses, phone numbers, email addresses, birthdates, site usernames, account balances, IP address, browser and OS details, last login information and a list of played games. Moreover,

```
 3    citizenship : ,
 4    "signupDate": "2019-01-18T04:25:06+00:00",
 5    "custom1": "",
 6    "birthDate": "1980-XX-XX",
 7    "custom3": "",
 8    "portalId": "39",
 9    "secretAnswer": "",
10    "gender": "M",
11    "agentId": "3987",
12    "id": "450XXXX",
13    "secretQuestion": "",
14    "city": "MiddleXXXXXXXXXX",
15    "depositCount": 2,
16    "additional":
      "\"{\\\"a_aid\\\":\\\"goa_b99f66d5-f87b-4ce4-a495-21db58c81fa6\\\",\\\"address\\\":\\\"12
      XXXXX
      Avenue\\\",\\\"city\\\":\\\"MiddleXXXXXXXXX\\\",\\\"zip\\\":\\\"2XXX\\\",\\\"birthdate\\\":\\
      \"1980-XX-XX\\\",\\\"phone\\\":\\\"+610XXXXXXXXXX\\\",\\\"terms\\\":15,\\\"newsletter\\\":fal
      se,\\\"payment_status\\\":\\\"NOT VALIDATED\\\",\\\"gender\\\":\\\"M\\\"}\"",
17    "_consumed_from": "player_affiliate_canada",
18    "birthCountry": "",
19    "bonusAmount": 0.0,
20    "loginCount": 1,
21    "note": "",
22    "state": "",
23    "version": 0,
24    "custom2": "",
25    "providerCode": "qs",
26    "_event_origin": "enricher",
27    "referralCode": "goa_b99f66d5-f87b-4ce4-a495-21db58c81fa6",
28    "email": "XXXXXXXXX@gmx.com",
29    "registrationDate": "2019-01-18T04:25:06+00:00",
30    "username": "XXXXXXXXX8080",
31    "zip": "2XXXX",
32    "terms": 15.0,
33    "lastLogin": "2019-01-19T05:12:27+00:00",
34    "timestamp": "2019-01-19T05:12:27.095120",
35    "isDepositor": true,
36    "phone": "+610XXXXXXXXXX",
37    "subaffiliate": {
```

Figure 2: A very small portion of the redacted user data leaked by the server (Cimpanu, 2019)

Besides, Justin Paine likewise found approximately 108 million records containing data on current bets, wins, deposits, and withdrawals. Data on deposits and withdrawals additionally included payment card subtleties.

```
64    "eventTimestamp": "2019-01-18T15:10:04+00:00",
65    "agentId": "3987",
66    "id": "CE_EVENTS_GROUP_1_V2_canada_ce_events_canada_0_47598668",
67    "_consumed_from": "ce_events_currencies_canada",
68    "event": "WITHDRAW",
69    "instrument": "paymentiq",
70    "_event_origin": "enricher",
71    "instrumentType": "CreditcardWithdrawal",
72    "status": "IN PROGRESS",
73    "amountEUR": 946.7294268893498,
74    "instrumentTransId": "pantaloonew_69819064",
75    "timestamp": "2019-01-18T15:10:04.414738",
76    "processedTime": "0000-00-00 00:00:00",
77    "portal": {
78       "default_lang": "en_GB",
79       "name": "pantaloo",
80       "title": "KahunaCasino",
81       "platformid": 39,
82       "countries": "",
83       "root_agent": 3981,
84       "http_host": "kahunacasino.xyz;kahunacasino.com;kahunacasino.igp;ca-payapi-kah.igp.cloud;",
85       "skin": "pantaloonew",
86       "active": 1,
87       "id": "75"
88    },
89    "eventPayload":
      "\"{\\\"pspFeeBaseCy\\\":null,\\\"txId\\\":\\\"69819064\\\",\\\"maskedAccount\\\":\\\"XXXXXX*
      *****XXXXX\\\",\\\"userId\\\":\\\"4505221\\\",\\\"txAmount\\\":\\\"-1500.00\\\",\\\"txAmountC
      y\\\":\\\"AUD\\\",\\\"txTypeId\\\":\\\"109\\\",\\\"accountId\\\":\\\"40eecc3d-785d-4fe5-8793-
      a778ff43e523\\\",\\\"accountHolder\\\":\\\"XXXXXXXX
      XXXXXXXXX\\\",\\\"provider\\\":\\\"Payvision\\\",\\\"pspFeeBase\\\":null,\\\"pspFeeCy\\\":nul
      l,\\\"attributes\\\":{\\\"successUrl\\\":\\\"https:\\\/\\\/www.kahunacasino.com\\\/payment
      Redirect\\\/success?processor=paymentiq&method=creditcard&type=withdrawal&txId=${ptx.id}\\\"
      ,\\\"failureUrl\\\":\\\"https:\\\/\\\/www.kahunacasino.com\\\/paymentRedirect\\\/fail?pro
      cessor=paymentiq&method=creditcard&type=withdrawal&txId=${ptx.id}\\\"},\\\"txName\\\":\\\"Cre
      ditcardWithdrawal\\\",\\\"pspFee\\\":null}\""
```

Figure 3: A very small portion of the redacted transaction data leaked by the server (Cimpanu, 2019)

The uplifting news was that the payment card subtleties indexed in the Elasticsearch server were somewhat redacted, and they were not exposing the user's full monetary details. Nonetheless, the horrendous news was that people who found the database would have known the names, personal residences, and phone numbers of players who as of late won an amount of cash and could have involved this data to target users as part of scams or extortion schemes.

In addition, there have been multiple Elasticsearch database breaches, yet this is uncommon and one of the biggest to date. Around 5,088,635,374 records (more than five billion) were uncovered after a U.K.-based security firm unintentionally uncovered its "Data breach Database", which put way colossal data-related security occurrences from 2012 to 2019, without secret key insurance.

Legal Issues

A legal issue or issue of law is a legal question that is the foundation of a case. It requires a court's decision. It can also refer to a point on which the evidence is undisputed, the outcome of which depends on the court's interpretation of the law (USLEGAL, 2022).

- **Security patches**

A security patch update is an update that is often pushed from a software developer to all the devices that have the software that needs the update. The purpose of a security patch update is to cover the security holes that major updates or initial software downloads did not (Networkcoverage, 2022). As indicated by the security researchers, an unprotected or unpatched version of the open-source web application which is the Elasticsearch server was at fault. This features the significance of applying the latest updates and security fixes to your company's operating system and any software it utilizes, which are presented by technology companies to fix bugs found in the software or operating system. Because of the carelessness of the organization and not installing the security patch update(s), the hackers got the ideal chance to take advantage of those circumstances.

- **Consumer Litigation**

Continue reading..

- **Extent of penalties**

Continue reading…

- **Compassion for the information**

Information leakage brings about the loss of sensitive data of the clients, and the outcomes can be disastrous. Sensitive information can be uncovered in various ways, including purpose leaks, stray remarks, document theft, and hacker divulgence. While credit checking services will make you aware of the fact that your identity has been taken and help you in disputing charges and accounts opened in your name, they cannot prevent your identity from being taken.

A few businesses are comprised on security controls to stay aware of their adversaries. As indicated by the new Threat Stack study, the greater part of businesses has diminished security endeavours to fulfil deadlines or business needs. Since data breaches have become more extensively publicized, businesses have invested in breach mitigation plans, accepting the "not if, but when" acknowledgment of the certainty of data breaches.

- **Warning**

The server that has been presented to information break should caution all impacted people straightaway. In most cases, the server should be cautious, administrative specialists. The workplace of the Commissioner of the Information was fundamentally cautioned no less than 72 hours of the disclosure of the break as per the GDPR rule.

Social Issues

The changes in computer information technology (IT) infrastructure from a unified, firmly managed mainframe-only computer system with no open Internet ties to a decentralized, for the most part globally re-appropriated environment with plenty of Internet-associated devices all over the planet. A connected change in IT culture in numerous businesses, from one that accentuates internal control and thorough framework testing to one that emphasizes "innovation" and a "get software out quick and fix the bugs later" outlook, which may put a strain on the preeminent senior IT executives to focus cost reserve funds over protection. The Internet's innate absence of assurance as a device planned to be involved by reliable users in academic, corporate, and government research centres before being utilized for business purposes has brought about interminable security refreshes over the underlying framework.

- **Inferior Leadership**

Numerous players and clients have communicated worries about the company's leadership. The tone is set by pioneers, particularly CEOs. From the top, the message should be clear. Everything begins at the top, with a culture of incredible skill, attention to detail, vigorous security controls, and consumer protections. In the event workers do not hear and see this message consistently, pioneers must re-examine how they can show others

how it's done. Online casino companies would now decide if the failure was because of an absence of authority, an absence of arrangement, an absence of precautions, or a lack of unfortunate practices.

- **Belated information to the customer**

Continue reading…

- **No safety of the data**

    Online casino breach was brought by an absence of security mindfulness and inability to fix an obscure vulnerability, rather than malicious attacks from a country state or a worldwide malware crusade

- **Not a proper credit bureau**

    For many players, one of the troublesome parts of the data breaks is that they have little control over whether their information is utilized in the scheme. Even though web-based gambling company lacked sufficient cybersecurity initiatives, players' and clients' assessment has not remained predominantly negative. Following that, many started to address on the off chance that they could trust the organizations, and everyone was stressed about what if their data would be stolen and used improperly.

- **Gluttony of notoriety**

    Since individuals were concerned enough about their FICO assessment to pay online gambling club organizations to analyse their released data, most of which had proactively been hacked, representing a gamble of burglary, which would adversely affect their financial assessment. Likewise, after becoming mindful of the information break, online gambling club organizations decided not to tell their clients, liking to go on with the same old thing until the information break became gigantic.

Ethical Issues

Ethical issues occur when a given decision, scenario, or activity creates a conflict with a society's moral principles. Both individuals and businesses can be involved in these conflicts since any of their activities might be put into question from an ethical standpoint. Individuals are subject to these issues in their relationships with other individuals or in their relationships with organizations and the same goes for organizations. These conflicts are sometimes legally dangerous since some of the alternatives to solve the issue might breach a particular law. On other occasions, the issue might not have legal consequences, but it might generate a negative reaction from third parties. Ethical issues are challenging because they are difficult to deal with if no guidelines or precedents are known. For this reason, many professional and industry associations have ethical codes that are discussed and approved by key participants to provide a useful framework for companies and individuals to make adequate decisions whenever they face one of these conflicts (MyAccountingCourse, 2022).

- **Virtue Theory**

According to the virtue theory, virtue means doing the right thing at the right time in the right way, in the right amount, toward the right people (Baase, 2022) However, the online casino group did not pass the information to its client about the breach in the right time which was not the legitimate step taken.

- **Deontological Theory**

According to the deontological theories, rationality is the standard for what is good, and deontologists argue that logic or reason determines rules of ethical behavior and that actions are intrinsically good because they follow logic (Baase, 2022). Online casino group said that they uncovered the truth to its client solely after the guarantee of the breach and stealing of their information. It should not have been that way rather all information about the customer's data needed to be informed.

- **Utilitarianism Theory**

The principle of Utilitarianism says, "In any given situation, you should choose the action that produces the greatest food for the greatest number" – the principle of utility. An act is right if it tends to increase aggregate utility (Baase, 2022). An act is wrong if it tends to decrease aggregate utility. The organization's choices were troublesome to all parties involved. The data was at risk, a great number of the investor were at misfortune and a large portion of the businesses surrendered. Nobody was happy with the insight about the breach later.

- **Rights**

Online casino groups did not keep their clients' updates about their information before the breach was public as it's their right to know about their private information. Moreover, they did not illuminate their accomplices and investors as they were at an enormous misfortune.

- **Social Justice**

Continue reading…

Professional Issues

One of the biggest data breaches relating to the online casino industry was detected at the beginning of 2019. What was alarming was the sheer volume of data left exposed there was information about a whopping 108 million wagers (supanet, 2019). Database which contained more than 70 million log files comprising nearly 100 GB of data stored from March 2019 including detailed device data, links to photos and videos, and around 800,000 email addresses have been stolen at the same time.

- **Accountability for cybersecurity**

The online casino industry uses the cloud base service to store all its information in depositories (also known as buckets), which include emails, spreadsheets, social media

posts, files- basically any raw data in the form of text, numbers, or geospatial data. Unfortunately for elastic, this has resulted in many high-profile breaches involving well-known brands from a variety of industries (Russell, 2020). Because of unfortunate cybersecurity rehearses, the online casino group left itself at risk. The online casino group was unable to detect attackers getting to its network since it did not take suitable measures to track approaching malicious traffic.

Companies that fail to invest in their own cybersecurity readiness must recognize that the fines they could face for non-compliance with data privacy laws are incredibly expensive not to mention the cost of losing the trust of their customers," Campagna added. "In fact, Google was just fined $57 million by CNIL, the French data protection watchdog, for failing to comply with GDPR's transparency and consent laws" (Riley, 2019).

- **Justice and Fairness**

 Continue reading…

- **Breach of contract**

Continue reading…

- **Existence of Duty**

The online casino industry chose to notify the clients and players as soon as possible of the information break since time is a factor in relieving harm. When data breach casualties are made mindful of the breach, they will do whatever it may take to relieve the damage. The longer a fraud goes on, the more cash is stolen, and out-of-pocket expenses increase.

- **Integrity**

It is one of the rules for PC proficiency, truth be told, and fair. It depicts speaking the truth about the capabilities and imperatives in experience to finish any job. They ought to be affable to the clients and offer all the required or related data about programming, representatives ought to open up to the capacities, security, and restrictions of the application. However, on account of the Elasticsearch server after the colossal information

spillage, just the association was just educated yet not clients which is a real sense disregards the uprightness, and which is a conspicuous infringement of the set of principles ACM and IEEE CS since the code features the essential moral upsides of honesty and decency including specific activities.

Conclusion

To whole up, with online casinos transforming into a staple substitute across countries like the United Kingdom, various sites are appearing suddenly and not all are safeguarded or secure. Countless billions of trades happen online through Mastercard's, e-wallets, and wire moves in web betting conditions. These spot wagering firms are among the best focuses for developers and extortionists. There are two critical courses through which advanced criminals centre around their assets, and they integrate getting the money and getting hold of exclusive information shared by performers. That is the reason it is fundamental for online wagering foundations to make arrangements that are liberated from any risk for both the customers and the managers. The data breach affected users from nearly every continent, with some countries reporting a higher amount of user activity. The average number of daily users in the United States was over 10,000, while Canada had 7, 700, likewise, Australia had 6,200, and Brazil had 3,800.

"Free wagering and gaming applications are specifically unarmed against assaults and hacks from cybercriminals," as indicated by the specialists, who are after clients' very own information or incorporate hazardous programming to get to their gadgets. "Cybercriminals could putatively hack other applications, view records saved money on the gadget, settle on decisions, and send SMS from the hacked gadget assuming that they utilized this progression to introduce malware or comparable onto a client's telephone," specialists added. "More terrible yet, on the grounds that people all around the world were under isolation or self-disconnection because of the Coronavirus pandemic, the effect of a break like this might be far more terrible. An aggressor could utilize the presented data to send off phishing assaults against purchasers, presenting them with additional information and monetary gamble. The makers likewise risk losing a huge number of gamers, and on the grounds that a considerable lot of the clients are

from Europe, Europe's protection office could hit the organization with an enormous charge for the information spill.

At long last, the most secure game-plan for the EU is to adopt a rivalry regulation strategy that coordinates specific information insurance standards. This coordinated technique would add an additional level of safety for the two customers and organizations to the EU's current powerful collections of rivalry and information insurance regulation. If accurately executed, it can diminish the risk of client hurt from information breaks as well as the capability of punishments for significant associations with gigantic volumes of uncovered buyer information. The incorporated arrangement is adequate since it is direct to execute and gives huge advantages to all partners: clients, organizations, and the public authority. The consolidation survey methodology, which is the central issue of correspondence among organizations and the public authority, can be utilized to carry out this procedure.

Continue reading…

Appendix

- **Introduction (Continue Reading……)**

Back in early 2010, when the first version of Elasticsearch was released, the future (we were dependably informed) was orange. Or on the other hand, was it black? Or green? No one truly knew. No one knew how the NoSQL space would advance, nor how Elasticsearch would turn out to be utilized. In those days, we attempted to have a horse in every race. We could converse with Elasticsearch with JSON, YAML, SMILE, CBOR, Thrift, and Memcached protocol. We could indicate settings using JSON, YAML, Java properties, and environment variables. Something that made Elastic search so well-known was its adaptability and its familiarity. It was not difficult to get everything rolling, and simple to integrate Elasticsearch into our application, regardless of how unusual the design was. Six years later, Elasticsearch has evolved into a strong pursuit and analytics engine. It has been downloaded by millions of people and is a center innovation relied upon by hundreds of thousands of users and companies. Adaptability and leniency are no longer as significant as:

- o   A reliable stable cluster
- o   Predictable performance

- o Clear error message
- o Warning early about problems that may occur in production
- o Safety from attacks

- **Background of the scandal (Continue Reading….)**

Security analyst Bob Diachenko found the cracked database. Depicting it as "Data was all-around organized", Diachenko expressed that the flawed database contains colossal information of previously reported and non-reported security incidents subtleties, which include:

- Hash type (the way a password was presented: MD5/hash/plaintext, and so forth.)
- Leak date (year)
- Password (hashed, encrypted, or plaintext, depending on the leak)
- Email
- Email domain
- Source of the leak

Attackers might take advantage of the sensitive information exposed to database leaks. Hackers can send off designated phishing attacks, participate in account takeover extortion, and even sell the stolen data on the dark web.

Elasticsearch servers have continued to leak the protected personal information of millions of people and organizations. The latest server breach happened when Peekaboo's application developer, Bithouse, left the Elasticsearch database open, which contained more than 70 million log records involving almost 100 GB of information stored from March 2019. The uncovered information included detailed device data, links to photos and videos, and around 800,000 email addresses. There has forever been a security concern about Elasticsearch servers. Security specialists focused on that breach happens because of a built-in assurance when there are no password protections or firewalls. Indeed, even Elasticsearch gave a few suggestions on the most proficient method to get their servers, which include secure authenticated sign-in, appropriate encryption, layered security, and review logging (Cisomag, 2020).

- **Legal Issues (Consumer Litigation (Continue reading….))**

With consumer protection lawsuit cases, citizens take legal action against companies that engage in misleading practices or scams, fail to protect personal information, or provide poor service. New York and New Jersey laws allow consumers to sue for actual damages, plaintiff legal fees, and punitive damages in instances where the business practices were wilful or done in bad faith (KGGLaw, 2022). Here, victims of data breaches will be able to file a grievance. In January 2019, an online casino group leaked the names, social security numbers, birthdates, emails, and credit card details of more than 108 million people.

- **Legal Issues (Extent of penalties (Continue reading…))**

As the monetary operation is levied by any provincial division, the fines will shift incredibly and are normally reliant upon the severity of the encroachment, as well as the number of people concerned and the idea of the compromised information. Online casino companies need to pay the refund to the clients and players and proposition credit insurance to those whose information was spilled. Businesses who do not adhere to the laws of regulators, for example, the OFFICE for Civil Rights under HIPAA or the PCI DSS Security Standards Council face fines and penalties.

- **Social Issues (Belated information to the customer (Continue reading…))**

According to the security researcher, it was found that a portion of the domains was possessed by a similar organization, while others were claimed by organizations situated in a similar structure in Limassol, Cyprus, or worked under a similar eGaming permit number given by the public authority of Curacao — a little Caribbean Island — suggesting that they were doubtlessly worked by a similar substance. The partnership consumed a large chunk of the day to instruct its clients, which was a huge advertising issue. A sum of 108 million wagers was possibly uncovered because of the hack.

- **Ethical Issue (Social Justice (Continue reading…))**

Historically and in theory, the idea of social justice is that all people should have equal access to wealth, health, well-being, justice, privileges, and opportunity, regardless of their legal, political, economic, or other circumstances. It is often associated with identity politics, socialism, and revolutionary communism (investopedia, 2022). To which, the accomplices and the clients were not informed eventually by the online casino group which is not legitimate justice to its kin.

- **Professional Issues (Justice and Fairness (Continue reading…)**

Justice should be characterized as adherence to rules of conduct, whereas fairness should be characterized as people's moral evaluations of this conduct. In this case, there has been a scarcity of compensatory justice. Companies have a moral responsibility to obey fairness principles whilst compensating clients for harm they have caused. Online casino groups harm patron and gamers by failing to safeguard their personally identifiable information and endangering their financial security. Regardless of whether the client did not suffer identity fraud immediately after the breach or throughout the protracted process, personal information misfortune is irreversible withinside the virtual era.

- **Professional Issues (Breach of contract (Continue reading…))**

A contract is breached or broken when any of the parties fails or refuses to perform its promise under the contract. A breach of contract is a legal cause of action in which a binding agreement is not honoured by one or more parties by non-performance of its promise by him renders it impossible (ipleaders, 2017). Thus, a contract violation is as often classified as either a "material breach" or an "immaterial breach" for recognizing the suitable legal solution or "remedy". In this case, the company swore that the clients' information and security would not be uncovered and kept confidential, but this promise was broken, resulting in a contract breach.

- **Conclusion (Continue reading….)**

To effectively avoid Elasticsearch (or similar) data breaches, a different mindset to data security is required and one that allows data to be a) protected wherever it may exist, and by whoever may be managing it on their behalf. Standard encryption-based security is one way to do this, but encryption methods come with sometimes-complicated administrative overhead to manage keys. Tokenization, on the other hand, is a data-centric security method that replaces sensitive information with innocuous representational tokens. This means that, even if the data falls into the wrong hands, no clear meaning can be derived from the tokens. Sensitive information remains protected, resulting in the inability of threat actors to capitalize on the breach and data theft (Russell, 2020).

References

Admin, 2010. *Online Casinos Description.* [Online]
Available at: https://www.casinobonusboard.com
[Accessed 10 May 2022].

Baase, S., 2022. *Ethics.* Kathmandu: Pearson.

Cimpanu, C., 2019. *Online casino group leaks information on 108 million bets, including user details.* [Online]
Available at: https://www.zdnet.com
[Accessed 11 May 2022].

Cisomag, 2020. *Unprotected Elasticsearch Server Leaks 5 Billion Records.* [Online]
Available at: https://cisomag.eccouncil.org
[Accessed 11 May 2022].

investopedia, 2022. *Social Justice.* [Online]
Available at: https://www.investopedia.com
[Accessed 11 May 2022].

ipleaders, 2017. *A BRIEF OVERVIEW ON BREACH OF CONTRACT.* [Online]
Available at: https://blog.ipleaders.in/a-brief-overview-on-breach-of-contract/?msclkid=f285d4c5d13411eca91c5ca617157927
[Accessed 11 May 2022].

KGGLaw, 2022. *Consumer Protection Lawsuits.* [Online]
Available at: https://www.kgglaw.com/class-action-lawsuits/consumer-protection/#:~:text=With%20consumer%20protection%20lawsuit%20cases%2C%20citizens%20take%20legal,provide%20poor%20service.%20Lawsuits%20may%20be%20filed%20against%3A
ainst%3A
[Accessed 12 May 2022].

localhistories, 2021. *A History of Online Casinos.* [Online]
Available at: https://localhistories.org
[Accessed 11 May 2022].

MyAccountingCourse, 2022. *What are Ethical Issues?*. [Online]
Available at: https://www.myaccountingcourse.com
[Accessed 11 May 2022].

Networkcoverage, 2022. *Why is it Important to Update Security Patches?*. [Online]
Available at: https://www.netcov.com/why-is-it-important-to-update-security-patches/
[Accessed 12 May 2022].

Riley, D., 2019. *108M online casino customer records exposed in latest case of misconfigured database.* [Online]
Available at: https://siliconangle.com/2019/01/21/108m-online-casino-customer-records-exposed-latest-case-misconfigured-database/?msclkid=fe75e0f3d14011ec9d074c2a6a3249da
[Accessed 11 May 2022].

Russell, A., 2020. *What is Elasticsearch and why is it involved in so many data leaks?*. [Online]
Available at: https://www.techradar.com
[Accessed 11 May 2022].

supanet, 2019. *The Biggest Online Casino Data Breaches - Updated.* [Online]
Available at: https://www.supanet.com
[Accessed 11 May 2022].

USLEGAL, 2022. *Legal Issue Law and Legal Definition.* [Online]
Available at: https://definitions.uslegal.com
[Accessed 11 May 2022].

20048968