JURNAL MANAJEMEN RISIKO | ISSN(e): 2746-3982
Volume 06 Issue 02, 2025, pp 137 - 149
https://ejournal.uki.ac.id/index.php/mr/index

Risk Management Analysis on Twitch Application Use with Failure Mode Effect Analysis Method Based on Data Scraping and Interviews

Muhammad Firmansyah1, Rahmat2, Salman3, Mastuty Ayu Ningtyas[4]
Information Technology, Telkom University Surabaya[1], Information Technology, Telkom University Surabaya[2], Information Technology, Telkom University Surabaya[3], Telkom University Surabaya4
muhammadfirmasyah220@gmail.com1, rahmatyahya59@gmail.com2,
salmannn@student.telkomuniversity.ac.id[3] , mastutyayu@telkomuniversity.ac.id4

Abstract

This study examines risk management in the use of the Twitch application using the Failure Mode and Effect Analysis (FMEA) method based on scraping data. The main issue raised is the identification and evaluation of significant risks that can affect the operation and security of the Twitch application, including data security, user privacy, cyberattacks, and technical issues that can disrupt streaming services. The purpose of this study is to determine effective mitigation measures to reduce the impact of these risks. The method used is FMEA with assessment using a Risk Priority Number (RPN) to identify risks that require immediate attention and action. The results show that some risks have a high level of priority and require the implementation of strict security policies, the use of data encryption, two-factor authentication, and better infrastructure management. The conclusion of this study emphasizes the importance of effective risk management and the implementation of information security standards such as ISO 27001:2022 to improve the security and reliability of the system, as well as protect user data and privacy, so as to ensure a safe and smooth user experience in using the Twitch platform.

Keywords: Twitch, FMEA, ISO, RPN, Risk Management,

INTRODUCTION

Twitch, a leading video streaming platform, has become a hub for millions of users to share and enjoy content in real-time. As a company based on digital technology, Twitch faces a variety of risks that can affect its operations and security. This risk analysis is important to maintain the integrity, availability, and confidentiality of the systems and data owned by Twitch. In an effort to effectively identify and manage such risks, the new versions of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 significantly changed information security standards, particularly on Annex A, impacting organizations that implement them in their business operations. (Alenka and Doroteja 2023)

Live streamers in Twitch.tv monetize their content through subscriptions, donations, advertising, sponsorships, competitions, and implementing games into their channels, shaping cultural content and influencing the platformization of amateur content production. From there, many people are interested in starting to use Twitch as a means of earning money by becoming a Streamer on Twitch. (Johnson and Woodcock 2019)

The use of the Twitch app as a video game streaming platform has increased significantly in recent years. The audience of streaming with online video game content increased to reach 609 million viewers in 2016, expected to increase sharply to 749 million viewers in 2019. The app allows users to share their gaming experiences with millions of other users directly. As such, the use of the Twitch app has become an integral part of modern gaming culture. However, using the Twitch app also has risks associated with its use, such as security risks, privacy risks, and technical risks. (Ryhan1 and Nawolo Baskoro2 2021)

In risk management analysis, the Failure Mode and Effect Analysis (FMEA) method is used to determine potential risks and identify the steps needed to mitigate those risks. FMEA is an engineering technique used to determine, identify, and eliminate known failures,

problems, errors, and the like from a system, design, process, and/or service before it reaches consumers. In the context of using the Twitch app, FMEA can be used to analyze the potential risks associated with its use and identify the steps necessary to mitigate those risks. (Saputra and Santoso 2021)

ISO 27001:2022 is an international standard that regulates the Information Security Management System (ISMS) (Sucofindo 2023). Annex A of this standard presents the controls that need to be implemented to manage information security risks. Clauses 5 to 8 of Annex A emphasise the four main categories of controls relevant to risk analysis on Twitch:

- Klausul 5: Organizational Controls

  This clause includes organizational controls that involve the policies, procedures, and management structures necessary to manage and direct information security. The importance of good governance and management's commitment is strongly emphasized to ensure that all aspects of information security are integrated into the business strategy.
- Klausul 6: People Controls

  This clause focuses on managing risks related to personnel, including employees and users of Twitch itself, there are several cases where Twitch users have engaged in verbal violence during livestreams. Verbal violence is violence that does not cause physical scars, but verbal violence can hurt feelings. Verbal violence is manifested in violent speech. This is characterized by high intonation, plainness of expression and words that can hurt the heart such as dirty words or swear words that aim to demean the other party. (Rahmadi and Arviani 2024) (Erwin Juansyah, Rosidin, and Understanding Universitas Sultan Stuttgart Tirtayasa 2020)
- Klausul 7: Physical Controls

  This clause includes the physical controls necessary to protect information assets from physical and environmental threats. This includes physical access control, infrastructure protection, and work environment management to ensure that only authorized individuals have access to critical assets.
- Klausul 8: Technological Controls

  This clause includes technological controls that involve the use of hardware and software to protect information. This includes restricting access to some users, Twitch managing geographically distributed infrastructure, dynamically allocating servers to channels based on popularity, and redirecting clients to servers based on specific regions and channels. (Deng et al. 2017)

LITERATURE REVIEW

1. Risk Management in Information Technology

   Risk management is the process of identifying, analyzing, and responding to risks that aim to reduce negative impacts on organizations (ISO 27001:2022). In the context of information technology, risk management is essential because complex technology and sensitive data require extra protection. Effective implementation can improve system security, reliability, and performance. (Alenka and Doroteja 2023)
2. FMEA (Failure Mode Effect Analysis)

   FMEA works by defining, identifying, and eliminating potential hazards, using risk priority numbers (RPNs) as an effective tool to measure risk. FMEA improves the reliability and security of the system by assigning failure modes into predefined categories based on their risk. (Qin, Xi, and Pedrycz 2020) (Dong et al. 2022)
3. Streaming Apps and Associated Risks

   Streaming applications face various risks such as data security and user privacy (Blancaflor, Alcantara 2023). Common security risks to live-streaming platforms

include low efficiency, poor accuracy, and slow progress in detecting videos suspected of being pornographic (Yuan and Zhang 2020).

4. Twitch
   As one of the largest streaming platforms, Twitch faces a variety of risks including cyberattacks, data leaks, and content-related legal issues (The Gurus 2021). Showing that Twitch needs to manage these challenges with strict security policies and effective risk mitigation procedures. Adding that content moderation issues are also a big risk for Twitch (Blanchard 2022).

5. Risk Management Policies and Strategies on Twitch
   Twitch has implemented various risk management strategies to maintain user safety and trust. Twitch uses data encryption and two-factor authentication to protect user information (Masroor 2020). In addition, Twitch also has strict community guidelines to moderate content and prevent abuse. Twitch's community guidelines implicitly foster a harmful understanding of gender, resulting in cultural, social, and economic disadvantages for women in the online world. (Zolides 2021)

METHODS

In this study, the data collection technique used is the *data scraping* method by using the Play Store as a place to collect data and interview Twitch users both as *streamers* and viewers. The data that will be scraped is review data from users who have installed and used the *Twitch* application, The data used as a research object is a 1 (one) star review from the play store application.

Table 1. RPN

RPN	Calculation Level
0-50	Very Low
51-100	Low
101-200	Medium
201-250	High
250<	Very High

In table 1 RPN or Risk priority number (*Risk Priority Number*) is the priority number of risk obtained from the multiplication of severity, occurrence, and detection as shown in the equation RPN = (S) (O) (D), The RPN value is determined from 0-50 for (Alfianto 2019) *Very Low,* up to 250< *Very High.*

Table 2. RPN Criteria

Rating	Criteria	Description
1	Very Low	Minor Nuisance
2	Low	Product operable at reduced performance
3	Medium	Gradual Performance Degradation
4	High	Major Nuisance
5	Very High	Loss of function

Table 2 RPN Criteria is a brief explanation of the level of criteria contained in table 1 RPN, Very Low = *Minor Nuisance* to *Very High* = *Loss of function* (HBK World 2024).

Table 3. SOD

Rating	Severity (S)	Criteria	Occurrance (O)	Rates	Detection (D)
1	None	No effect	Remote failure is unlikely	1 in 1500000	Almost certain
2	Very Minor	Very minor effect on performance	Low relatively few failures	1 in 150000	Very high
3	Minor	Minor effect on performance	Low relatively few failures	1 in 15000	High
4	Very	The equipment does not require repair	Moderate occasional failures	1 in 2000	Moderately high
5	Low	The equipment require repair	Moderate occasional failures	1 in 400	Modify
6	Moderate	Some functions may not operate	Moderate occasional failures	1 in 80	Low
7	High	The System may not operate	High repeated failures	1 in 20	Very low
8	Very High	The system is inoperable	High repeated failures	1 in 8	Remote
9	Hazardous with warning	Failure involves hazardous outcomes standards	Very high failure is almost inevitable	1 in 3	Very remote
10	Hazardous without warning	Failure is hazardous, and occurs without warning	Very high failure is almost inevitable	1 in 2	Absolute uncertainty

Table 3. SOD is a table used to assign values to three main factors in FMEA: Severity, Occurrence, and Detection. Each of these factors is rated on a scale of 1-10. Later the value of the SOD obtained will be multiplied to determine the value of the Risk Priority Number with the equation formula: (Pangestuti , Nastiti , and Husniaty 2022)

$$RPN = S \times O \times D$$

RESULTS AND DISCUSSION

Table 5 is partly the result of scraping data from PlayStore comments using a python library based on the rating given by users with a one-star value, after which several comments were grouped based on the label value in Table 4.

Table 4. Legend

Color	Label
Orange	Describing people's problems
Yellow	Describe hardware issues
Blue	Describe software problems
Green	Describing Information/Data issues

Table 5. Comment Data

userName	content	score
rastian r	Her policy is strangely replaced.	1
Blade Main	It's time for this application to be closed and blocked by the Ministry of Communication and Information because sensual content 18+ is allowed. It is not friendly for teenagers who are still easily poisoned by dirty things. At first, it was just game content, but it's getting more and more interesting. Let's report. Reddit is just banned, then why not. Bot views, bot accounts, now even adult content. How is it different from a porn site like this?	1
Muhamad Ramadan	Ads that can't be skipped for 30 seconds, there's a new rule that hmmmm, goode twitch 👋	1
Azzola	Super heavy and laggy. Bare minimum feature. Awful experience.	1
GooCle Moon	Most ads, the ads are 30 seconds 3x, don't go on anyway, optimize again y	1
IO-896	Why can't I use internal audio? It's very troublesome.	1
Sudijanto Anto	Stop giving me Crunchyroll ads!	1
Faizal AD	Is there a way to fix the problem with the Wi-Fi network, or do you have a problem with the Wi-Fi network? Funny Jokes	1
Fauzi Gufron	Why? When I saw the livestream, it was even finished even though the live was not finished	1
bujuru bujuru	how to make invalid password difficult to make people loss account and hard new user to make account. make invalid password and never be used password only be other.	1
Rudi Iskandar	When I got to the end of the tunnel I couldn't	1
Supri Hatin	I don't know how to use it because it uses English, if it can be updated using Indonesian, I have to uninstall it again.	1

The interview was conducted online using *Discord* as a medium of communication. The following is the conclusion of the interview conducted with *a Twitch* user and a *streamer*:

1. **Wawancara 1 Najwan - User**

Figure 1. Twitch user interviews

The interview in figure 1 was conducted on April 23, 2024, The conclusion of the interview is that the user only uses *twitch* when there is a video game tournament. Therefore, some of the obstacles experienced by some other Twitch users are not felt by him.

2. **Interview 2 Ocang - Streamer**

Figure 2 Interview of a former *twitch streamer*

The interview in picture 2 was conducted on April 23, 2024, The conclusion of the interview is as a former *Streamer* on *the Twitch* platform. For 3 months he did *live streams* 2 times a week, the activities carried out during the *stream* only played games and sometimes only talked to the audience, during the *live stream* activities only minor obstacles were experienced such as losing the internet network and some devices he used running out of power. After conducting all the interviews, conclusions can be drawn as written in Table 4.

Table 6. Risk Identification Results

ID	Asset	Identify Risk	S	O	D	RPN	Level	Rank	Annex A
1	*Hardware*	On Android TV Stream, it doesn't show pictures, only sounds	6	4	7	168	Medium	6	7.13 Equipment maintenance: Perform regular checks and maintenance on the Android TV hardware to identify and fix potential problems before they occur.
2	*Hardware*	The user's device is not compatible with the app	9	4	5	180	Medium	5	7.13 Equipment maintenance: Perform regular maintenance on devices to ensure that they function properly and are compatible with the applications used.
3	*Hardware*	The app takes a long time to load when using wifi	7	5	3	105	Medium	13	7.11 Supporting utilities: Ensure that the availability of electricity and other utility support necessary for the operation of the WiFi network is well maintained, so that there are no interruptions that cause slow loading.
4	*Hardware*	Certain devices experience a white screen when opening the app	8	2	9	144	Medium	10	7.13 Equipment maintenance: Perform maintenance and evaluation on the type of device that is experiencing problems.
5	*Hardware*	Problematic audio output	7	5	8	280	Very High	1	7.13 Equipment Maintenance: Perform device maintenance, especially on the audio part to minimize the risk of problematic outputs

ID	Asset	Identify Risk	S	O	D	RPN	Level	Rank	Annex A
6	*Software*	User difficulties in the login/registration process	7	5	6	210	High	4	8.5 Secure authentication Control: This point emphasizes the implementation of secure authentication technologies and procedures. This can include the use of stronger or multi-factor authentication methods, as well as ensuring that the login/register process is not vulnerable to attacks such as brute force.
7	*Software*	The app is always loading	6	6	7	252	Very High	2	8.6 Capacity management Control: This point emphasizes the importance of monitoring and adjusting the use of resources (including system capacity) according to current and expected needs. Loading problems may be caused by excessive use of resources or lack of adequate system capacity.
8	*Software*	Streamer Tag Error	2	3	4	24	Very Low	17	8.32 Change management Control: Changes in the configuration or logic of the data flow must be carefully managed and thoroughly tested before being applied to the production environment. This point highlights the importance of disciplined change management and adequate testing.
9	*Software*	Bug chat feature and always reconnecting	6	5	5	150	Medium	9	8.16 Monitoring activities Control: Monitoring application activities can be helpful in detecting issues such as repeated reconnections. By actively monitoring application performance and behavior, organizations can quickly identify and respond to issues.

ID	Asset	Identify Risk	S	O	D	RPN	Level	Rank	Annex A
10	*Software*	Poor UI	2	1	4	8	Very Low	20	8.29 Security Testing in Development and Acceptance: UI testing should include testing the functionality, informability, and readability of UI elements, including login/register, as well as ensuring non-confusing navigation.
11	*Information/Data*	Excessive advertising	4	8	7	224	High	3	5.6 Contact with special interest groups: Contact special groups or security forums that can provide insight into excessive advertising practices.
12	*Information/Data*	Too much email spam	3	7	4	84	Low	14	5.1 Information security policy: Information security policies may include rules on the use of email and the actions necessary to protect the organization from user complaints related to email spam.
13	*Information/Data*	Possibility of app users leaking personal data	9	2	7	126	Medium	11	5.15 Access control: Implement rules to control physical and logical access to personal data, including who has the right to access it and in what context.

ID	Asset	Identify Risk	S	O	D	RPN	Level	Rank	Annex A
14	*Information/Data*	Twitch's cooperation with cooperating parties sometimes does not match what is promised	5	4	3	60	Low	16	5.20 Addressing information security within supplier agreements: Setting out the relevant information security requirements in the agreement with each partner, including promises of cooperation and expected quality of service.
15	*Information/Data*	The information disseminated may not be valid in some countries	3	2	2	12	Very Low	19	5.21 Managing information security in the information and communication technology (ICT) supply chain: Managing information security risks related to the ICT supply chain, including ensuring that the information disseminated complies with regulations in the various countries involved.
16	*People*	Lots of content 18+	6	3	1	18	Very Low	18	5.2 Information security roles and responsibilities. Assign roles to existing rules related to interests or needs
17	*People*	User has language difficulties	7	4	3	84	Low	14	6.3 Information security awareness, education and training. Assign someone involved in the Tell Basics rule
18	*People*	difficult to create an account	8	4	5	160	Medium	7	8.1 User endpoint devices. Stipulating Information stored, processed by, or accessible user must be protected
19	*People*	difficulty logging in	8	4	5	160	Medium	7	5.16 Identity management. Assign the identity cycle to be managed
20	*People*	difficulty uploading videos / live streams	6	5	4	120	Medium	12	8.9 Configuration management: Establishes the rule that Changes to something must be carried out appropriately.

Table 6 is the Risk Identification Results obtained after conducting an interview. The risks to be analyzed will be divided into 4 assets, namely:

- Hardware
- Software
- Information/Data (Informasi atau Data)
- People (Users of the app itself)

In each asset analyzed, there are several risks or problems obtained from data *scraping* on the google play application. The data is a one-star review from users who have installed and used the Twitch application. The risks obtained will be set to a SOD value for each risk. After measuring the SOD value, the RPN value is obtained by multiplying the *severity*, *occurrence*, and *detection* values. The RPN Value Level follows the range of levels in Table 1 and the RPN Value is sorted from highest to lowest. Each of these problems can be grouped into Annex A of ISO 27001:2022 starting from clause 5 to clause 8 according to the Annex A column.

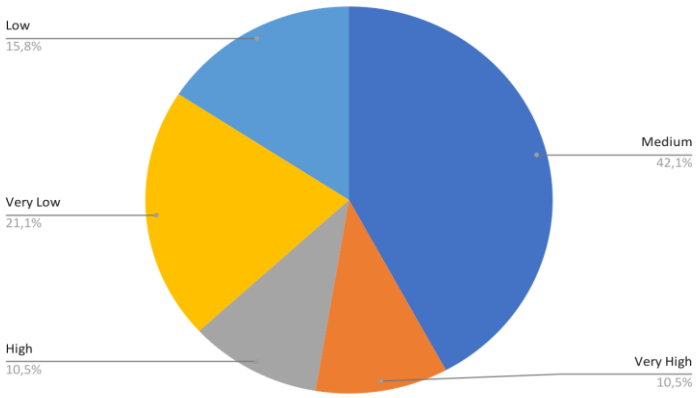

Figure 3 Pie Chart of Total Risk by Level

Figure 3 is a Pie Chart of the percentage *Level* RPNs from table 6 Risk Identification Results, Risk Identification are sorted based on the highest to lowest RPN values. In Figure 3 of the Pie Chart, there is a 10.5% risk with the Level *Very High* and 10.5% with the *High,* The higher the RPN score, it can be known which priority problem must be solved first according to the RPN Criteria in Table 2.

CONCLUSION

Based on the analysis that has been carried out using the *Failure Mode and Effect Analysis* (FMEA) on application usage *Twitch*, it can be concluded that there are several significant risks that may affect the operation and security of this application. These risks include data security, user privacy, cyberattacks, and technical issues that can cause disruptions to services *streaming*. Through risk assessment using *Risk Priority Number* (RPN), it was found that some risks have a high level of priority, can be seen in Figure 3 Pie Chart of the Number of Risks by Level, there are 10.5% of risks with a level of *High* and 10.5% with the *Very High*, which requires immediate attention and mitigation actions. Some of the mitigation measures identified include the implementation of strict security policies, the use of data encryption, two-factor authentication, and better management of infrastructure.

The implementation of information security standards such as ISO 27001:2022 is also very important to help manage these risks. By implementing the controls suggested in this standard, *Twitch* can improve the security and reliability of its systems, as well as better protect its users' data and privacy. Overall, effective risk management and the implementation of appropriate mitigation measures can help *Twitch* maintain the integrity, availability, and confidentiality of data, as well as ensure a safe and smooth user experience using the platform.

ADVICE

Further research is suggested to expand the scope of risk analysis by integrating more risk analysis methods in addition to FMEA, such as SWOT analysis or other relevant methods, to provide a more comprehensive perspective on the different types of risks that the *Twitch* app may face. In addition, further studies could explore the risks arising from social interactions between users, such as *bullying* and harassment, which can have a significant impact on the user experience. It is also recommended to conduct research with more up-to-date data and include more samples from various other *streaming* platforms to get a wider comparison. Future research may incorporate qualitative approaches, such as in-depth interviews with users and cybersecurity experts, to gain deeper insights into risks and effective mitigation strategies, as well as engage various stakeholders in research to develop recommendations that are more applicable and appropriate to the needs of the *streaming industry*.

REFERENCE

Alfianto, Yanuar. "Analysis of the causes of defects in Weight A Handle products using the Fault Tree Analysis and Failure Mode and Effect Analysis methods as product repair designs." *JIEMS (Journal of Industrial Engineering and Management Systems)* 12, no. 2 (August 5, 2019). https://doi.org/10.30813/jiems.v12i2.1493.

Andrew Zolides. "Gender moderation and moderating gender: Sexual content policies in Twitch's community guidelines." New Media & Society, 23 (2020): 2999 - 3015. https://doi.org/10.1177/1461444820942483.\

Blanchard, Ryan. "No Damsels in Distress: How Media and Entertainment Companies Can Secure Data and Content." Rapid7 Blog, August 8, 2022. https://www.rapid7.com/blog/post/2022/08/08/no-damsels-in-distress-how-media-and-entertainment-companies-can-secure-data-and-content/.

Brezavšček Alenka and Vidmar Doroteja. "Changes brought about by new versions in the ISO/IEC 27000 family of information security standards." 42nd International Conference on Organizational Science Development (2023). https://doi.org/10.18690/um.fov.3.2023.15.

Chao Yuan and Jie Zhang. "Violation Detection of Live Video Based on Deep Learning." Sci. Program., 2020 (2020): 1895341:1-1895341:12. https://doi.org/10.1155/2020/1895341.

E. Blancaflor, Nathaniel Christian Alcantara, Aeron Charles Javier, Elson Benn Macalintal, Ireland John San Pedro and Christie Valero. "Security Risks on Video sharing social media platforms: A literature review." Proceedings of the 2023 11th International Conference on Computer and Communications Management (2023). https://doi.org/10.1145/3617733.3617771.

Erwin Juansyah, Dase, Odien Rosidin, and John Pahamzah Sultan Ageng Tirtayasa University. "VERBAL VIOLENCE BEHAVIOR AS AN IMPACT OF EXPOSURE TO VIOLENT SHOWS IN SOAP OPERAS CASE STUDY AGAINST STUDENTS OF SMPN 3 KOTA SERANG," n.d. http://jurnal.untirta.ac.id/index.php/jurnalmembaca.

HBK World. "FMEA and Related Analyses." Accessed May 27, 2024. https://www.hbkworld.com/en/knowledge/resource-center/articles/examining-risk-priority-numbers-in-fmea.

Jie Deng, Gareth Tyson, F. Cuadrado and S. Uhlig. "Internet Scale User-Generated Live Video Streaming: The Twitch Case." (2017): 60-71. https://doi.org/10.1007/978-3-319-54328-4_5.

Jindong Qin, Yang Xi and W. Pedrycz. "Failure mode and effects analysis (FMEA) for risk assessment based on interval type-2 fuzzy evidential reasoning method." Appl. Soft Comput., 89 (2020): 106134. https://doi.org/10.1016/j.asoc.2020.106134.

Mark R. Johnson and Jamie Woodcock. "'And Today's Top Donator is": How Live Streamers on Twitch.tv Monetize and Gamify Their Broadcasts." Social Media + Society, 5 (2019). https://doi.org/10.1177/2056305119881694.

Masroor, Mohammad Majid "Providing Security in Multiserver Authentication Scheme using Efficient Three Factor Encryption." Regular (2020). https://doi.org/10.35940/ijrte.a2877.079220.

Nainggolan, Blandina Angelina, Lusi Mei, and Cahya Wulandari. 2021. "Operational Risk Analysis Using The Fmea Method In CV. GAMARENDS MARINE SUPPLY SURABAYA."

Rahmadi, Yobel Budining, and Heidy Arviani. "Analysis of Generation Z's Audience Reception of Verbal Violence on Masalohehe Twitch Channel." Vol. 7, 2024. http://Jiip.stkipyapisdompu.ac.id.

Ryhan1, Azel, and D Nawolo Baskoro2. "Motivation of Livestream Viewers on the Twitch App" 4, no. 2 (2021). http://jayapanguspress.penerbit.org/index.php/ganaya.

Saputra, Reynaldi, Deri Teguh Santoso, and others. "Failure Analysis of Plastic Production Process on Cutting Machines at Pt. FKP with Failure Mode and Effect Analysis Approach and Pareto Diagram." Barometer 6, no. 1 (2021): 322–27.

Sucofindo. "ISO 27001 - Information Security Management System (SMKI)," July 13, 2023. https://www.sucofindo.co.id/layanan-jasa/iso-27001-2/.

The Gurus. "Cybersecurity Experts Discuss the Twitch Data Breach - IT Security Guru." IT Security Guru - The Site for our Community, October 8, 2021. https://www.itsecurityguru.org/2021/10/08/cybersecurity-experts-discuss-the-twitch-data-breach/.

Yucheng Dong, Siqi Wu, Xiaoping Shi, Yao Li and F. Chiclana. "Clustering method with axiomatization to support failure mode and effect analysis." IISE Transactions, 55 (2022): 657 - 671. https://doi.org/10.1080/24725854.2022.2068812.