

DOI: https://doi.org/10.48009/2_iis_2026_123

Governance for gaming cybersecurity: A case study of Nintendo

Wenli Wang, *Robert Morris University*, wangw@rmu.edu

Michael Guida, *Robert Morris University*, mvgst304@mail.rmu.edu

Paul Kovacs, *Robert Morris University*, kovacs@rmu.edu

Abstract

The video gaming industry is booming — and so are cyberattacks against it, from credential stuffing and DDoS to large-scale data and source-code leaks. Yet cybersecurity governance in gaming remains understudied relative to other sectors. This paper addresses that gap through a qualitative single-case study of Nintendo, analyzing its documented security incidents and its responses from 2018 to 2026 — including the Gigaleak, the 2020 account breaches, the ENLBufferPwn vulnerability, the Teraleak, and the 2026 roadmap leak. This research proposes to Nintendo the applications of the governance frameworks from the National Institute of Standards and Technology (NIST) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Specifically, it demonstrates how Nintendo can benefit from NIST CSF (Cybersecurity Framework) 2.0, NIST SSDF (Secure Software Development Framework), and CISA best practices to surface governance gaps and recommend proactive controls. The case study of Nintendo supports the proposition that NIST frameworks and CISA policies can strengthen systematic cybersecurity governance for the hacker-targeted video gaming industry, emphasizing prevention over reaction.

Keywords: gaming, cybersecurity, governance, NIST CSF 2.0, NIST SSDF, CISA

Introduction

The gaming industry is flourishing, and the reasons are apparent. As online gaming innovations proliferate and global players' involvement escalates, revenues continue to rise. Analysts project that the industry will exceed \$300 billion in yearly sales by 2028 (PricewaterhouseCoopers, 2024). However, the expansion of the gaming sector has also led to a surge in cybersecurity concerns. The gaming industry encounters substantial cybersecurity threats, including hacking, cheating, and piracy, which jeopardize revenue, reputation, and game development. High-profile incidents involving companies such as Sony, Activision Blizzard, and CD Projekt Red underscore the gravity of these threats (Ibrahim, 2024; Szatmáry, 2024).

The video gaming sector is a significant target for cyberattacks, with a 94% increase in web attacks against games from Q1 2023 to Q1 2024, and with the month of June 2024 surpassing the one billion attack threshold (Williams, 2024). The Asia-Pacific and Japan (APJ) region notably impacted these cyber threat figures, recording 186 billion Distributed Denial of Service (DDoS) attacks during January 2023 to June 2024. The APJ region dominates the gaming market in global revenue, producing USD \$85.8 billion in 2023, as it possesses a significant player base (i.e., 23% of its population) which profoundly influences the video gaming industry (Williams, 2024).

Researchers have examined numerous factors contributing to the rising incidence of cyber risks within the gaming industry (Zhao, 2018; Szatmáry, 2024). Gamers often place their trust in gaming software that requires sensitive personal information, allowing them to pay real money or cryptocurrency for in-game

products (Wallace, 2022). This sensitive information and data may serve as significant financial incentives for a threat actor. Malicious actors may engage with and disrupt gaming for users, potentially compromising the game and their networks. Although extensive research has been undertaken in other industries (Cobanoglu et al., 2021; Tariq, 2024), there is comparatively less understanding of the gaming industry. This paper aims to utilize a case study of the renowned gaming corporation Nintendo, to advocate for formal applications of the cybersecurity governance frameworks in the video gaming industry to enhance its cybersecurity measures, both proactively and in the aftermath of an attack.

The following research questions (RQs) are to be answered in this research:

RQ1: What governance frameworks and policies are suitable for enhancing the video gaming industry's cybersecurity?

RQ2: How to apply these cybersecurity frameworks and policies for the video gaming industry?

This research uses Nintendo as a case study because it is a leading global gaming company that has experienced multiple documented cybersecurity incidents. These incidents provide valuable insights into cybersecurity governance challenges and responses that are relevant to the broader gaming industry. There already exists an emerging consensus that using cybersecurity frameworks may lead to controls that mitigate and eradicate cybersecurity threats (Delgado et al., 2021), our research adds to that consensus with an in-depth case study of Nintendo.

We will describe and analyze Nintendo's security breaches in the period of 2018-2026. We will discuss how Nintendo has addressed their security issues and enhanced its security measures. Then we will recommend how Nintendo could apply formal governance frameworks and recommended best practices to further enhance its security posture, especially proactively.

Background

The video game industry faces threats from malicious cybersecurity actors. It has dealt with diverse intrusions, such as malicious payloads, malware, ransomware, DDoS, phishing, and leaks of personally identifiable information. Despite the industry's efforts, threats to the gaming industry are on the rise. Williams (2024) reported that the industry saw a significant increase in gaming-related cyberattacks in 2024, including bots, web attacks, and Distributed Denial of Service (DDoS). Relentless criminals probe for vulnerabilities on a daily – and often hourly – basis. Types of cyberattacks in the video game industry and their statistics are exemplified below:

1) Downloaders accounted for most threats, responsible for 93% of all attack attempts during Q2 2024 and Q1 2025 (Kaspersky, 2025). 64% of gamers are concerned about the security of their personal information within online games. Data through late 2025 showed a significant surge in cyber-attacks targeting the gaming community, confirming that phishing threats and security concerns are at an all-time high.

2) In-game currencies and virtual goods account for high volumes of cyberattacks. About 28% of gaming industry data breaches involve ransomware, largely driven by financial gains. In 2025, ransomware constitutes 27%-39% of total breaches, closely aligned with 28% average over the years. Credential stuffing is frequently utilized as the initial step in a highly coordinated ransomware attack.

3) Mobile games are 10 times more likely to be targeted by hackers compared to console games.

4) Gaming-related DDoS attacks increased by 48% in the first half of 2020, as the COVID pandemic led to increased online gaming activities. In 2020, the gaming industry suffered more than 240 million web application attacks, a 340% increase over 2019.

These statistics are quite alarming to gaming companies. Due to these growing threats, applying suitable governance frameworks and policies is crucial to protecting the gaming industry and enhancing its cybersecurity. This research aims to help improve the gaming industry's overall cybersecurity governance, as exemplified in the Nintendo case.

Cybersecurity governance includes both proactive and reactive measures. Proactive measures aim to reduce or prevent the possibility of cyber incidents before they occur through activities such as secure software development, risk assessment, employee training, multifactor authentication, and continuous monitoring. Reactive measures center on responding to and recovering from incidents after they occur, including incident response, containment, investigation, stakeholder communication, and system restoration. While both approaches are important, this study emphasizes proactive governance through NIST CSF 2.0, NIST SSDF, and CISA best practices because preventing cyber incidents is generally more effective and less costly than responding to them after a breach.

Methodology

This study employs a qualitative single-case study approach to examine cybersecurity governance in the video gaming industry through Nintendo. This research design is grounded in established case study methodology literature, including Yin (2018), which supports the use of case studies for in-depth examination of contemporary phenomena within real-world contexts. Nintendo was selected because it is a leading global gaming company, has experienced multiple documented cybersecurity incidents involving different attack types, and provides sufficient publicly available information for analysis.

This case study relies on secondary sources, including Nintendo statements, cybersecurity reports, academic literature, government guidance, and reputable technology news sources. Cybersecurity incidents were selected if they involved unauthorized access, data exposure, service disruption, software vulnerabilities, or significant operational and governance implications.

The analysis used qualitative content analysis and governance mapping. Each incident was examined in terms of the attack type, affected assets, organizational impact, Nintendo's response, and relevant governance controls. The incidents were then systematically mapped to NIST CSF 2.0, NIST SSDF, and CISA best practices to identify governance gaps and evaluate how these frameworks could strengthen cybersecurity governance.

Case Study – Nintendo Cybersecurity

The case study is about Nintendo and its security breaches during the period of 2018-2026. Nintendo is a name ingrained into gaming culture worldwide. Some of the Nintendo security breaches exemplified cyberattacks in the video gaming industry, and Nintendo's reactions were also typical in the industry.

Nintendo was founded in 1889 by Japanese creator Fusajiro Yamauchi. The Nintendo video game company we know today started much differently by initially designing colorfully illustrated playing cards known as Hanafuda. The colorful card game was successful in Japan, helping to establish Nintendo as a top gaming company. In 1970s, the company shifted its business towards developing electronic video game system and

distributed its first Color TV-game in 1977. The Nintendo Entertainment System debuted in Japan as the Famicom system in 1983 and two years later, in 1985, in the United States, forever changing the gaming industry. Nintendo has succeeded in the video game sector over the last forty years. According to Statista (2025), as of October 2025, Nintendo has sold 154.01 million units worldwide, including over 50 million in North America. The Nintendo corporation is responsible for iconic video game characters such as Super Mario, The Legend of Zelda, Donkey Kong, and Pokémon. The Nintendo Corporation continues to innovate consoles and games, create and establish iconic franchises, and create a legacy in the video gaming industry that has served millions of fans worldwide.

Nintendo has enjoyed many great successes in the video gaming industry, but like many corporations, it faces threats in the cybersecurity field. Nintendo has access to sensitive information regarding user accounts, personal information, sensitive data, intellectual properties, supply chain, firmware, in-game social networks, and industry trade secrets. And these assets are often the targets of cyber criminals.

The following describes more details of attack types and Nintendo's responses in 2018-2026.

2018-2020 Gigaleak

Nintendo has been one of the most frequent targets of large-scale information leaks within the video gaming industry, with incidents such as the Gigaleak exposing years of internal company data across multiple console generations, including early concepts, prototypes, and canceled projects. These recurring breaches have raised concerns about the company's security posture and its ability to safeguard proprietary information (Doolan, 2022).

Nintendo was the victim of a significant informational leak known as the Gigaleak, which occurred between 2018 and 2020. The incident began when large volumes of internal Nintendo data were anonymously posted on the website 4Chan. According to IGN Entertainment which has Gamer Network, the leaked information included gigabytes of files and documentation from internal Nintendo projects, spanning both SNES era and Nintendo 64 development materials. The leak also contained source code for major titles such as The Legend of Zelda: Ocarina of Time and Super Mario 64, along with information on previously unknown or canceled projects (Skrebels, 2020).

IGN also reported that the Gigaleak may have been linked to an earlier intrusion by Zammis Clark, a security researcher previously arrested for hacking Microsoft who subsequently accessed Nintendo's confidential game development servers while on bail. Clark's breach reportedly exposed code for unreleased games, and later leaks—including Pokémon related source code and the broader Gigaleak—have been attributed to this unauthorized access (Skrebels, 2020).

The company reported that it is addressing these threats through a comprehensive, multi layered strategy that includes physical and technical countermeasures, collaboration with external specialists, improvements to its internal information security systems, the establishment of formal information management policies, and ongoing employee training (Doolan, 2022).

The hack may be connected to the broader security failures Nintendo experienced in April 2020, which is discussed below.

2020 Data Breaches

In April 2020, Nintendo experienced a significant data breach that affected 160,000 accounts that lacked protection such as multi-factor authentication. The hackers gained access to data by using an account checker tool to identify vulnerable credentials. According to TechRepublic, SpyCloud reported that

attackers relied on a combination of crimeware and older breached data to identify and take over accounts with vulnerable logins as part of a credential stuffing campaign (Whitney, 2020).

After acquiring the data, threat actors could exploit user accounts without multi-factor authentication and steal the information required to facilitate additional unauthorized logins across Nintendo services. Nintendo officially released a statement confirming that attackers had been impersonating the Nintendo Network ID login process throughout early April 2020. According to the company, exposed data included users' nicknames, dates of birth, gender, country or region, and email addresses, while no payment information appeared to have been compromised (Moore Coyler, 2020).

Two months later in June 2020, more than 300,000 Nintendo accounts were compromised. Nintendo also warned users to change their passwords and usernames if cybercriminals could obtain their vital information. Nintendo also apologized for this cyber incident, proposed to users how to set up proper two-way authentication, and conducted an internal investigation.

2021-2022 Buffer Overflow and Hardware Vulnerability

Another Nintendo's cyber incident during 2021–2022 involved a critical vulnerability known as ENLBufferPwn discovered in the Nintendo Switch, Nintendo 3DS, and Wii U consoles. The exploit allowed attackers to steal user information, interfere with gameplay, and potentially gain direct access to the console.

The vulnerability received a 9.8/10 “critical” rating from the Common Vulnerability Scoring System. Initially identified in 2021 and reported to Nintendo, Nintendo spent much of 2022 quietly patching the issue across major titles such as Nintendo Switch Sports, Mario Kart 8, and the Splatoon series. First party games were particularly susceptible due to a C++ buffer overflow in the Network Library, which made them high value targets for exploitation (Sansom, 2023).

2024 Teraleak

In October 2024, a Discord user known as GameFreakOUT uploaded approximately one terabyte of internal Pokémon related material to a server titled FeakLeak. The volume and sensitivity of the leaked content led the community to refer to the incident as the “Teraleak.” The data included information on upcoming titles such as Pokémon Legends: Z-A, minutes from internal Pokémon Company meetings, concept art from the original 1997 anime, and source code for legacy titles including Pokémon HeartGold and SoulSilver. Because the breach originated from Game Freak's internal systems, it also exposed personal information belonging to employees.

Game Freak confirmed that data pertaining to more than 2,000 current and former staff members had been compromised in the August 2024 intrusion. Six months after the leak, Nintendo filed a request for a subpoena on April 18 in the U.S. District Court for the Northern District of California, seeking to compel Discord to provide identifying information for the user, including name, address, phone number, and email address. Although Nintendo issued DMCA (Digital Millennium Copyright Act) takedown notices at the time of the breach, much of the leaked materials remain accessible online (Thubron, 2025).

2025 Crimson Collective Nintendo Breach

In October 2025, Nintendo confirmed that external web servers had been tampered with following claims by the hacking group Crimson Collective. While no customer data, payment information, or internal development assets were accessed, the attackers were able to modify certain public-facing server components. Nintendo addressed this breach publicly by acknowledging that external servers hosting its websites were briefly targeted, denying that any sensitive internal systems or customer data were compromised, and clarifying that no development, business, or personal information had been leaked.

2026 Nintendo Roadmap Leak

More recently, a March 2026 Nintendo data internal roadmap leak marked one of the most extensive cybersecurity failures in the video gaming industry, exposing internal development roadmaps, hardware specifications, financial projections, and strategic communications. The leaked materials revealed Nintendo's software pipeline through 2027, including major franchise entries, new intellectual property, and expanded indie partnerships. The breach also exposed multiyear development timelines for the forthcoming Switch 2 console (i.e., next-generation hardware) and its exclusive titles (e.g., *Star Fox*, *Duskblooms*, *Zelda: Ocarina of Time*), highlighting significant performance upgrades, and a targeted Q3 2026 release window. Independent analysts verified the authenticity of the leaked materials, indicating that attackers gained unauthorized access to internal systems.

Nintendo bypassed addressing the leaked timelines, pivoting instead to direct reveal of leaked titles in summer 2026. It confirmed *Legend of Zelda: Ocarina of Time*, as well as the upgrade of Nintendo 64 classic to Nintendo Switch 2, validating some discussed details of the roadmap leak.

Overall, these cybersecurity incidents experienced by Nintendo in 2018-2026 highlight ongoing risks associated with persistent targeting of video gaming companies by threat actors, reinforcing the need for stronger governance and continuous monitoring (Ćemanović, 2025). The most recent 2026 Nintendo Roadmap Leak incident further disclosed critical governance failures in access control, credential management, and internal network segmentation, reinforcing the need for structured cybersecurity frameworks (Ramblings of a Gamer, 2026).

Results

RQ1: What governance frameworks and policies are suitable for enhancing the video gaming industry's cybersecurity?

We recommend three frameworks: NIST CSF 2.0 and the NIST Secure Software Development Framework (SSDF), and CISA for cybersecurity governance for Nintendo and the general video gaming industry.

NIST Frameworks

The National Institute of Standards and Technology (NIST) would be suitable for ensuring a proper framework. The NIST was founded on March 3, 1901, to help develop a proper measurement standard and technology in the United States. The NIST framework for cybersecurity was introduced in 2014 to help companies manage and mitigate risks to growing cyber threats. NIST (2024) states that "The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risks and protect their networks and data. The framework is designed for voluntary application regarding the company's requirements. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection." NIST cybersecurity frameworks can be incorporated as an approach to the video gaming industry's cybersecurity issue, exemplified in Nintendo. NIST CSF 2.0 and NIST SSDF frameworks are particularly applicable.

NIST CSF 2.0 Framework

All the iterations of the NIST CSFs are consistent in their process-based approach. They categorize the framework into five key areas, often called the "NIST Cybersecurity Framework Core." These five core

areas are designed to help reduce and manage cybersecurity risk. The five key areas are “identify, protect, detect, respond, and recover” (NIST, 2024).

NIST Cybersecurity Framework (CSF) 2.0 is the latest iteration of NIST CSF and was published in 2024 (NIST, 2024). It focuses on helping companies reduce and manage cybersecurity risks by introducing new updates and expanded guidance on emerging threats and framework applicability.

NIST 2.0 emphasizes a great response to third-party risk and relies on governance to help integrate cybersecurity to assist with a greater focus on risk management strategies. The Framework Core is a functional tool to help a company with risk management, compliance, security posture updates, governance, supply chain risk management, and strong communication between teams on the dangers of cybersecurity risks.

Due to its robust features, companies in the video game industry could benefit from the application and framework of the updated NIST CSF 2.0. These features help a company by providing guidance on identifying, protecting, detecting, responding to, and recovering from cybersecurity attacks. These proactive and reactive approaches can help a company strengthen its cybersecurity posture, protect private information, and help build trust with users and stakeholders.

NIST SSDF Framework

The Secure Software Development Framework (SSDF), created by NIST in 2020, is a set of guidelines and best practices for integrating security into software development. SSDF helps developers secure their software and vulnerabilities through key components using best practices, security controls, integration with existing standards, and risk management. By following these concepts, a company can help achieve a stronger software security posture from cyber threats.

NIST SSDF provides a strong coding practice that can help ensure a strong security framework when developing game code. SSDF allows software developers and coders to allow proper dynamic testing, static code analysis, and help with security reviews. A strong focus on vulnerability assessment helps developers identify vulnerabilities during the testing phase and when software is released. SSDF can help with patching new updates safely, communicating with users of any cyber breaches, and preventing future software compromises.

CISA Best Practices

Cybersecurity and Infrastructure Security Agency (CISA) was established in 2018 by the United States Department of Homeland Security (DHS) to help protect the United States’ cybersecurity and infrastructure from threat actors. CISA can help provide cybersecurity protection, an incident response plan, collaboration with government agencies, and help provide critical infrastructure protection.

In addition to the secure software development strategies and policies stated in NIST SSDF, CISA recommends self-attestation as one of the best practices for secure software development.

For industry, CISA can provide its corporations with resources, tools, and guidance to ensure a stronger cybersecurity posture. This can be a useful framework to establish government collaboration, share threat information, guide the protection of assets, assist in an incident response plan, and offer training programs and educational resources.

RQ2: How to apply these cybersecurity frameworks and policies for the video gaming industry?

Applying NIST CSF 2.0

The NIST CSF2.0 can help gaming companies like Nintendo. By aligning with the NIST CSF 2.0 framework, Nintendo can strengthen its cybersecurity governance, serving as an example in the video gaming industry.

The five core functions and their respective subfunctions (see Table 1), proposed in NIST CSF 2.0, provide a comprehensive framework to help businesses enhance their security measures, achieve security resilience and awareness, safeguard critical assets and sensitive information. It is unclear whether Nintendo implemented NIST CSF 2.0 into its cybersecurity internally. Nevertheless, we suggested Nintendo actions that map to each subfunction of the five core functions (see Table 1).

NIST CSF 2.0 framework can help Nintendo to navigate the growing threat of cybercrime related to the video gaming industry by giving the tools to better identify, assess, and mitigate vulnerabilities. Application of NIST CSF 2.0 can mitigate Nintendo cyber risks, especially those related to its assets management and risk management. Suggested actions in *Respond* and *Recover* core functions are also relevant to Nintendo's response and recovery of its Gigaleak and Teraleak incidents. This rapid response can help Nintendo minimize any potential damages of security breaches as well as managing customer perception. The framework's proactive strategies in asset and risk management, incident detection and monitoring as well as testing also assists Nintendo in its prevention and adaptation to any emerging threats.

Table 1. Applying NIST Cybersecurity Framework 2.0 to Nintendo Cybersecurity Governance

NIST CSF 2.0 Core Functions	NIST CSF 2.0 Core Subfunctions	Suggested Nintendo Actions
1. Identify	1.1 Asset management	Nintendo should develop a comprehensive inventory of its hardware, software, and data assets, encompassing gaming consoles, user information, and online services.
	1.2 Risk management	Nintendo should conduct regular risk assessments to proactively identify vulnerabilities and potential threats to its systems and data.
	1.3 Governance	Nintendo should establish clear policies and procedures for cybersecurity governance, outlining roles and responsibilities for managing cybersecurity risks, are important.
2. Protect	2.1 Access Control	Nintendo must implement strict access controls to ensure that only authorized personnel can access sensitive systems and data.
	2.2 Security	Nintendo should encrypt sensitive data and establish secure coding practices to protect against vulnerabilities in game development.
	2.3 Training and awareness	Nintendo, being a large company, needs to provide regular training for employees to be aware of any potential threats the company might face.
3. Detect	3.1 Incident detection	Nintendo should establish security to detect early incidents, such as intrusion detection systems and security audits.
	3.2 Monitoring	Nintendo should hire cybersecurity experts must continue to detect and monitor any threats. Tools to detect these types of anomalies should be used across all systems and networks.
4. Respond	4.1 Collaboration	Nintendo should have a strong communication connection with law enforcement, law officials, and cyber security experts to help enhance response times and capabilities.
	4.2 Incident response plan	Nintendo must develop and maintain a strong incident response plan that outlines steps and procedures for handling security incidents.
	4.3 Testing	Nintendo should have regular training exercises to test the effectiveness of its overall response plan.

5. Recover	5.1 Communication	Nintendo should create a communication channel to inform stakeholders, users, and partners about the recovery effort after an incident.
	5.2 Improvement	Nintendo should, after experiencing a cyber security breach, conduct a post-review and analyze the response areas and how to improve the process and technology.
	5.3 Recovery Planning	Nintendo should create a recovery plan outlining steps to help restore operations, including data backups.

Applying NIST SSDF

The SSDF is a crucial framework for Nintendo due to the many threats it faces when protecting its assets, intellectual properties, user data, and its overall integrity. Table 2 shows the four main NIST SSDF activities and suggested Nintendo actions according to these CISA best practices.

The application of NIST SSDF is especially important to mitigate Nintendo's risks related to its source code issues such as buffer overflow. Nintendo had a buffer overflow vulnerability referred to as ENLBufferPwn in many of its first-party games for the Nintendo 3DS, Switch, and Wii U. NIST SSDF framework would help because of its structured security throughout the software design and development cycle to prevent exploits such as buffer overflow. It is important for any new development to understand and detect where previous buffer overflow attacks occurred and what steps were taken to eliminate any vulnerabilities. NIST SSDF also ensures that developers implement measures such as input validation and bound checking so buffers do not exceed their intended allocated size. Nintendo heavily uses C and C++, especially for the Nintendo Switch. These two computer languages have been known to be susceptible to buffer overflow attacks. NIST SSDF urges developers to use modern programming languages to help reduce vulnerabilities to buffer overflow as these newer languages may even have automatic memory and safe libraries.

Table 2 Applying NIST Secure Software Development Framework to Nintendo Cybersecurity Governance

NIST SSDF Activities	Suggested Nintendo Actions
Prepare the Organization (PO)	Nintendo should establish a secure framework for software development. It should prepare to start performing secure software development across the organization, from staff to technology. It should set policies, conduct training exercises, conduct ongoing training with personnel, and implement tools.
Protect the Software (PS)	Nintendo should ensure the integrity and security of the software. It should ensure that codes, technologies, and environments are protected from threats from environmental factors or cyber threats. It should also allow developers to protect sensitive information and maintain secure coding practices.
Produce Well Secured Software (PW)	Nintendo's teams of developers should minimize security vulnerabilities in the software upon release. It should emphasize that the software be tested and any vulnerabilities found in the software be fixed before the software is released to the public.
Respond to Vulnerabilities (RV)	Nintendo developers should take a proactive method for helping identify, analyze, and mitigate software vulnerabilities after the software is released to the public throughout its life cycle.

Other researchers and/or research groups have suggested similar or supplementary activities as those in NIST SSDF. Williams (2024) stated that video game developers should understand the importance of including cybersecurity considerations when designing, developing, and maintaining games to ensure data is kept safe and the game continues functioning as expected. It recommended strategies for strong cybersecurity in the video game industry, such as building security into the game development process, monitoring games in production, securing authentication methods, securing infrastructure, running security exercises, and engaging users.

The Cyber Management Alliance also had some further recommendations for companies in the video gaming industry on how to strengthen their overall cybersecurity measures. The website states that a company should secure software development lifecycle, employee cybersecurity training and awareness, third-party risk management, game client-server security, incident response, and business continuity. Implementing these security measures must be an ongoing effort to stop cyber threats. Companies implementing these security measures can enhance their overall security, continue to grow brand loyalty, and ensure consumer trust.

Applying CISA Best Practices

Table 3 shows suggested CISA best practices for Nintendo to adopt. The application of CISA best practices is essential to mitigate Nintendo's risks such as user account data breaches.

Table 3. Applying CISA Best Practices to Nintendo Cybersecurity Governance

CISA Best Practices	Suggested Nintendo Actions
Use strong passwords	Strong passwords can help prevent threat actors from easily infiltrating gaming server. It is important to for Nintendo users to follow guidelines using CISA suggestions for making the password long, appearing random, and unique.
Implement Multifactor Authentication (MFA)	Multi-Factor Authentication (MFA) requires users to set up two or even more verification steps to ensure a layered approach to security. Nintendo's adopting MFA provides a layered approach, making user access information harder for threat actors.
Regularly update firmware and software	Regular updates to the firmware and software help keep Nintendo systems up to date, allowing stronger protection from vulnerabilities and threat actors.
User education and training	An important strategy to keep users protected is to make all Nintendo personnel and staff aware of the dangers of cyber threats and to have ongoing training and exercises to continue to learn and understand the awareness of threats and safe practices.
Utilize encryption	Nintendo should apply encryption to ensure that information and data are converted to code to prevent unauthorized access by threat actors. Only authorized users can obtain this information with the proper decryption key.
Back up data	Nintendo should back up data as crucial to strong security measures. This allows crucial data to be restored in the event of data loss due to multiple factors, including cyberattacks and accidental data loss.
Engage in collaboration and information sharing	Information sharing is an important step in helping Nintendo understand threats, vulnerabilities, and previous incidents. This information can help Nintendo learn from its prior incidents and better responses to threats in the future.
Segment the network	When Nintendo divides the network into smaller and isolated segments, it helps limit access to secure information. This allows Nintendo to contain a threat within a specific segment, preventing the threat from spreading to the entire network.

As suggested, Nintendo did implement multi-factor authentication for its users after data breaches. In addition, Nintendo asked its users not to reuse their NNID password when creating new accounts after data breaches. Nintendo also practiced better network segmentation after its web incident.

Discussion

Nintendo must continue to enhance and improve its security measures with governance as cybersecurity must remain a constant priority. The strategic areas where Nintendo can investigate and strengthen are regular risk management, timely employee training and awareness, advanced technology adoption, incident response planning, collaborative information sharing, third-party risk management, and regular policy

reviews and updates. Some of them overlap with NIST CSF 2.0 and SSDF governance frameworks and CISA best practices.

For instance, Nintendo's user information and intellectual property are crucial assets that need protection. Risk management identifies, assesses, and prioritizes potential risks that could negatively impact an organizational asset. Risk management involves steps to help minimize the likelihood of risks occurring and reduce their potential impact. Nintendo needs to manage these risks with physical and digital countermeasures. These initiatives can help bolster Nintendo cybersecurity defense, protect its digital assets, and contain data leaks.

This January 2026, Nintendo released a statement on its main website which publicly reaffirmed its commitment to player safety. The company emphasized that safeguarding online play requires a multidisciplinary strategy that integrates advanced technology, research driven insights, community support, and skilled human oversight. Nintendo noted that these efforts are strengthened through collaboration, stating that meaningful progress is achieved when industry partners work toward shared goals. As part of this ongoing initiative, the company continues to invest in, adapt, and expand its approaches to user safety, with particular attention to protecting the most vulnerable players (Nintendo, 2026). Nintendo now allows users to report unsafe activities, including cyber threats, to its own main website. This is an excellent initiative to keep communicating with player user base to both detect vulnerabilities earlier and enhance user trust.

As indicated above, Nintendo's statements regarding cybersecurity show a proactive approach to protecting its users. This can help users feel that Nintendo takes their security and safety seriously. This allows users to continue to build trust with Nintendo and keeps the company resilient in keeping up with the changing threats in the cyber community.

This paper's focus on the Nintendo case study only exemplifies how companies in the video gaming industry had to deal with threat actors and threats over the years. As suggested cybersecurity governance for Nintendo, the video game industry altogether must take a proactive approach to ensure cybersecurity governance and compliance to ensure sufficient countermeasures against the continuous rising of threats and cyberattacks.

This may include innovative methods. For instance, blockchain may help video game industry cybersecurity with decentralized servers and encryption (Rishiwal et al., 2024). The video gaming industry uses often centralized platforms, which make the digital assets on centralized servers focal targets of cyber threat actors (Rishiwal et al., 2024). A decentralized server would allow users to have their information stored and processed across multiple servers, making it more difficult for a threat actor to attack a single source. Rishiwal et al. (2024) further suggested how decentralized blockchain technology can help solve the problem of centralization. Blockchain can provide better protection from fraud by using decentralized technology to encrypt players' personal information and in-game assets. As a result, it gives users greater control over their assets, allowing users ownership and providing extra layers of security. This architectural change also increases reliability to players - in case one node is compromised or fails, other nodes can still operate with continuing service and security.

Conclusion

The cybersecurity challenges faced by the video gaming industry continue to increase as threat actors evolve their techniques and increase their targeting of high value intellectual property, development infrastructure,

user data and their digital assets. Nintendo's breaches from the 2018-2020 Gigaleak, large scale data breach in 2020, Teraleak in 2024, server tampering in 2025, and the most recent 2026 roadmap leak reveal that even an industry leader remains vulnerable to persistent and increasingly sophisticated attacks. These incidents reveal systemic weaknesses in access control, cloud governance, supply chain security, and internal segmentation, all of which are critical domains that could be addressed by modern cybersecurity governance frameworks.

Applying the NIST CSF 2.0 and NIST SSDF (Secure Software Development Framework) as well as CISA best practices such as self-attestation for secure software development is crucial to both proactively and reactively protect against cyberattacks for the video gaming industry. Cybersecurity strategy must represent a forward-thinking approach to risk management. The secure software development policies and practices are necessities for reducing risks proactively. The suggested frameworks and best practices serve as strong guidelines for gaming corporations like Nintendo and contribute to the entire video gaming industry overall. The NIST frameworks are not just tools for compliance but can be a vital component for strategic planning, risk management, and keeping corporations secure in the digital age (Szatmáry, 2024). The goal for the gaming corporations is to continue providing a safe and enjoyable environment for the gamers. By prioritizing cybersecurity governance like the NIST frameworks and CISA best practices, the video gaming industry can continue innovating in its products and services and at the same time provide security and privacy for its adoring gaming fans.

The paper's main contribution is showing how NIST CSF 2.0, NIST SSDF, and CISA best practices can be applied to address cybersecurity incidents in Nintendo to exemplify common governance gaps in the video gaming industry. While this study focuses on a large, leading gaming corporation, future research could examine how cybersecurity governance frameworks may be adapted for smaller gaming companies and independent studios with limited resources.

References

- Cobanoglu, C., Dogan, S., Nanu, L., Fragniere, E., & Yagci, K. (2021). Hospitality and Tourism Information technology. In *USF M3 Publishing, LLC eBooks*.
<https://doi.org/10.5038/9781732127593>
- Cyber Management Alliance. 2024. "How game development companies can strengthen cybersecurity measures", Retrieved on 05/09/2026 from <https://www.cm-alliance.com/cybersecurity-blog/how-game-development-companies-can-strengthen-cybersecurity-measures>
- CISA. (n.d.) *Cybersecurity & Infrastructure Security Agency*. <https://www.cisa.gov/>
- Ćemanović, A. 2025. "Nintendo admits server tampering incident, denies data breach", Retrieved on 05/09/2026 from <https://cyberinsider.com/nintendo-admits-server-tampering-incident-denies-data-breach/>
- Delgado, M. F., Esenarro, D., Regalado, F. F. J., & Reátegui, M. D. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3C TIC Cuadernos De Desarrollo Aplicados a Las TIC*, 10(2), 123–141. <https://doi.org/10.17993/3ctic.2021.102.123-141>

- Doolan, L. 2022. “*Shuntaro Furukawa reveals what Nintendo is doing to combat info leaks and security threats*”, Retrieved on 05/09/2026 from <https://www.nintendolife.com/news/2022/07/shuntaro-furukawa-reveals-what-nintendo-is-doing-to-combat-info-leaks-and-security-threats>
- Federal Trade Commission. (n.d.). NIST cybersecurity framework. <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework>
- Ibrahim, A. (2024). Guarding the future of Gaming: The imperative of Cybersecurity. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 1–9. <https://doi.org/10.1109/iccr61006.2024.10532843>
- Kaspersky. 2025. “*Press ‘Play’, stay alert: How cybercriminals exploit the popularity of Gen Z’s favorite games*”, Retrieved on 05/09/2026 from <https://www.kaspersky.com/blog/gen-z-gaming-report-2025/>
- Moore-Coyler, R. 2020. “*Cybercriminals managed to breach thousands upon thousands of Nintendo accounts and make illegal purchases*”, Retrieved on 05/09/2026 from <https://www.tomsguide.com/news/nintendo-switch-breach-exposes-160000-users-what-to-do-now>
- Nintendo.(n.d.). Governance and compliance. <https://www.nintendo.co.jp/csr/en-us/report/governance/index.html>
- Nintendo. 2026. “*An update to our shared commitment to safer gaming*”, Retrieved on 05/09/2026 from <https://www.nintendo.com/us/whatsnew/an-update-to-our-shared-commitment-to-safer-gaming/>
- NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. *National Institute of Standards and Technology*. <https://www.nist.gov/cyberframework>
- PricewaterhouseCoopers. 2024. “*Perspectives: global entertainment & media outlook 2024–2028*”, Retrieved May 18, 2025, from <https://www.pwc.com/gx/en/issues/business-model-reinvention/outlook/insights-and-perspectives.html>
- Ramblings of a Gamer. 2026. “*Nintendo leak: What gamers need to know about the 2026 revelations*”, Retrieved on 05/09/2026 from <https://ramblingsofagamer.com/nintendo-leak-what-gamers-need-to-know-about-the-2026-revelations/>
- Rishiwal, V., Agarwal, U., Yadav, M., & Alotaibi, A. (2024). Blockchain-secure gaming environments: A Comprehensive Survey. *IEEE Access*, 12. DOI: [10.1109/ACCESS.2024.3510467](https://doi.org/10.1109/ACCESS.2024.3510467)
- Sansom, A. 2023. “*First-party switch and 3DS games could have compromised your security*”, Retrieved on 05/09/2026 from <https://www.tomsguide.com/news/nintendo-switch-severe->

[vulnerability-patched-what-you-need-to-know](#)

- Skrebels, J. 2020. “*Nintendo Gigaleak: Everything we know and all the major discoveries*”, Retrieved on 05/09/2026 from <https://www.ign.com/articles/nintendo-gigaleak-everything-we-know-and-all-the-major-discoveries>
- Statista. 2025. “*Nintendo Entertainment System (NES) lifetime unit sales worldwide as of October 2025, by Region*”, Retrieved on 05/09/2026 from <https://www.statista.com/statistics/1101896/unit-sales-nes-region/>
- Szatmáry, K. S. (2024). Cybersecurity of the gaming industry. In *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)* (pp. 000441–000446). <https://doi.org/10.1109/sisy62279.2024.10737510>
- Tariq, M. U. (2024). Cybersecurity risk assessment models and theories in the travel and tourism industry. In *Advances in hospitality, tourism and the services industry (AHTSI) book series* (pp. 1–17). <https://doi.org/10.4018/979-8-3693-2715-9.ch001>
- Thubron, R. 2025. “*Nintendo files DMCA subpoena ordering Discord to identify ‘Teraleak’ Pokémon leaker*”, Retrieved on 05/09/2026 from <https://www.techspot.com/news/103595-nintendo-files-dmca-subpoena-discord-identify-teraleak-pokemon.html>
- Wallace, J. 2022. “*Gaming industry: The need for cybersecurity (protocols)*”, Retrieved 05/09/2026 from <https://cologix.com/blog/gaming-need-cyber-security/>
- Whitney, L. 2020. “*Nintendo data breach reportedly caused by credential stuffing*”, Retrieved on 05/09/2026 from <https://www.techrepublic.com/article/nintendo-data-breach-reportedly-caused-by-credential-stuffing/>
- Williams, S. 2024. “*Cyber threats surge in gaming industry through 2024*”, Retrieved 05/09/2026 from <https://securitybrief.co.uk/story/cyber-threats-surge-in-gaming-industry-through-2024>
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.
- Zhao, C. (2018). Cyber security issues in online games. *AIP Conference Proceedings*, 1955, 040015. <https://doi.org/10.1063/1.5033679>