Securing Next-Generation Broadcast Media Enterprises Against Cyberthreats

Media consumption patterns have significantly shifted to hyperconnected and multiplatform media ecosystems, pushing media enterprises to adopt production and distribution strategies that reach diverse audiences. Broadcast media enterprises have developed a variety of Internet Protocol (IP)-based content delivery systems to build these new media ecosystems, but doing so also opened the door to increased threats at every stage of broadcasting, from media production to consumer experience.

Broadcast media enterprises' concerns about cybersecurity threats can be divided into two groups: corporate IT security issues, which are prevalent across all businesses (e.g., data centers, network applications); and broadcast media security challenges, which are specifically related to the organizations' core business activities.

It is critical to address the latter cybersecurity concern and understand how to develop a cyberresilience strategy to meet the challenges, especially during the broadcast of high-profile live events.

Cybersecurity Challenges for Broadcast Media Networks

Today's broadcast media organizations are operating in an environment of improved formats, changing platforms, better processor speeds and over-the-top (OTT) delivery, which enables media to be viewed on practically any device. These technological advancements have significantly impacted the media sector. There are countless business opportunities, but, at the same time, these changes come with cybersecurity challenges that broadcast media enterprises must address to compete. These challenges increase significantly during the live broadcast of high-profile events such as the Olympic Games or the International Federation of Association Football (FIFA) World Cup tournament, including avoiding or minimizing service downtime, protecting consumer data security and privacy and protecting intellectual property, notably copyrights.

There are several common cybersecurity challenges and threats faced by the broadcast media industry, including:

- **Distributed denial-of-service (DDoS) attacks**—One of the most frequent and widespread types of cyberattacks against media enterprises is DDoS attacks.[1] DDoS attacks typically place an undue demand on the vital infrastructure of media enterprises, which makes their services unavailable, resulting in both financial and

MUHAMMAD MALIK | PH.D, CISA, CISM, CISSP, CLP

Is an information security leader with more than 20 years of experience in enterprise security and consulting for public and private organizations. He focuses on enterprise security governance and strategies, information security frameworks, security architectures, security solution designing, and building and deploying managed security services. He also leads security consulting, risk assessment and policy development. Malik has led the development of several information security programs, working closely with executive leadership, chief information security officers (CISOs) and operational teams to transform their security programs. He has more than five years of experience heading the information security assurance department at a media group operating across five continents. He also serves as chief editor at *Information Security Buzz*. Malik can be reached at *https://www.linkedin.com/in/dr-muhammad-malik-45940a/*.

OTT platforms are also increasingly targeted by cyberattacks, particularly when users sign up for services and communicate with a payment gateway.

reputation loss. DDoS attacks frequently have an underlying economic or political context, and the risk of them occurring increases dramatically during live broadcasts of high-profile events.

- **Media platform vulnerabilities**—Media enterprises frequently make use of out-of-date software or fail to implement comprehensive authentication and verification methods, providing hackers with a wide range of attack vectors against their digital infrastructure. One study found that more than 50 percent of media organizations that offer content management systems have security flaws that can put them at risk.[2]
- **Connected devices**—Broadcasting a tournament live to millions of households requires the use of multiple connected devices and systems such as cameras, outside broadcasting (OB) vans and control rooms. But this results in an increase in attack surfaces and, thus, heightens the risk of cybersecurity attacks occurring.
- **Malware attacks**—Threat actors can inject a form of malware (e.g., viruses, worms, botnets, Trojans, spyware, adware) to jam the transmission network and steal confidential information.
- **Ransomware attacks**—One of the main goals of media enterprises is to control the timing of content distribution to the public. By managing the schedule of content releases, media enterprises can build up the audience's excitement. However, cybercriminals can disrupt the schedule of highly anticipated content by launching a ransomware attack to take control of systems containing intellectual property, prohibiting employees from accessing, releasing or even altering it. The average ransom payment amounts have nearly doubled since 2020.[3] Hence, it is no surprise that ransomware is the most significant type of cyberattack the broadcast media industry can be affected by.[4] Trends show that ransomware will remain a prominent advanced persistent threat (APT), especially as Ransomware-as-a-Service (RaaS) groups continue to operate with impunity.[5]
- **Cloud-based attacks**—In the broadcast media industry, cloud computing is becoming increasingly necessary as there is always a growing need for instant access to entertainment and places. As a result, broadcast media enterprises all over the world are moving to the cloud to ensure quick delivery of digital material. OTT streaming services, which distribute digital material directly to users over the Internet, are ultimately made possible with the help of the cloud. However, media enterprises need to be aware of the various types of cyberattacks that arise from adopting a cloud environment for broadcasting, such as cloud-based DDoS and cloud malware injection attacks. These cloud-based attacks against media broadcast enterprises are challenging to defend against because the scale and complexity of broadcast networks in the cloud environment can make it difficult to recognize and mitigate the attack.
- **Delay patching**—Broadcast vendors often deliver security vulnerability patches slowly. Even when patches are released, broadcast media enterprises do not always patch their systems within the industry-recommended time frame. Delays are often due to the system's critical need for availability during important content delivery times, such as major sporting events. One study found that 60 percent of vulnerable broadcasting systems have remained vulnerable up to six weeks after a patch was released.[6]
- **OTT platform security**—OTT platforms are increasingly popular media services, but they usually have a complicated architecture that contains custom code, third-party libraries and integration with third-party applications such as customer relationship management software and payment gateways. Due to their growing popularity and intricate design, OTT platforms are also increasingly targeted by cyberattacks, particularly when users sign up for services and communicate with a payment gateway.
- **Set-top box (STB) security**—The demand for media-rich home entertainment services has led to new ideas and business opportunities in the set-top box (STB) market. Next-generation STBs will integrate video content from multiple signal sources and allow content distribution to various viewing devices. However, this amount of source diversity and content portability makes content naturally more vulnerable to piracy and complicates security requirements. Hacker attacks, software security flaws and device tampering pose a constant threat

LOOKING FOR MORE?

- Explore the *Risk Scenarios Toolkit. www.isaca.org/risk-scenarios*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

to STBs, their associated conditional access (CA) systems and digital rights management (DRM) technologies. These threats can have a negative impact on the reputation and financial health of STB manufacturers and operators.

- **Pirated streaming**—Viewers sometimes go to extreme measures to gain access to high-profile events on television, such as pirated streaming. Although this is not a cybersecurity issue, cyberattackers take advantage of this and set up pirated streams and it can result in a loss of revenue for broadcast media enterprises. According to a report published in March 2021, sports piracy is costing the industry as much as USD$28.3 billion a year, showing the scope of the problem affecting broadcasters globally.[7]

Figure 1 illustrates the cybersecurity challenges from content production to consumer.

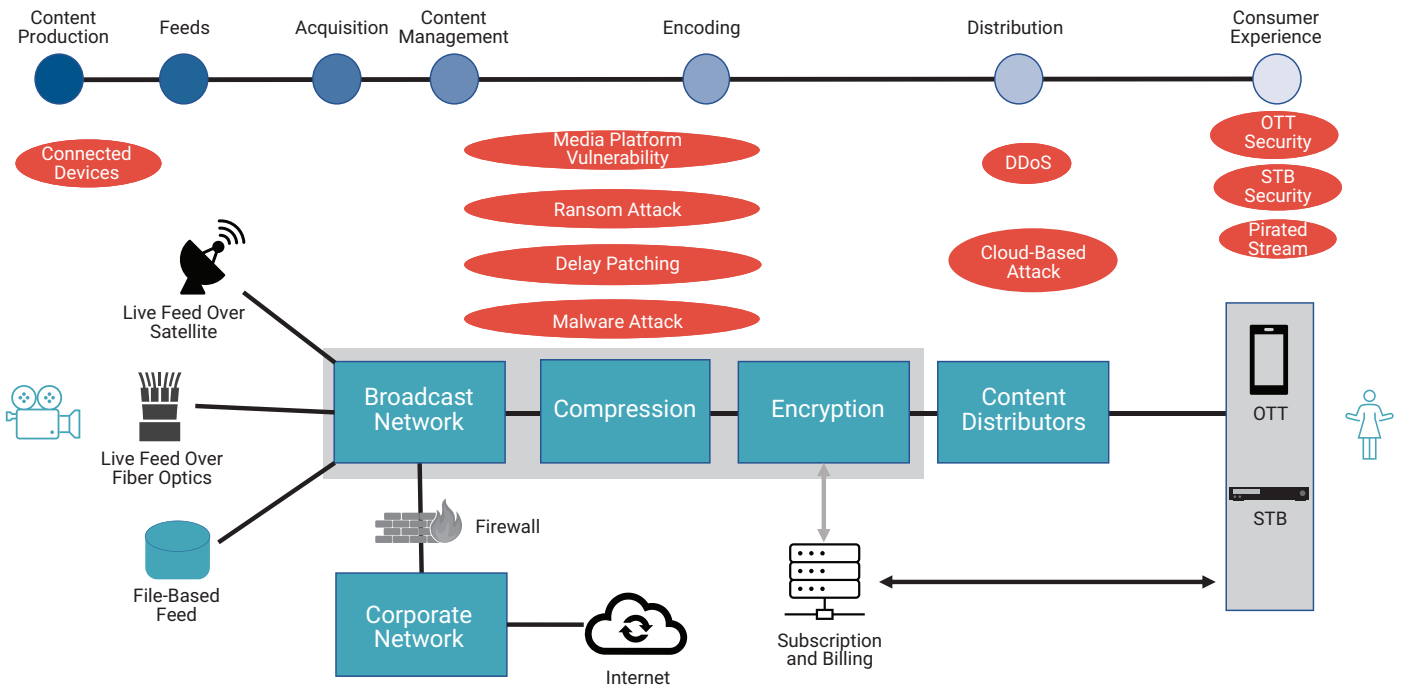
Why Cybersecurity Is a Growing Concern

High-profile sporting events have tremendous global viewership. Such events are prime targets because adversaries can target more victims than usual. Cybersecurity is a significant concern for the broadcast media industry because:

- A broadcast media network can experience considerable disruption and financial loss due to a breach or cyberattack. Moreover, if the attack stops the delivery of essential services and information, it can cause discomfort, uncertainty and even panic, especially during high-profile live events.
- For a broadcast media enterprise to keep a positive reputation and remain competitive, viewer trust is essential. A cyberattack or data breach could lead to customers losing faith in the network and the brand, which could ultimately reduce viewership and revenue.
- Even if a broadcast media enterprise has the exclusive rights to stream a specific event, cybersecurity problems could damage the network's reputation and cause it to be excluded from future events.
- A large volume of data, including the private information of staff members and viewers, financial data, and intellectual property, is gathered and stored by broadcast media enterprises. Cybersecurity measures help ensure that these data remain secure and protected from unauthorized access or theft.

FIGURE 1

Cybersecurity Challenges During Media Content Delivery



- Broadcast media enterprises typically use social media to connect with their audience, share content and promote their brand. According to Deloitte's digital media trends survey, 60 percent of respondents attributed cyberattacks on media organizations to social media platforms, suggesting the protection of social media accounts is vital for media enterprises.[8]

To protect sensitive data, ensure operational continuity, build viewer trust, thwart hacking and abide by legal obligations, broadcast media enterprises must prioritize cybersecurity.

Cyberresilience Strategy

Having a robust cyberresilience strategy for broadcast media enterprises is essential. The overall objectives of a cyberresilience strategy are to:

- Enable the enterprise's business strategy of hyperconnected and multiplatform media ecosystems.
- Reduce risk to within appetite.
- Increase information security capability for the media-specific systems, devices and broadcast networks to respond to emerging threats.

Having a robust cyberresilience strategy for broadcast media enterprises is not just about reducing cyberrisk but also driving value to the business. The cyberresilience strategy should be implemented at each broadcasting stage—acquisition, production, distribution and consumer experience. As shown in **figure 2**, to define the strategy, the enterprise must understand its current state of cyberresilience in relation to its business objectives. To do so, it can assess threat risk and measure cyberresilience capability maturity level against the relevant security framework. Next, the target state is defined in relation to business initiatives, desired cyberresilience capability maturity level and defined risk target. A gap analysis between the current and target states is conducted to define the roadmap of cyberresilience initiatives, including prioritization of initiatives and allocation of budget.

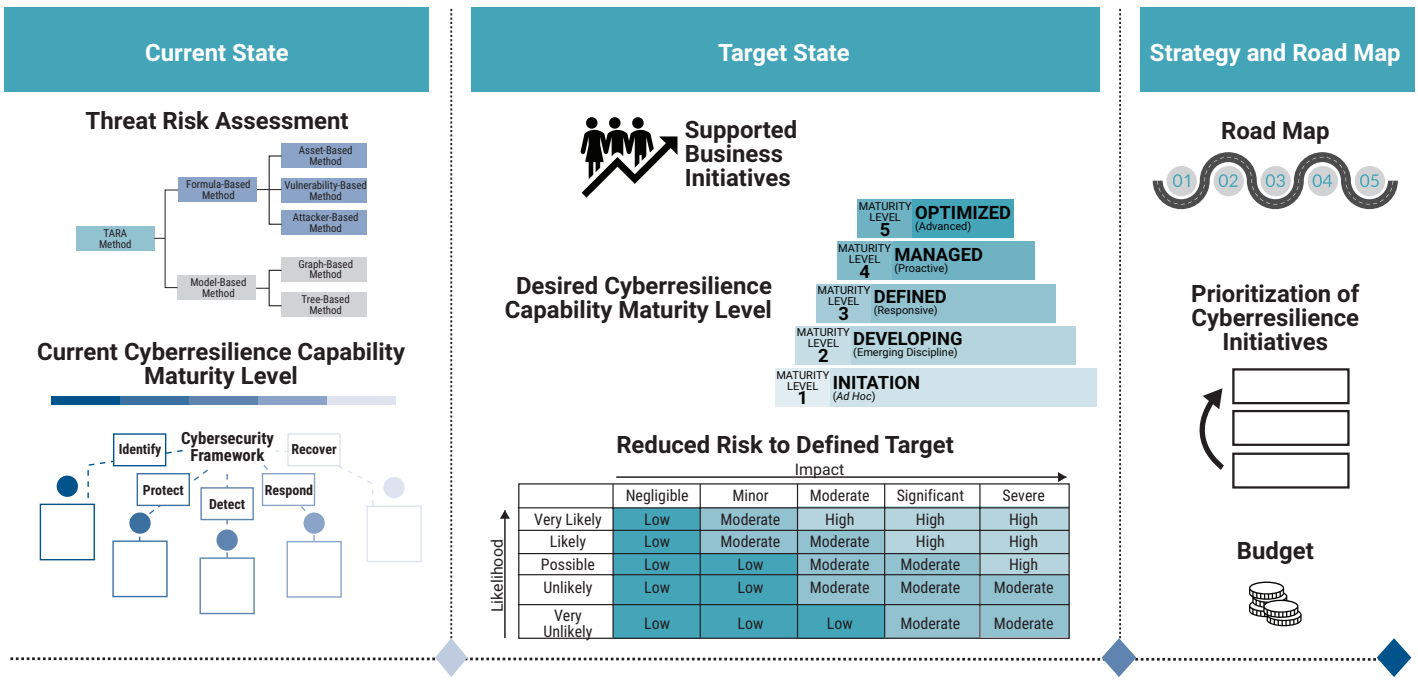
Efficient cyberthreat assessment, sharp cyberrisk profiling and robust security initiatives and safeguards are required to maintain an effective cyberresilience strategy.

Cyberthreat Assessment

A cyberthreat assessment formally evaluates the degree of severity and nature of a threat to an information system. As there are many different types of cybersecurity threats to broadcast media enterprises, it is important to understand how to identify the relevant threats and prevent them before they develop into full-

FIGURE 2

Cyberresilience Strategy Approach



fledged attacks. Completing a cyberthreat assessment and measuring the organization's cybersecurity capability maturity level can be aided by security frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and International Organization for Standardization (ISO) 27001. These steps help broadcast media enterprises better understand the current state of their cybersecurity maturity.

Figure 3 shows an example of a cyberthreat assessment that can be adopted to capture relevant threat levels for an enterprise. The assessment defines the main threat actors targeting the media industry with motivation. The assessment also shows the relevant threat level and recent examples of cyberattacks on media enterprises by corresponding threat actors.

Cyberrisk Profiling

A risk profile is a quantitative analysis or risk calculation of the various types of threats an enterprise or its assets face. Cyberrisk profiling is crucial because it can help clarify how threats affect a media establishment's operations.

Media and Types of Cyberrisk

Based on the threat assessment, **figure 4** depicts the top risk to broadcast media enterprises when broadcasting high-profile live events and subsequent security controls (strategic initiatives) to prevent, detect, respond to or recover from such risk scenarios.

Nonnegotiable Cyber Controls

There are several controls that the media and broadcasting industry can adopt to address cyberthreats.

Nonnegotiable cyber controls (NCCs), if designed, implemented, and operated effectively, can significantly reduce the risk profile for a broadcast media enterprise. **Figure 5** gives examples, but they are not all-encompassing. There is no single security solution to deter adversaries, as each list depends on an organization's risk appetite.

Cyberresilience Strategy Road Map

The first and foremost step in achieving cyberresilience is to develop solid security foundation capabilities covering end-to-end broadcasting stages,

FIGURE 3

Cyberthreat Assessment

Threat Actor	Motivation	Threat Level	Cyberattack Examples
State-sponsored actors	• Espionage • Theft of information and intellectual property • Cyberpropaganda • Disruption or sabotage	Very high	• TV5 Monde attack in 2015[a] • Cyberattack on Australian media enterprise Nine[b] • There has been a 100 percent rise in nation-state attacks in the past three years.[c]
Cybercriminals	• Financial fraud • Extortion • Identity theft	Very high	• Many Cox Media stations had broadcasting interruptions in June 2021 as a result of a ransomware attack.[d] • Ransomware attack on Madsack Media Group in Germany[e] • In 2018, video piracy cost the US economy US$29.2 billion in lost revenue.[f] Online media piracy reportedly increased significantly in 2022.[g]
Activist groups	• Publicity for a cause	Moderate	• Breach of far-right social media platform Gab[h]
Disgruntled or malicious insiders	• Emotionally, financially or politically based	High	• The *New York Post* website was hacked by one of its own staff members.[i]

Sources: a) Corera, G.; "How France's TV5 Was Almost Destroyed by 'Russian Hackers,'" BBC, 10 October 2016, *https://www.bbc.com/news/technology-37590375*; b) 9News, "Nine Network Under Attack by Cyber Hackers, Threatening New Services Nationwide," 29 March 2021, *https://www.9news.com.au/national/nine-network-hit-by-cyber-attack-threatening-news-services-nationwide/c653fe12-a5c4-4da8-9a33-b902f1325eed*; c) University of Surrey, Guilford, England, "New Academic Study Highlights 100 Percent Rise in Nation-State Attacks in the Last Three Years," 14 April 2021, *https://www.surrey.ac.uk/news/new-academic-study-highlights-100-cent-rise-nation-state-attacks-last-three-years*; d) Tapper, J.; E. Perez; R. Young; "Cox Media Group Hit by Cyberattack Last Week, Sources Familiar Tell CNN," CNN Politics, 9 June 2021, *https://edition.cnn.com/2021/06/09/politics/cox-media-group-cyberattack/index.html*; e) Kannenberg, A.; "Suspicion of Ransomware: 'Cyber Attack' on the Madsack Publishing Group," Heise Online, 23 April 2021, *https://www.heise.de/news/Verdacht-auf-Ransomware-Cyberangriff-auf-die-Verlagsgruppe-Madsack-6026905.html*; f) Blackburn, D.; J. Eisenach; D. Harrison Jr.; *Impacts of Digital Video Piracy on the U.S. Economy*, NERA Economic Consulting, Global Innovation Policy Center and US Chamber of Commerce, June 2019, *https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf*; g) Gose, L.; "Piracy Rates Grow as Streamers Raise Prices and Cut Content," Comic Book Resources, 14 February 2023, *https://www.cbr.com/piracy-streamers-rise-2022-prices-raise/*; h) Greenberg, A.; "Far-Right Platform Gab Has Been Hacked—Including Private Data," *Wired*, 28 February 2021, *https://www.wired.com/story/gab-hack-data-breach-ddosecrets/*; i) *Dark Reading*, "NY Post Falls Victim to Insider Threat," 27 October 2022, *https://www.darkreading.com/attacks-breaches/ny-post-falls-victim-to-insider-threat*

FIGURE 4

Cyberrisk Affecting High-Profile Events

Cyberrisk Scenarios	Key Risk Drivers	Business Impacts	Strategic Initiatives (Security Controls)
Broadcast network disruption	• Inherent security issues with broadcast products • Low maturity of nonnegotiable cyber controls (NCCs) on the broadcast network • Lack of business continuity planning (BCP)	• Loss of revenue and business service disruption • Contractual considerations with the event body to deliver the content • Brand damage impairing an organization's ability to retain or attract customers	• Crown jewels identification • One hundred percent adoption compliance of NCCs for all crown jewels • Business continuity plan • Third-party risk management program for broadcast vendors
Compromise of subscription and billing service	• Lack of web application control • Immature DevSecOps • Lack of security awareness for developers • Insufficient security monitoring	• Loss of revenue and business service disruption • Damage to reputation	• Web application firewall • DevSecOps maturity • Security training for developers • Security monitoring
Sensitive data leakage	• Lack of user awareness • Frequent use of Universal Serial Buses (USBs) to store and transfer data • Lack of encryption of sensitive data • Lack of data prevention controls at all exit points	• Threat to business operations • Loss of revenue • Damage to reputation • Breach of regulatory obligations	• Data leakage prevention • USB control • Security awareness program
Illegal live streaming	• No intelligence-based antipiracy service • No forensic watermarking to track illegal distribution • No antipiracy terms and conditions in customer contract • Lack of customer education	• Loss of revenue and revenue retention • Illegal competition • Contractual and regulatory considerations	• Intelligence-based antipiracy service • Forensic watermarking solution • Customer contract maturity • Public relations and customer education (e.g., "Piracy is a crime, and it is illegal.")
Social engineering attacks on VIPs and reporters	• Low employee awareness • Organizational culture (i.e., security is a technical problem) • Lack of human risk profiling	• Loss of reputation • Intellectual property leakage • Loss of revenue	• Security awareness and training programs • Human risk profiling • Email gateway with sophisticated phishing detection technique • Phishing reporter for email
Compromise of OTT applications	• Insufficient security testing • Lack of visibility into security capabilities of OTT platform	• Loss of revenue • Damage to reputation	• Penetration testing • Robust supplier security assurance program • Supplier risk rating • Implementation of a DevSecOps framework
Compromise of STB	• Insufficient security testing • Lack of visibility into security capabilities of STB	• Loss of revenue • Damage to reputation	• Penetration testing • Robust supplier security assurance program • Supplier risk rating

including people, processes and technology. The security foundation will address very high risk factors affecting the broadcast media enterprise during high-profile live events.

Once a security foundation is in place, the next milestone is to develop the highest priority capabilities, which will help to mitigate high risk factors with extreme impact. The remaining high risk factors are mitigated once the advanced capabilities are developed. The road map of initiatives to mitigate risk and strengthen cyberresilience capabilities for media broadcast enterprises is presented as an example in **figure 6**.

In addition, when deploying a cyberresilience capability it is helpful to review the specific broadcast media cybersecurity standards that are emerging as

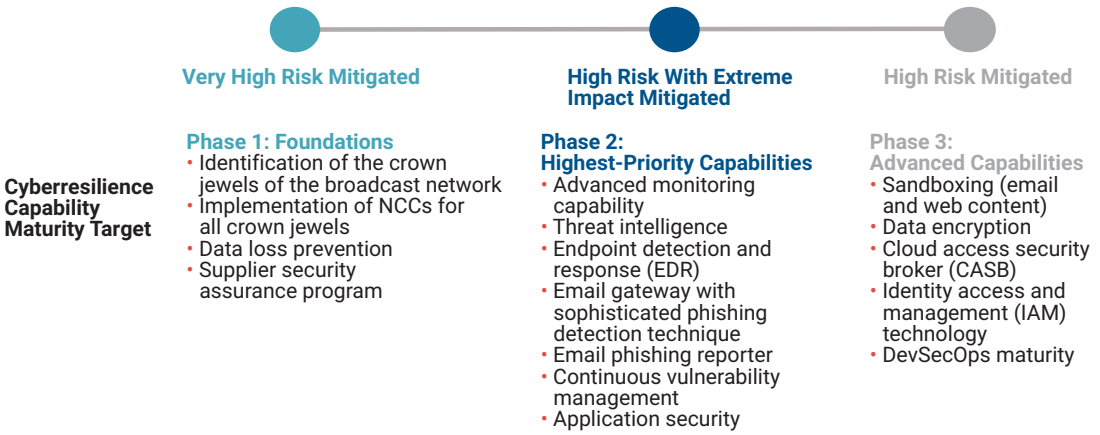
FIGURE 5

NCCs for Broadcast Media Network

NCCs	Potential User Resistance	Upfront Cost (e.g., Staff, Software, Hardware)	Ongoing Maintenance Cost
Application allow listing of approved and trusted programs for content management	Medium	High	Medium
Patch management strategy for crown jewels of broadcast network	Low	High	High
Secure administration with multifactor authentication (MFA) for the supporting broadcast engineers and for vendor support	Medium	High	Medium
Network segmentation within the broadcast network based on the business function and the enterprise network	Low	High	Medium
Advanced threat protection for all high-profile broadcast equipment	Medium	High	High
Continuous incident detection and response	Low	Very High	Very High
Role-based security awareness training for broadcast engineers, reporters and very important people	Medium	High	Medium
Penetration testing	Low	Medium	Low

FIGURE 6

Cyberresilience Strategy Road Map



these standards define security best practices and controls specific to the broadcast industry. These standards include:

- The Content Delivery and Security Association Content Protection and Security Standard[9]
- The Motion Picture Association Content Security Best Practices Common Guidelines[10]
- The Digital Production Partnership Committed to Security program[11]
- The European Broadcasting Union security recommendation[12]

Conclusion

The digital era has long been seen as the vanguard of advancement, and the way media content is consumed has been one noticeable effect of digital technology. Technology advancements have made it possible for users to switch from traditional methods of media consumption to digital technologies involving Internet streaming via mobile phones, tablets and other devices. At the same time, it has also presented a number of cybersecurity challenges and risk that can lead to the compromise of broadcast media enterprises' content, data and business systems. Given these challenges, it is essential for broadcast media enterprises to develop a cyberresilience strategy when broadcasting high-profile live events and to determine what cybersecurity challenges the enterprise faces specifically related to

core broadcast business services.

Endnotes

1 European Broadcasting Union, *R141 Mitigation of Distributed Denial of Service (DDoS) Attacks,* Switzerland, June 2015, *https://tech.ebu.ch/docs/r/r141.pdf*

2 BlueVoyant, *Media Industry Cybersecurity Challenges: A Vendor Ecosystem Analysis*, USA, *https://www.bluevoyant.com/resources/media-industry-cybersecurity-challenges*

3 *Trend Micro, Business Friction Is Exposing Organizations to Cyber Threats*, Japan, *https://www.trendmicro.com/explore/en_gb_trendmicro-global-risk-study*

4 Sophos, *The State of Ransomware 2020*, United Kingdom, May 2020, *https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf*

5 Sakellariadis, J.; *Behind the Rise of Ransomware,* Atlantic Council, USA, August 2022, *https://www.atlanticcouncil.org/wp-content/uploads/2022/08/Behind_the_rise_of_ransomware.pdf*

6 *Op cit* BlueVoyant

7 Synamedia, "Sports Video Operators and Rights Owners can Tap Into a $28bn Goldmine With Synamedia Anti-Piracy Solutions," 15 March 2021, *https://www.synamedia.com/press/sports-video-operators-and-rights-owners-can-tap-into-a-28bn-goldmine-with-synamedia-anti-piracy-solutions/*

8 Westcott, K. *et al*.; "2022 Digital Media Trends, 16th Edition: Toward the Metaverse," Deloitte, 28 March 2022, *https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html*

9 Content Delivery and Security Association, Content Protection and Security Standard, USA, February 2016, *https://www.mesaonline.org/wp-content/uploads/2016/04/Content-Protection-Security-Standard-February-2016.pdf*

10 Motion Picture Association (MPA), *MPA Content Security Program*, USA, 2022, *https://www.motionpictures.org/wp-content/uploads/2022/02/MPA-Best-Practices-Common-Guidelines-V4.10-FINAL.pdf*

11 Digital Production Partnership, "Committed to Security," *https://www.thedpp.com/security*

12 European Broadcasting Union, *https://www.ebu.ch/home*