MEDIA CYBERSECURITY SEMINAR

AN EBU EVENT

SHAPING A MORE SECURE MEDIA INDUSTRY

PROGRAMME

WEDNESDAY 11 OCTOBER 2023 (10:00 – 18:00 CEST) PHYSICAL AND ONLINE ATTENDANCE

10:00 – 10:10

Welcome & Introduction

Antonio Arcidiacono & Hans Hoffmann (EBU)

KEYNOTE

10:10 – 10:40

Digital safety of Ukrainian journalists

General rules. How Ukrainian journalists are working with information and ways to save it. Examples.

Kseniya Minchuk/Oksana Baldina. Journalist, writer, videographer, content maker, podcast author. More than 9 years of experience in journalism. The author of texts about women, the LGBT community, the war in Ukraine, refugees. Participant of social projects aimed at disseminating information about domestic violence. Member of volunteer initiatives. She began her career in journalism as a literary editor at the Kyiv information agency “Slovo i Dilo”. She was a correspondent in the Kryvyi Rih media "Expert-KR". She had her own social projects of various types: from entertainment to a documentary film about inclusive theater, the author and editor of which she acted independently. At "Hromadske Radio" she created podcasts, photo reports, and video stories. During the full-scale invasion, began working with foreign publications, participating in conferences and meetings in Europe to talk about the war in Ukraine and journalism in this difficult time. https://www.facebook.com/kminchuk

SESSION 1: CURRENT THREAT LANDSCAPE AND REGULATIONS

10:40 – 11:10

Cyber trends and threats to media

Discussion about the 2023 cyber threat landscape relevant to attack and vulnerabilities of media and international responses to these attacks

Gerben Dierick combines running the network team at VRT with his role as Information Security Officer. He currently co-chairs the EBU’s Media Cybersecurity Group and lectures on networking and cybersecurity topics at the University College Leuven Limburg.

Pavlina Pavlova is a cyber policy expert working on advancing accountability in cyberspace. Before joining the CyberPeace Institute in Geneva as a Public Policy Advisor, she served as an official at the Organization for Security and Co-operation in Europe (OSCE). She was appointed the OSCE Chairmanship's Liaison Officer and coordinated programmes strengthening the human dimension of security. Pavlina's experience combines a decade of policy and political advisory, programme development, and stakeholder engagement at international and national institutions. Her research at the intersection of technology and governance was presented at the Yale MacMillan Center, the Carr Center for Human Rights Policy of the Harvard Kennedy School, and the Stanford Internet Observatory, among other fora, and published by Yale University, Leiden University, and the University of Padua.

11:10 – 11:40

Journalists security on social medias

This presentation will provide an overview of the risks and challenges that media professionals face when using social media platforms, such as harassment, doxxing, and account hacking. We will explore best practices for protecting personal and professional information online, as well as tools and resources that can help mitigate these risks.

Anais Kessous (CBC/Radio Canada) As an Information Security Advisor at the Canadian Broadcasting Corporation, Anaïs Kessous specializes in Open Source Intelligence (OSINT) analysis and provides journalists with unique insights and recommendations to maintain a secure online presence. Anaïs has a major in Education and a minor in Criminology from University of Montreal, a Certificate in Cyber Investigation from École Polytechnique de Montreal, and holds a private investigator's license in Quebec. Before her current role, she held a position at a Montreal- based private security firm, where she was responsible for investigations. She is dedicated to helping journalists identify and mitigate the risks of online harassment and doxxing, and regularly provides training on information security for media professionals. At the Media Cybersecurity Seminar, Anaïs will share her considerable expertise and guide participants through the best practices for social media safety. Attendees will receive practical tips,and strategies to help them navigate the unique challenges of social media and to fortify their digital security practices going forward. LinkedIn : Anaïs K

11:40 – 12:10

NIS2 and Cybersecurity Resiliency Act Updates

Overview of the current state of legislation in cybersecurity law in the EU and Germany and its significance for the media.

Jelle Werner (SR) Legal counsel with a focus on private and public media law. Practical experience in European media law through work at the ARD liaison office in Brussels. Since 2022 working in the legal department of Saarländischer Rundfunk as an expert in data protection law, cybersecurity law, telecommunications law and European media law.

12:10 – 13:10	*Lunch break*

KEYNOTE

13:10 – 13:40

Navigating the Disinformation Age: The Growing Threats of AI and Deepfakes

A cautionary look at how artificial intelligence and deepfake technology could be used to spread disinformation and erode public trust in factual journalism

Dan Patterson (Blackbird.AI) covers the technology trends that shape politics, business, and culture. He specializes in cybersecurity and emerging technologies like AI and machine learning, blockchain, IoT, and metaverse. Previously he was the tech reporter for CBS News, a senior producer at CNET, a senior reporter at TechRepublic, the digital platform manager at ABC News Radio, and a writer at various media companies. Previously he was the tech reporter for CBS News.

SESSION 2: PROJECTS / CASE STUDIES

13:40 – 14:10

Eurovision 2023

Andrea Walker (BBC) is an experienced and certified Information Security professional and Head of Information Security at the BBC. Andrea has a list of academic qualifications including a Masters Degree in International Affairs and Cyber Security, A certificate in Terrorism Studies, including Cyber terrorism and terrorism using ICT, and ISC2 Industry qualifications CISSP and CCSP.

Andrea has frequently worked with Information Security concerns involving hostile environments, high risk programmes and high profile national and global events, having been nominated for a BBC News award for her activities to secure the UK's snap general election results of 2019. Andrea, more recently, lead the cyber security aspects of the Eurovision Song Contest 2023 for the BBC.

Andrea's passion for what she does stems from a deep seated desire to protect the BBC and it's audiences all over the world. Helping to ensure freedom of speech and access to unbiased, uncensored and news free from disinformation.

14:10 – 14:40

Securing office 365

This presentation will show how RTVE has lowered the number of incidents against Office 365 by implementing security measures.

Alvaro Martin Santos is Head of Cybersecurity Processes in RTVE, where started working on IT Security and IAM 14 years ago. He is Computer Science Engineer and is pursuing a PhD in Industrial Engineering, with a specialization in Security of IP broadcasting technologies at UNED - Universidad Nacional de Educación a Distancia (Spain).

14:40 – 15:10

Media Sanitization for Media Companies

EFF Board Member Bruce Schneier use to say that "Data Is a Toxic Asset". When Toxic Assets become Toxic Waste, they must be properly disposed. You shouldn't throw your Media Company's data in the trash: someone may find it!

Marco Bellaccini is an IT Infrastructure Architect at RAI. He designs reliable, secure and automated IT systems for Television Production. He's an Electronic Engineer (EE MSc) who joined the TV Engineering Department of RAI in October 2014. Previously, he did Robotics research at The Biorobotics Institute of Sant'Anna School of Advanced Studies and at Sapienza University of Rome. Personal website: https://bellaccini.it - Twitter: https://twitter.com/lasagnasec - GitHub: https://github.com/marcobellaccini

15:10 – 15:40

How Ross transformed to improve our Product Security

How Ross Video changed it's people, processes and products in response to growing awareness of the importance of cybersecurity concerns among our customers; and how you can benefit.

John Naylor (Ross) A Chartered Engineer since 1992, John also holds an MBA from Henley Management College, the UK's oldest business school, and has studied Cybersecurity at the University of Texas, San Antonio which is ranked #1 in the subject by the USA's Department of Homeland Security and is a Certified Information Systems Security Practitioner (CISSP). He is outgoing chair of SMPTE's study group into securing PTP, and serves on NABA's cybersecurity technical subcommittee.

15:40 – 16:00 *break*

SESSION 3: BEST PRACTICES AND TOOLS

16:00 – 16.30

Vulnerability Management for Media companies and Media Vendors: EBU Recommendation

Together with the EBU, ORF conducted a security assessment of various codec manufacturers. In this session, the most important findings will be shared.

Joerg Scheiblhofer has been working in various areas of IT at ORF since 2002. Since 2021, he has held the role of CISO in ORF's "Directorate for Technology and Digitization" and leads the company's "Information Security Management". From the very beginning, he has paid particular attention to information security issues and to measures to increase awareness of this important topic at all levels. His membership in various international expert committees and working groups has also allowed him to gain a wide range of insights into the cybersecurity of the broadcast scene.

16:30 – 17:00

Privacy preserving search engine for journalists

In this talk we will describe our collaboration with the International Consortium of Investigative Journalists to build a privacy-preserving decentralized search engine to assist them in their investigations.

Carmela Troncoso is an Associate Professor at EPFL (Switzerland) where she heads the SPRING Lab. She holds a Master's degree in Telecommunication Engineering from the University of Vigo (2006) and a Ph.D. in Engineering from the KU Leuven (2011). Before arriving to EPFL she was a Faculty member at the IMDEA Software Institute (Spain) for 2 years; the Security and Privacy Technical Lead at Gradiant working closely with industry to deliver secure and privacy friendly solutions to the market for 4 years; and a pos-doctoral researcher at the COSIC Group. Carmela's research focuses on security and privacy. Her thesis "Design and Analysis methods for Privacy Technologies" received the European Research Consortium for Informatics and Mathematics Security and Trust Management Best Ph.D. Thesis Award; and her work on Privacy Engineering received the CNIL-INRIA Privacy Protection Award 2017. She regularly publishes in the most prestigious venues in Security (e.g. ACM Conference on Computer Security or USENIX Security Symposium) and Privacy (Privacy Enhancing Technologies).

17:00 – 17:30

How to control the social Media and Darkweb for harmful contents like Deepfake, Fake Campains and Disinformation.

How media companies are controlling the social media for harmful content and prevent their self from threats.

Ozan Akyol (SecWide) started his career as an IT consultant in the private sector in Turkey in 2007, after graduating from Melbourne university. He moved to governmental sector, fighting against cyber crimes in public organizations such as Turkish police and Ministry of Internal Affairs. He started his own company in 2018, providing cyber intelligence and penetration and security tests services. Ozan received several bug bounty awards from institutions such as Daimler and KIWI in Europe. He is now based in Austria and his company SecWide offers cyber intelligence and cyber security services in all Europe.

17:30 – 18:00

Production Security in the Age of the Cloud

Production is moving to cloud and hybrid cloud infrastructure with new workflows and new ways of sharing infrastructure with remote users and sub-contractors. Securing these innovative workflows using traditional perimeter-based security is extremely complex, and often unmanageable. At the same time, perimeter security is failing disastrously in many sectors, both business and government, as bad actors acquire ever more sophisticated technology.

However, in this perfect storm is the opportunity to move forward from a security model created at the birth of Internet and based on a security principle dating back thousands of years: build a wall to keep intruders out.

The solution lies in zero-trust security and its assumption that intruders are already inside the wall. Zero-trust, coupled with the principle of security by design, offers the ability to create security models that do not interfere with the creative process and where security can be turned up and down depending on production requirements and risk assessment. This is the purpose of the MovieLabs Common Security Architecture for Production.

As Senior Vice President Production Technology and Security, **Spencer Stephens** is engaged in projects on production technology and leads MovieLabs work in the security of production workflows.

He was principal author of the MovieLabs “Securing the 2030 Vision” whitepaper and leads the work on the Common Security Architecture for Production (CSAP). CSAP is a zero-trust architecture designed for protecting media production workflows in the cloud and in hybrid cloud infrastructure.

Prior to MovieLabs, Stephens served as CTO at Sony Pictures Entertainment, leading the studio's technology group working on technology innovation and application, touching on every part of the content path from on-set, through post-production and mastering to delivery to provide a full consumer experience.

He has managed the digital production group at Disney TV Animation, and a post-production facility at Warner Bros as well as being a leading contributor to the development of technology in motion picture and television production and distribution.

Stephens has an MS in Computer Science and an MS in Cybersecurity, both from the University of California, Berkeley, and a BSc in physics from the University of Sussex, UK.

Wrap-up - End of Day 1

18:00 – 21:30 ***Social event***

PROGRAMME

THURSDAY 12 OCTOBER 2023 (9:00 – 14:00 CEST) PHYSICAL ATTENDANCE ONLY

PLANNING THE DAY

09:00 – 09:30 Introduction and building the agenda

BREAK-OUT SESSIONS

	ROOM 1	ROOM 2	ROOM 3
09:30 – 10:15			
10:30 – 11:15			
11:30 – 12:15			
12:30 – 13:15			
13:15 – 14:00	**Debrief on break-out sessions and closing**		