MEDIA CYBERSECURITY SEMINAR

AN EBU EVENT

SHAPING A MORE SECURE MEDIA INDUSTRY

PROGRAMME

TUESDAY 12 OCTOBER 2021 (09:55 – 18:00 CET)

09:55 – 10:00	**Opening**	
10:00 – 10:10	**Welcome & Introduction**	Hans Hoffmann (EBU)

KEYNOTE SESSION

10:10 – 10:40	**Cybersecurity: Human-centric Reporting, and Risks for Journalists as targets** The CyberPeace Institute provides a perspective on two key themes in cybersecurity: (1) cybersecurity reporting and shifting the focus to what happens to people, the victims of cyberattacks, and (2) the importance of cybersecurity for journalists themselves.	Stéphane Duguin (CyberPeace Institute)

SESSION 1: CYBERSECURITY THREATS IN 2021

MODERATOR: RAINER JOCHEM (SR, MCS CHAIR)

10:40 – 11:10	**Cybersecurity threats to public service media in 2021** Public service media are increasingly a target for cyber-attacks. MCS group has done a compilation of all the threats they experienced in 2021.	Gerben Dierick (VRT)
11:10 – 11:40	**Hacking humans: the social media threat** Social media are an invaluable resource to journalists, but they're also a significant threat. This session will examine how social media and publicly available sources have been used to gather information about targets and facilitate attacks on them and their families.	Martin Turner (Full FrameTech)
11:40 – 12:10	**Ransomware attacks in 2021** Ransomware has a long history, going back to 1989. But they have become a massive problem as they more and more have an impact beyond the company, on end-consumers and the operations of critical infrastructure.	Don Smith (Secureworks)
12:10 – 12:40	**Modern standards keep us connected!** To keep the internet open, free and secure we need to adopt modern internet standards. They safeguard our connections, our privacy and our information and are needed for transparant use of the internet.	Gerben Klein Baltink (Internet.nl)
12:40 – 13:30	*– Lunch break –*	
13:25 – 13:30	*Opening*	

KEYNOTE SESSION

13:30 – 14:00	**Adventures in Securing High-Risk People** Newsrooms have security requirements not seen in other departments. What are they? How do we learn about them? How do we address them? This keynote will share adventures in securing high-risk people, including. building the newsroom security program at The New York Times.	Runa Sandvik (Security Researcher)

SESSION 2: MEDIA PROJECTS AND SECURITY

MODERATOR: GERBEN DIERICK (VRT)

14:00 – 14:25	**BBC Information Security Knowledge Graph** A quick overview on the BBC Information Security team's approach to capture the semantics and idiosyncrasies of a 100 year organisation into a working set of definitions of entities and their properties into a model that allows us to support of a dynamic and efficient risk management process.	Bruno Garrancho (BBC)
14:25 – 14:50	**Securing SRT live streams** SRT is an open source video transport protocol that enables the delivery of high-quality and secure, low-latency video across the public Internet. Stefan will present on the implementation of SRT at SWR and the challenges of QoS and firewall configurations in a media production environment.	Stefan Ringhoffer (SWR)
14:50 – 15:15	**Cybersecurity in sport events: the Euro 2020** The challenges around making the Euro 2020 secure, impacts of new production workflows on the broadcast network security, risks in infrastructure that include remote production, opetors working from home, and multinational venues, plus an outlook on what's next.	Vincent Gafanesch (UEFA) Geoffrey Crespin (EVS)
15:15 – 15:40	**Cybersecurity at CBC/Radio Canada's new broadcast facilities** CBC/ Radio Canada has recently moved to a brand new building. Security is at the heart of the migration project.	Philippe Edmond, Francois Legrand (CBC/Radio Canada)
15:40 – 16:00	*– Break –*	

SESSION 3: MEDIA SYSTEM VULNERABILITIES

MODERATOR: GERBEN DIERICK (VRT)

16:00 – 16:30	**Hacking broadcast systems** Broadcast Technology relies more and more on IT systems. This transition results in a fundamental change in protection goals and how to achieve them. While stability and availability remain the primary protection goals, the way to achieve them is fundamentally different in a digital infrastructure. Sadly, today's broadcast systems and infrastructures do not reflect this: They are easy to breach, because they rely on outdated security assumptions. In this presentation, we will investigate the most common shortcomings and how to avoid them.	Linus Neumann (Consultant & Hacker)
16:30 – 17:00	**Cybersecurity test campaign on smart TV receivers** DTG has investigated on how TV manufacturers are now having to reconsider how they categorise their products, the impacts of upcoming IoT legislation on Smart TVs and other network connected devices.	Alex Buchan (SafeShark)
17:00 – 17.30	**SMPTE ST 2110 Security and What standards organizations are doing** Securing SMPTE ST 2110 systems is becoming an important issue. Many users and equipment vendors do not know where to start. To assist, standards and related organizations such as SMPTE, JT-NM, AMWA, and the EBU are working on specific parts of the security challenge. This presentation summarizes the ongoing work in the different organizations.	Leigh Whitcomb (Imagine Communications)
17:30 – 18:00	**ROUNDTABLE:** **Making the pyramid green: how can media systems be more secure?**	Félix Poulin (CBC/Radio Canada), Peter Brightwell (BBC), Brad Gilmer (Gilmer & Associates), Leigh Whitcomb(Imagine Communications), Gerben Dierick (VRT), Ievgen Kostiukevych (EBU)
18:00	*– End of Day 1 –*	

PROGRAMME

WEDNESDAY 13 OCTOBER 2021 (09:55 – 16:45 CET)

09:55 – 10:00	**Opening and welcome**	Antonio Arcidiacono (EBU)

SESSION 4: SECURITY AWARENESS AND REGULATIONS

MODERATOR: RAINER JOCHEM (SR, MCS CHAIR)

10:00 – 10:30	**Digital Target Hardening** How my team apply 'Digital Target Hardening' to enhance the safety of individuals at risk from digital threat actors. This is achieved through leveraging wider information security tools as well as the application of specific tools and techniques.	Mike Bond (BBC)
10:30 – 11:00	**Executive awareness of cybersecurity** How to create, build and operate a successful top-down cybersecurity strategy. The presentation will provide you with key insight about how a cybersecurity strategy should be built, what would be the key drivers and how to get strong support from the executives	Fabrice Guye (ELCA)
11:00 – 11.30	**The security awareness programme at SRG** With the constant change in the cybersecurity landscape, media organizations can no longer just rely on technological defenses to keep them safe. Employees are an essential part of the security problem. This is why cybersecurity education is a priority and must be addressed in every organization. During this online session Mona Brunner from SRG will share insights of the security awareness programme at SRG.	Mona Brunner (SRG)
11:30 – 12:00	**GDPR and CLOUD Act: possible approaches for assurance and compliance** The invalidation of the Privacy Shield alongside the approval from the US government of the CLOUD Act has created several concerns within the cloud market. European cloud users are unclear on what risks they face when using the leading cloud services providers. Is there a compliance risk vis-a-vis the GDPR? Are there risks for the confidentiality of their data? Are there risks for their reputation? In this presentation, Daniele Catteddu, Chief Technology Officer at the Cloud Security Alliance (CSA), will provide an overview of the problem at stake and propose some possible compliance and technical solutions to continue an organization's transition to a cloud environment securely.	Daniele Catteddu (CSA)
12:00 – 13:30	*– Lunch Break –*	
13:25 – 13:30	*Opening*	

KEYNOTE SESSION

13:30 – 14:00	**Enabling Software Security with DevSecOps** A lot of folks talk about the "what" behind DevSecOps, but few have mastered the "how" that makes it a success. With Development and Operations functions fused together in most organizations, Security must become a first-class cultural component in software engineering practices. In this talk, Check Point Field CISO Cindi Carter will share the story of how her team at a health IT company succeeded in implementing the secure Software Development Lifecycle for an organization with more than 3500 reluctant developers worldwide. In this session, you will learn how to build in cybersecurity rather than bolting it on later:	Cindi Carter (Check Point Software Technologies)

- Understand the developer's mindset and motivation
- Exploit the company culture and incentivize developers to desire security
- Expand from a few early adopters to thousands of developers
- Overcome the roadblocks that arise along the way

SESSION 5: CYBERSECURITY LATEST PRACTICES

MODERATOR: LUCILLE VERBAERE (EBU)

14:00 – 14:25	**Microsoft's security portfolio: overview and feedback** Nowadays, Microsoft is one of the top leaders in the cybersecurity market, investing billions dollars in this field every year. Marketing aside, during this presentation, we will go through a quick overview about Microsoft's security solutions and share our field experience. Pros and cons will be exposed, benefits will be presented, and the real challenges behind the scenes, especially when migrating from a multi-vendors based security stack to a consolidated approach using Microsoft, will be explained.	Benoit Ramillon (UEFA)
14:25 – 14:50	**The secure credentials-sharing utopia** Credentials should not be shared between different users. Still, sometimes, password sharing is necessary: how can we do it right? There are many Password Managers that include functionalities for secure password sharing. However, there's no one-size-fits-all solution. We'll talk about Password Managers Pros and Cons, ways to share passwords with guests and we'll have a sneak peek at HW-tokens, FIDO2 and password-less solutions.	Marco Bellaccini (RAI)
14.50 – 15.05	*– Break –*	
15.05 – 15.30	**Creating Awareness against Cybersecurity Threats from Production to Distribution** Cybersecurity threats are becoming as innovative as the piracy services being served to end users. It is a billion dollar business. We can only minimize risks by protecting our most valuable content with the technology available to us. What can not be protected needs further awareness so threats can be detected with intelligent data available. Finally we need an enforcement strategy. Join us to learn more how to efficiently PROTECT, DETECT and ENFORCE together	Ilker Ürgenc (Akamai)
15.30 – 15.55	**Application Security Security Automated** It can be hard to cut through the marketing hype in cybersecurity. In this talk, I'll focus on application security (appsec), which is the root cause for a large number of hacks. I'll bring you through the basic building blocks of the four corners of appsec, what they do, and the tradeoffs. I'll tell you why fully autonomous appsec focuses on fuzzing, and why most enterprises (especially devops) are moving in that direction, contextualized within those tradeoffs and motivations.	David Brumley (ForAllSecure)
15.55 – 16.20	**Defending against the ransomware threat** Ransomware is currently on the top of media company lists of cybersecurity concerns. This session will consider some practical control steps in each of the 5 NIST Cybersecurity framework domains (Identify, Protect, Detect, Respond, Recover) to help mitigate ransomware risks to your organisation.	Andrew Sands (BBC)

CLOSING SESSION

16:20 – 16:45	**The cybersecurity outlook for 2022**	Rainer Jochem (SR, MCS Chair)
16:45	*– End of Day 2 and MCS 2021 –*	