11:00 – 12:20 | Room 11 | Tuesday – Aug.27

AUDIOVISUAL CONTRIBUTION AND INFRASTRUCTURE

CYBER SECURITY: I'VE BEEN INVADED, NOW WHAT?

Cybernetic attacks are becoming more frequent, leading to a halt in operations, data leak, reputation damage and financial loss. Since the occurrence of an incident is inevitable, it's up to the companies to prepare themselves to respond in a fast and effective way.
On this panel we will present the main aspects to be observed in monitoring activities and event detection, response processes to incidents, crisis management and resilience.

Chair: **Vinícius Brasileiro -** Executive Supervisor of Information Security / TV Globo

• INCIDENT RESPONSE - STAGES TO MINIMIZE IMPACTS AND DISCOVER WHAT FAILED
Speaker: **Bruno Cesar M. Souza -** In this brief lecture, Bruno Cesar M. de Souza will explain in a practical and brief way how an incident response process must be in its stages, focusing on possible real breach incidents. The order in which action must be taken will be explained using a methodology accepted internationally. It will be demonstrated how specialists respond in an effective way to a breach incident, containing the breach, investigating to discover how compromised the system is, exploited the vulnerabilities exploited and possibly those responsible, how to treat the incident minimizing damage, preventing new incidents and improving the response process.

• CRISIS MANAGEMENT DURING A CYBER ATTACK
Speaker: **Silvio Pezzo -** Professional of Cyber Security & Resilience, Audit, Risk, Crisis & BCP
In this talk we will present how to take a Crisis Management approach derived from ill-treated critical cyber incidents, including the steps of Declaration crisis, opening the Crisis Rooms, Crisis Response and its closure.

• INCIDENT DETECTION
Speaker: **Rodrigo Almeida Gonçalves -** Internet Security Manager / Globo.com
In this talk, incident cases will be presented and how the detection time factor is proportional to the impact on business . We will also present the evolution of the detection process since log review, through SIEM and now using big data and machine learning and how these technologies help reduce detection time and thereby restrict business impact.

Chair: Vinícius Brasileiro - Executive Supervisor of Information Security / TV Globo
Vinícius has degrees in Computing and Accounting from Estácio de Sá University and a master's degree in IT Audit also from Estácio de Sá University. With more than 15 years of experience in data security, governance, risk and compliance, he earned the Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified in Risk and Information System Control (CRISC) from ISACA; Certified Chief Information Security Officer (C|CISO) from EC-Council; Certified Business Continuity

Professional (CBCP) from DRII; Lead Auditor in Information Security Management System (ISO 27001:2005 LA) from BSI. He is also Director of Associates at ISACA – Rio de Janeiro Chapter and member of the Risk Management Special Study Commission and the Information Technology Study Commission – Security Techniques of the Brazilian Committee of Computers and Data Processing at ABNT.

Bruno Cesar M. Souza - Partner and Technical Director of Able Security
Bruno Cesar M. Souza, CISSP, OSCP, GPEN, GCFE, GCFA, GCIH – Partner and Technical Director at Able Security, with more than 17 years of experience in data security projects, specialist in penetration testing and data security incident investigation. He has worked on several vulnerability assessment projects, penetration tests, investigations and responses to data security incidents, computer forensics, security solution specifications and implementation for large companies from the following segments: aviation, digital commerce, financial, media, insurance, governmental, oil and gas, transportation and telecommunications in Brazil and the United Kingdom. He has worked in Manchester, UK, as a consultant for a penetration test team of a multinational company, leader of this segment in Europe. He held penetration test projects for security consultancy in Melbourne, Australia, in one of the major Australian banks. He has a degree in Computer Information Systems from PUC-Rio, certifications CISSP (Certified Information Systems Security Professional) since 2007, OSCP (Offensive Security Certified Professional) since 2010, SANS GCFE (GIAC Certified Forensics Examiner) since 2012, SANS GCFA (GIAC Certified Forensics Analyst), SANS GCIH (GIAC Certified Incident Handler) and certification SANS GPEN (GIAC Penetration Tester).

Silvio Pezzo - Professional of Cyber Security & Resilience, Audit, Risk, Crisis & BCP
He is currently Senior Executive in Crisis Management & Cyber Security for Latin America with 20 years of experience in Cyber Security and Resilience consulting. He has authored over 50 Continuity Plans, Crisis Management Plans, IT Disaster Recovery Plans, Pandemic and Emergency Response, including testing and simulations involving C-Levels and tactical / operational teams in companies across the most diverse segments of Brazil , Latin America and the Caribbean, including the financial industry, communications, telecommunications, oil, government, energy, retail, consumer goods and health.He is MBCP / CBCP certified by DRII-USA and official instructor of DRII (Disaster Recovery International Institute) for South America since 2014 and certified since 2006. He is a Professor of the Graduate Course in Crisis Management and Business Continuity at Presbyterian University. Mackenzie

Rodrigo Almeida Gonçalves - Internet Security Manager / Globo.com
Rodrigo holds a Bachelor of Computer Science degree from the Federal University of Minas Gerais. He has over 18 years of experience in TCP / IP networking, Internet Services and Web Application Security. He currently holds the position of Internet Security Manager at Globo.com, being responsible for the product security architecture and the defense strategy that ensures portals integrity and availability. In addition, he heads CSIRT.globo, which is responsible for managing incidents involving Grupo Globo's ASN.