CYBERCRIME MANAGEMENT CONFERENCE

3-5 October 2018
Manna Resorts
Glen Lorne
Harare

Theme: 'Transforming the Nation in the Face of Cyber Threats'.

In today's business environment, organisations are becoming increasingly vulnerable to criminal elements either through physical or digital means. In as much as organisations may have adequate physical security,- today's cyber environment requires maximum protection of the cyber infrastructure, as the threat of fraud, hacking, harm and loss have become realities in day to day operations. The daunting task faced by security and ICT administrators lies in knowing how to identify and proactively manage these risks to ensure the safety of organisations.

The rapid development of the Internet and technology has changed the landscape of conducting business in the world. However, this transition into the digital age has created immense opportunities for criminals; thereby presenting new challenges to the security and financial services sector. As security systems become digital, the growing emphasis on cybersecurity in the security sector is a natural evolution for the industry.

The purpose of this conference is to:

- Provide a platform for training of Government, parastatals, local authorities, the banking sector, academia and the private sector on cyber security
- Expose participants to new and emerging threats to cyber security and how to mitigate those threats
- Explore challenges, and proffer solutions to organisations facing threats from cybercriminals
- Provide an opportunity to share challenges and experiences, and to create smart partnerships in the fight against cybercrime.
- Provide a critical interface between industry and academia and chart the path for future collaborative arrangements

Conference Sub themes:

- Cyber-crime and cyber terrorism in the 21st Century
- Cyber-crime investigation
- Technologies for protecting Critical Infrastructure from Cyber Criminals
- Digital forensics and investigation.
- Cyber-crime Law and procedure
- Identity Thefts, Card cloning and E-business related Crimes Investigation of white collar crimes
- Emergency Crisis Management and Disaster Recovery

Who should attend?

The programme is designed for:

- Directors of Security
- Finance Directors
- Accounting Officers
- Auditors
- Chief Security Officers
- CEOs of Companies
- Operation Managers
- ZRP Commercial Crime Division Officers
- Bank ICT and Security Officers
- Security supervisors.
- Loss Control Officers
- Risk Control Managers
- Risk Officers
- ICT personnel
- Security Managers

Added benefits for attending the programme.

Over and above enhancing skills, this training will empower participants on the following broad aspects:

- Knowledge on real-time crime & incident data
- Information on how cyber/internet crimes are committed and how they can be minimized and investigated
- How to craft Enterprise Risk Management programmes, cyber incident response procedures/plans; and policies that meet organisational goals
- Recognize the potential financial benefits of crime prevention or reducing pilferage
- Discuss challenges, barriers, and solutions to creating a comprehensive crime prevention plan
- Increase awareness of new trends of how cybercrimes are being committed
- Find expertise in design, support and engineering of security solutions that minimize risks
- Learn to integrate facilities, maintenance and IT departments
- Improve risk assessment & management.
- Expedite response time of emergency response personnel
- Improve synergies and potential partnerships among law enforcement, judiciary, security staff and ICT personnel
- Network with security practitioners from other organisations and learn about crime trends in various sectors in Zimbabwe
- Cut security related costs by adopting realistic and effective security strategies

Practical Demonstrations

- How attackers deploy phishing (email) attacks using online systems
- How hackers can steal information over a network/WIFI How attackers can steal all passwords from computers
- How smart phones can be used to spy using simple apps
- How a hacker can steal bank details
- How Identity theft is orchestrated

PROGRAMME OF EVENTS

TIME	DAY ONE
0830 hours to 1630 hours	Impact of Cybercrimes in the 21st Century
	New and emerging threats of cyber-crime and cyber terrorism
	Challenges of Cyber-crime investigation
	Practicals
	Risk Analysis, penetration tests, mitigation & security audits
0830 hours to 1630 hours	**DAY TWO**
	Technologies for protecting Critical Infrastructure from Cyber Criminals
	Digital forensics and investigation
	Identity Thefts, Card cloning and E-business related Crimes Investigation of white collar crimes
	Practicals
	Cyber-crime Law and procedure
	Preservation of Cyber Evidence and presentation in Court
0830 hours to 1630 hours	**DAY THREE**
	Cyber Security Incident Response Plan
	Emergency Crisis Management and Disaster Recovery Plan

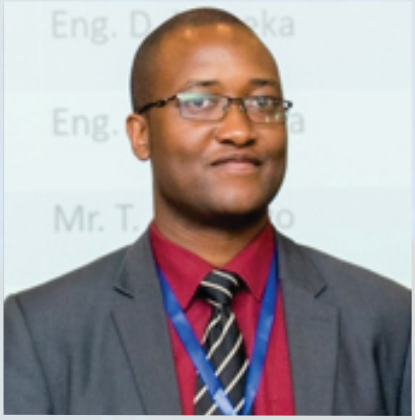
PROFILES

DR. RICH YOUNG (PH.D. CISSP, CISA, COSO)

Dr. Young is a 23 year veteran in the Information Security & Cyber Risk environments with extensive hands-on expertise for establishing and maintaining the enterprise vision, strategy and program to ensure information assets are adequately protected using the best practices methodologies and tools relevant to IT Risk Management. Dr. Young has previously held various senior management positions at Barclays PLC (Chief Information Security Officer), Citigroup (SVP Information Security), Deutsche Bank (Americas Office-CISO), Freddie Mac (Director, Enterprise Risk Management)

SIMON KARUKI

Simon is the Regional Head of Corporate Security and Investigation Services at Ecobank East Africa where he is charged with overseeing Security, Fraud Risk and Investigations management. He holds a Masters of Science Degree in Security and Risk Management from the university of Leicester. He is also a Certified Fraud Examiner (CFE). Simon has handled several complex Fraud Investigations during his career which spans for more than nine years.



ROBERT T ROSENTHAL SHONIWA

Engineer Robert T.R.Shoniwa is a cybersecurity specialist with a B.Tech in Computer Science, and an M.Tech in Information Security and Cyber Forensics from SRM University in India. He is also a Certified Ethical Hacker and an Access Data Certified Forensics Examiner (ACE).

His passion lies in cybersecurity and the development of collaborative research solutions. Shoniwa has collaborated with various local and international institutions such as the Zimbabwe Research and Education Network, (ZIMREN)), the Ministry of ICT and Cybersecurity, the University of Oxford and the Data Carpentry Foundation.

Shoniwa is also a member of several organisations including ZICT, - the ICT division of the Zimbabwe Institute of Engineers (ZIE) where he is the Cybersecurity Representative; the Computer Society of Zimbabwe (CSZ) IT Security Special Interest Group (SIG) where he is a committee member, and the Zimbabwe Internet Governance Forum (ZIGF) where he is a member of the Multi-Stakeholder Consultation Team,s responsible for capacity building and stakeholder engagement. He is also a member of several computing and engineering bodies such as IEEE, ACM, ACM-SIGSAC, IEEE Computer Society, ISOC Zimbabwe Chapter and the IETF. Shoniwa has also played a key role in hosting a number of conferences, workshops and seminars some which were aimed at igniting innovation in young researchers. He has also presented papers at local and regional fora.

JOICE BENZA

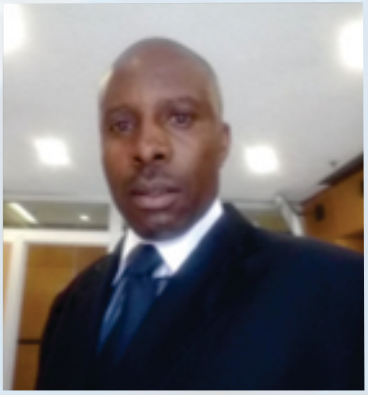
Joice is the founder, Managing Consultant and CEO of X-Pert Solutions, which focuses in delivery of complete ICT Solutions and Project Management. Prior to setting up X-Pert Solutions, Joice was a senior Executive and CIO at the helm of large corporates, where she implemented a multiplicity of Insurance Systems, Infrastructure, Customer Relationship Management(CRM) and ERP Solutions. She has over 30 years diverse ICT experience and expertise, gained locally and across Sub-Sharan Africa. Joice has extensive expertise in implementation of Insurance, Pensions Administration, Banking as well as other Financial Services Sector Systems. Among her various achievements she has set up and managed Business Continuity Plans and ICT Disaster Recovery Centers.

Joice has experience in running with National and Sector Projects which include the Year 2000 project and Computer Society Industry Systems. Joice holds an MBA degree from Nottingham Trent University (UK), a Diploma in Management Studies from Nottingham Trent University (DMS, UK), Financial Management Diploma (ACCA, UK) and a Certificate in E-management from Wits University (SA). She also holds a Certificate in Business Project Manager (Wits University, SA), holds an EDP (UZ) from the University of Zimbabwe and is a Member of the Computer Society of Zimbabwe (MCSZ). She is member of the Institute of Consulting (UK) and a member of ZNIC (Zimbabwe Institute of Consultancy). Joice sits on the Computer Society of Zimbabwe Council and other several Boards and Chairs a multiplicity of ICT Steering Committees.

TATENDA MUJATI

Tatenda is the Head of Information Technology at Grant Thornton Zimbabwe. She is an IT Audit and Security specialist with over 10 years' experience in consulting for specialized services ensuring the confidentiality, integrity, and availability of systems, networks, and data. She is passionate about the planning, analysis, development, implementation, maintenance, and enhancement of information security services.

Tatenda is a qualified Certified Information Systems Auditor with vast experience in IT systems security, project management, IT advisory and risk assurance. She holds a BSc. Honours degree in Information Systems and has had professional training and certifications in technical areas including Digital Forensics, Penetration Testing, IT Governance, Risk Management COBIT, Networking, System Implementation Reviews and Project Management. Tatenda is also a board member of the ISACA Harare Chapter.



CLEMENCE CHIMBARI

Clemence Chimbari is the Principal Public Prosecutor under the National Prosecuting Authority of Zimbabwe, (NPA). He holds a Bachelor of Laws (LLBs) degree from the University of Zimbabwe, and is currently attached to the Economic Crimes and International Cooperation section at the NPA head office in Harare. He has 26 years' experience in Public Prosecution and has attended several local and international conferences on cybercrime.

TENDAI MUNYARADZI MARENGEREKE

Tendai is an expert in Cyber Security; a certified Oracle Java Programmer and a Certified Ethical Hacker. He holds a Masters of Technology in Information Security & Cyber Forensics from SRM University in India, and a Bachelor of Technology (Honours) degree in Computer Science from the Harare Institute of Technology. He is also an Academic Exchange Scholarship.

Alumnus- Computer Science Academic Exchange (Daejeon University, South Korea).

Tendai has written several research papers in the areas of Information Security. His research interests are Defensive Security/ SIEM, Machine Learning, Security Analytics, NLP and Python Programming.

INNOCENT MAPANGA

Innocent Mapanga is a PhD fellow at SRM University. He holds an M.Tech in Computer Science and Engineering from the Delhi Technological University and a BSc (Hons) Computer Science from the Bindura University of Science Education.

He is a members of various computing and engineering bodies such as ACM, IEEE, IETF, CSI, Youth Sig on the ISOC Chapter, ISOC Zim Chapter.
Work History:

- IBM, Co-Founder RIPTech Consultancy Services
- Region Technical Support Specialist-SADC
- Civil Aviation Authority of Zimbabwe
- Namibian Embassy
- Harare Institute of Technology (Chairman - Computer Science Department)

Innocent has ICT experience spanning over 10 years with key competencies in the design and deployment of high end ICT infrastructure solutions to allow business continuity in the aviation, higher education, tele communications and banking industries. He works with Enterprise, Midrange and Entry level Cisco, Redhat, IBM and Dell EMC solutions, overseeing their design and deployment. He has participated in the crafting of the minimum body of knowledge for the Computer Science curriculum for Zimbabwean Universities, a draft policy for IPv6 for Zimbabwe, and has participated in the drafting of the Cyber Security bills for the Republic of Zimbabwe.
In his free time, he mentors young people keen on starting Tech businesses, and those interested in generating a positive change in the Internet ecosystem,- including reviews and contributions to internet policies and cyber laws.
His other interests lie in secure protocol design, algorithms and performance evaluation for computer networks, IoT Environment and Cyber Physical Systems.
Mapanga's research interests are in Network Security, Adversarial learning, Machine learning, Game Theory, IoT Big Data

Registration Form

Cyber Crime Management Conference

REGISTRATION DETAILS					
Company Name		Cost of attending **$1000.00** inclusive of accommodation and **$600.00** exclusive of accommodation	**HIT Banking Details**		
Postal Address			**Name:** Harare Institute of Technology		
Postal Code			**Bank:** CBZ Sapphire Branch		
Telephone Number			**Account Number:**02420583120037		
Email Address			**Swift Code:** COBZZWHA		
City and Country			**Branch Sort Code:**6120		
Nature of Business			*finance-inquiries@hit.ac.zw*		
Name of Delegate(s)	**Designation**	**Email Address**	**Phone Number**	**CONTACT PERSONS**	
				Ms. Benhilda Nyamuziwa	**0772919888**
				Email - *bnyamuziwa@hit.ac.zw*	
				Mr. Leonard Madyagwayi	**0775072970 / 0716216212**
Authorization By: Name		Position			
Signature		Date		**Email –** *lmadyagwayi@hit.ac.zw*	

Method of payment *(tick appropriate box)*

Cash Payment		Bank Transfer		Pay Now	

1. Payment terms: On return of a registration form, full payment is required within 7 working days, and payment must be received prior to the conference date. HIT reserves the right to refuse entry into the conference should full payment not have been received prior to this date. Cancellation will be charged under the terms set as below.
2. Cancellations: No Shows & Substitutions: Cancellations received in writing more THAN 21 days prior to the event conference carry a 50% of the event fees as cancellation fees. Should cancellation be received between 21 days and the date of the event, the full conference fee is payable and non-refundable. Non-payment or no attendance does not constitute cancellation.
3. Alterations to advertised package: HIT reserves the right to alter this programme without notice or penalty, and in such situations, no refunds or part-refunds or alternative offers will be made. Should HIT permanently cancel the conference, for any reason whatsoever, the client shall be well provided with a credit of equivalent amount paid towards the cancelled conference. In the case of a postponed or cancelled conference.
4. In the case of a postponed conference, no refunds will be made as arrangements for attending on the next conference will be considered.
5. In the event of a cancellation of the conference, HIT will not be responsible for covering the costs of air fare, accommodation or other travel costs incurred by clients.