

**Cyber Security and the Financial Industry-
Risks and Operational Impact**

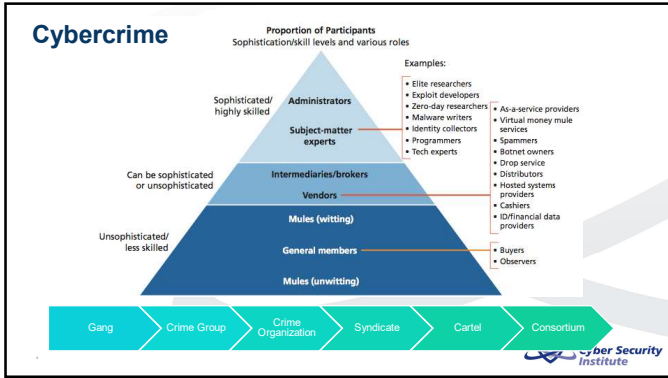
Moonstone & CSI Roadshow 2019
 Prof. Elmarie Biermann
 Elmarie@cybersecurityinstitute.co.za
 Justin Westcott
 justin@cybersecurityinstitute.co.za

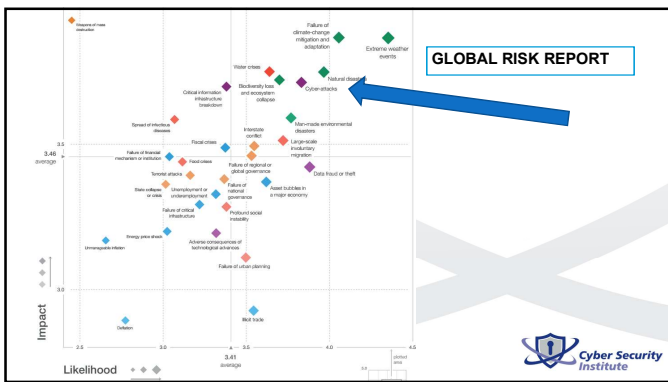
Current Status

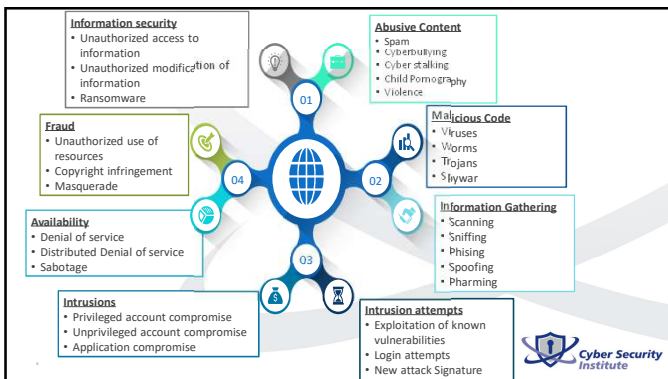
- Local Breaches
 - Liberty Breach
 - Master Deeds Records
 - Gautrain
- International Breaches
 - British Airways
 - Facebook

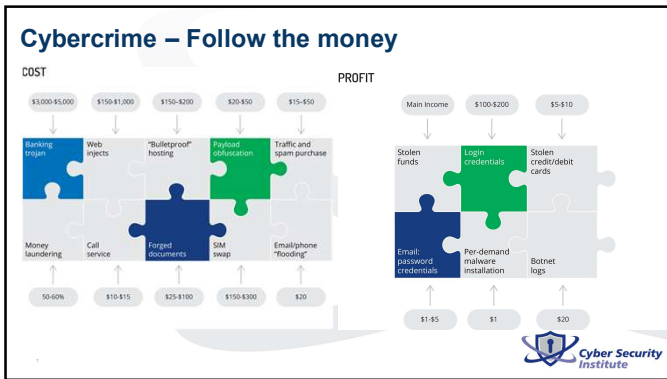
Threat Profiles

- **Cybercrime** - Most common, main goal is monetization
- **Nation State** - depending on company profile can be espionage, intellectual property theft, sabotage
- **Insider Threat** – monetization, sabotage / revenge
- **Hacktivism** – indirect target for a political / social statement









Cyber Attack Methods

- Sextortion
- Everything as a service (has, raas, etc.)
- Invoice changes (email attack)
- Malware
- Phishing
- Social Engineering
- Spam

The development of Cyber services for hire

Job Scams

Quick Warning: You are likely required to send your money before...

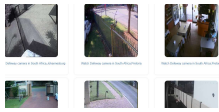


1. Know the signs: 'Yellow jobs scam exposed' covered in The Times was broadcast of Government Communication and Information System Fraud Prevention meeting. According to the alert, Fraudsters increasingly use government employment agencies that collect thousands of inquiries and send them to their personal email, which they use to contact you.

2. Beware of job offers that are too good to be true: Government Jobs Application Page on Facebook offering jobs in the UK Police Service, departments of home affairs, health and education, the UK Social Security Agency, Transport and the Treasury are others.

3. Beware of job offers that are too good to be true: Beware of job offers that are too good to be true. Beware of job offers that are too good to be true. Beware of job offers that are too good to be true.

PHYSICAL vs CYBER SPACE

- 4th Industrial Revolution
- Offline vs Online environment
- Sensors
- Smart Devices
- Movement of crime

SOCIAL MEDIA & OSINT

- Open Source Information
- Social media attacks
- Social Intelligence
- Cyber Hygiene
- Profiling
- Reconnaissance as a first step



YOUR DIGITAL TATTOO



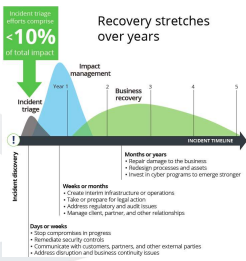

Incident Impact - Real

Cyberattack impact factors:

- **Technical investigation**
- **Customer breach notification**
- **Regulatory compliance**
- **Attorney fees and litigation**
- **Post-breach customer protection**
- **Public relations**
- **Cybersecurity improvements**






But also:

- **Insurance premium increases**
- **Increased costs to raise debt**
- **Impact of operational disruption**
- **Value of lost contract revenue**
- **Devaluation of trade name**
- **Loss of intellectual property**
- **Lost value of customer relationship**


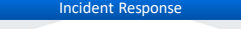








PATH TO CYBER RESILIENCE

- Regulations & Legislation
 - POPIA
 - Cybercrime Bill
 - GDPR
- Standards & Frameworks
 - ISO27001/27002
 - NIST
- Intelligence
- Policies & Procedures







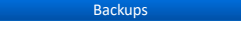






14

CYBER RESILIENCE: TOOLS & TECHNIQUES

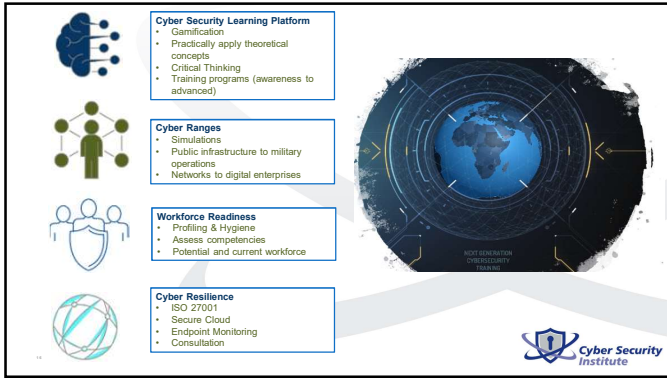


15

CYBER RESILIENCE: TOOLS & TECHNIQUES



16



Cyber Security Learning Platform

- Gamification
- Practically apply theoretical concepts
- Critical Thinking
- Training programs (awareness to advanced)

Cyber Ranges

- Simulations
- Public infrastructure to military operations
- Networks to digital enterprises


Workforce Readiness

- Profiling & Hygiene
- Assess competencies
- Potential and current workforce

Cyber Resilience

- ISO 27001
- Secure Cloud
- Endpoint Monitoring
- Consultation

Next Generation Cyber Security Institute



Power is in the hands of those who control information

Prof. Elmarie Biermann
Elmarie@cybersecurityinstitute.co.za

Justin Westcott
justin@cybersecurityinstitute.co.za