Designing Robustness and Resilience in Digital Investigations

Dr. Philipp Amann, MSc
Dr. Joshua I. James

DFRWS EU 2015
25 March 2015
Overview

• What triggered the research?

• How did we do it?

• Key findings & recommendations

• Europol’s EC3 – ‘Walking the walk’

• Q & A
Challenges...

• Complex and changing requirements, and rapid technological advancements

• Increasing volume, scope and sophistication of cybercrime & global scope – CaaS

• Criminal abuse of legitimate services providing anonymity and privacy

• ...
Challenges...

• Attribution

• Access to and admissibility of electronic evidence

• Cross-border cooperation

• Acquiring and retaining skills and expertise

• Staff turnover and ‘knowledge drain’

• ...

[Image 0x451 to 720x540]
[Image 558x-4 to 702x67]
Taking a step back...

• How can LE conduct digital investigations effectively and efficiently?

• In LE, what is the role of robustness and resilience when it comes to digital investigations?

• What are the key elements in the context of a digital investigation framework design that can withstand changes but also adapt in a controlled/planned manner?
Some definitions...

• Resilience – long-term capacity to adapt to change and new risk environments, and develop within certain boundaries

• Approach to addressing unexpected events but also a practice that aims at actively monitoring relevant factors and managing any deviations

• Includes monitoring, situational awareness and forward-looking analysis as key practices
Some definitions...

- Robustness – the ability resist change
- Important to ensure that the basic principles of police work are maintained while adapting to a changing environment
- Not all that can be done should be done (?)
Objectives

- Surveying and analysing the current state of robustness and resilience practices
- Extracting key elements of robustness and resilience
- Describing how to include these elements when designing digital investigation capabilities
Approach

- Literature research

- Structured online survey – 35 closed and open questions – 72 recipients (LEAs), 21 responses ~ 29% response rate

- Stakeholder interviews
Does your agency have a digital forensics strategy?
**Main standards or guidelines used in digital forensics?**

<table>
<thead>
<tr>
<th>Organization/Group</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>RITS Computer Forensics group</td>
<td>1</td>
</tr>
<tr>
<td>International Organization for Standardization (ISO)</td>
<td>3</td>
</tr>
<tr>
<td>Council of Europe (Budapest Convention, Electronic Evidence Guide)</td>
<td>4</td>
</tr>
<tr>
<td>National Institute of Standards and Technology (NIST)</td>
<td>4</td>
</tr>
<tr>
<td>International Association of Computer Investigative Specialists (IACIS)</td>
<td>5</td>
</tr>
<tr>
<td>Association of Chief Police Officers (ACPO)</td>
<td>7</td>
</tr>
<tr>
<td>Developed in-house</td>
<td>13</td>
</tr>
</tbody>
</table>
Training and Education

**Continuous digital forensics education/training plan in place?**
- No: 33.3%
- Yes: 66.7%

**Use of e-learning to train digital forensics staff?**
- No: 52.0%
- Yes: 48.0%

**Personal development portfolio for staff?**
- No: 47.6%
- Yes: 42.4%
Training and Education (cont’d)

- **Mentoring system in place?**
  - No: 19.0%
  - Yes: 81.0%

- **Hand-over between outgoing and incoming digital forensics staff?**
  - No: 85.7%
  - Yes: 14.3%

- **Further education and training considered during performance evaluations?**
  - No: 52.0%
  - Yes: 48.0%
Key findings & Recommendations

Do you use a reporting standard (incidents, case description, final reports, etc.)?

- Yes: 66.7%
- No: 33.3%
Key findings & Recommendations

Tool Support

Do you use standardized digital forensics tools?

- No: 38.9%
- Yes: 61.1%

Do you use open-source digital forensics tools?

- No: 33.6%
- Yes: 66.4%
Do you have a Quality Management System in place?
Do you have a Knowledge Management Program in place?

- No: 84.2%
- Yes: 15.8%
Are the digital forensics software tools that your agency uses ‘court-approved’?
Key findings & Recommendations

Co-operation and PPPs

Co-operation with academia?
- Yes: 76.2%
- No: 23.8%

Co-operation with the private sector?
- Yes: 57.1%
- No: 42.9%
Key findings & Recommendations

Do you have a digital forensics R&D unit?

- No: 71.4%
- Yes: 28.6%
Key findings & Recommendations

Average staff turnover

Digital forensic examiners

Digital forensic investigators
Key findings & Recommendations

How would you rate your agency’s robustness and resilience? (1 – Lowest 5 – Highest)

- Five: 0.0%
- Four: 33.3%
- Three: 42.9%
- Two: 4.8%
- One: 19.0%
Greatest challenges in conducting digital investigations?

- Tool Support: 2.5%
- Co-operation (Industry and/or Academia): 6.3%
- Staff Turnover: 7.5%
- Backlog of Cases: 10.0%
- Investigations of new Forms of Digital Crimes: 12.5%
- Budget: 20.0%
- Training and Education: 20.0%
- Number of qualified staff: 21.3%
Key findings & Recommendations

**Strategic Level**
- Digital Forensics Strategy
- Standardization
- Forensic Discipline
- Continuous Education and Training
- Research and Development
- Co-operation

**Operational Level**
- Standardization
- Continuous Education and Training
- Research and Development
- Co-operation
- Human Resources
Future Research

- Development of additional KPIs
- Digital forensics framework
EC3 – Who We Are and What We Do

European Cybercrime Centre
EC3 Core Services

**European cybercrime info/intel focal point**

**Support to Member States' cybercrime investigations**

**Platform to pool skills and expertise & tool support for MS**

**Collective voice of European cybercrime investigators**

**OPERATIONAL**

- Coordination of High Profile Operations
- On-the-Spot Operational Support
- Operational, Technical and Forensic Analysis
- Digital IT Forensics Support

**STRATEGIC**

- Digital Forensics and R&D
- Outreach to Public/Private Partners
- Strategic and Forward Looking Assessments
- Training and capacity building
EC3 Intelligence/Knowledge Products

**CYBER-INTEL**

- **Cyber Bits**
  - **Trends:** Modus operandi, tool or technique used by cyber criminals. Emerging patterns and crime series.
  - **Knowledge:** Offer guidance and raise awareness.
  - **Technology:** Technical developments having impact law enforcement work.
  - **Tools:** Presentation of tailored tools to support operational activities.

- **OSINT Dashboard**

- **Strategic Assessments of Operations**

**STRATEGY**

- **iOCTA**

- **Project 2020: Scenarios for the Future of Cybercrime**

- **Police Ransomware Threat Assessment, Review of Criminal Forums, etc.**

- **Strategic Assessments of Operations (e.g. Onymous)**

- **Quantitative Quarterly Report on Cybercrime, CC Dependencies Map**

- **ICANN Guide for Dummies, Assessment of Bitcoin, Top 10 External Cyber Threats, etc.**
EC3 Projects, Products and Services

• Taxonomy and business case for the exchange of information/intelligence between LE and CERTs

• Anonymized cross-matching solution

• Design of standardized EU-wide training and capacity building measures (ECTEG, UCD, CEPOL,…) – Training Competency Framework

• Prevention and awareness
EC3 Projects, Products and Services

• Active stakeholder management, cross-domain and cross-disciplinary (e.g. EC3AAN)

• EC3 Training Courses (Avila, Selm)

• Position papers on legislative issues

• Research and Development

• Malware analysis, Decryption, …
Thank you
philipp.amann@europol.europa.eu