EUROPEAN CYBERCRIME CENTRE

EC3

EUROPOL

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

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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**
- **…**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Challenges...

- **Attribution**
- **Access to and admissibility of electronic evidence**
- **Cross-border cooperation**
- **Acquiring and retaining skills and expertise**
- **Staff turnover and 'knowledge drain'**
- **...**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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?**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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 (?)**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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**

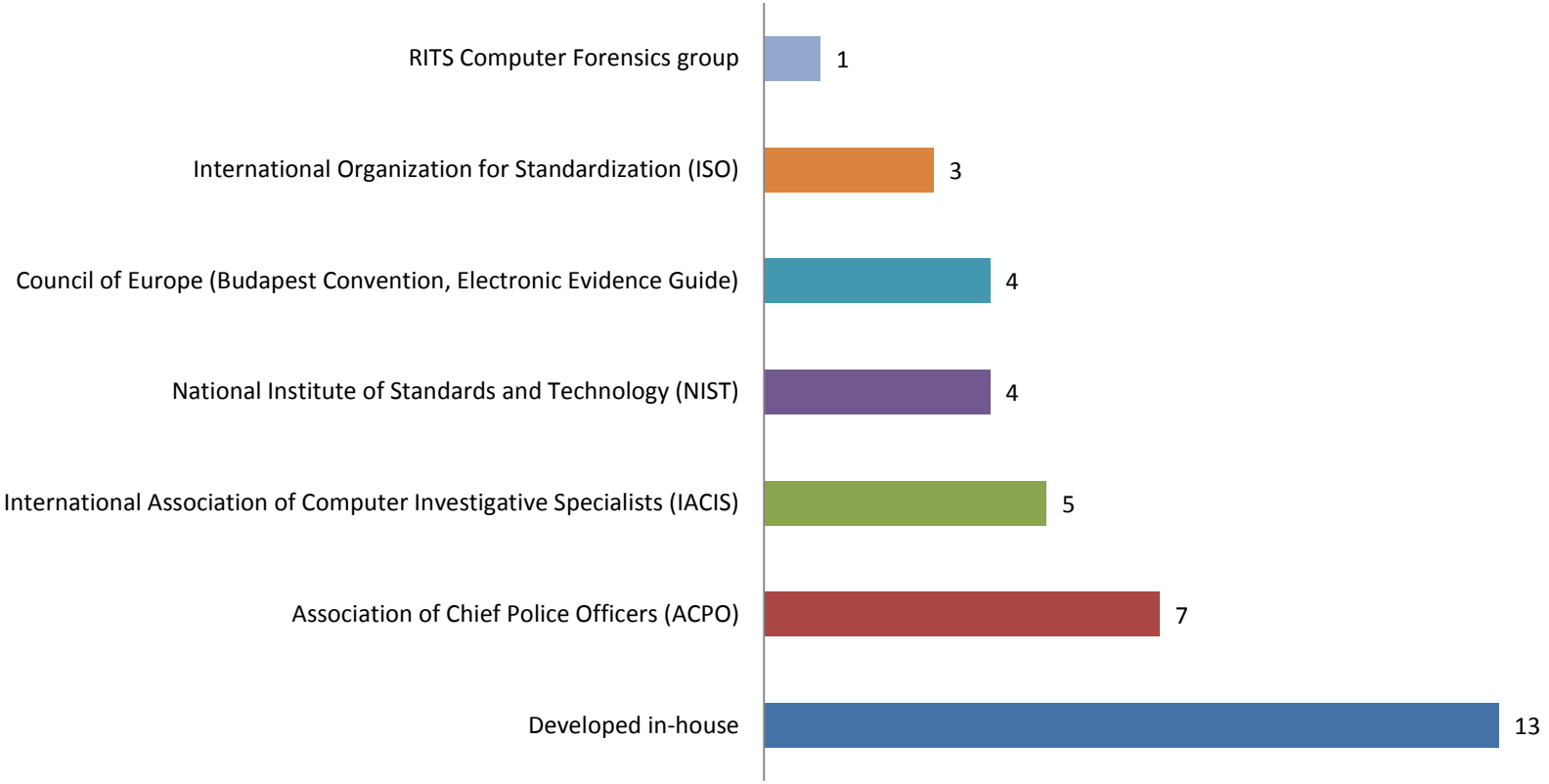
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

Does your agency have a digital forensics strategy?

Key findings & Recommendations

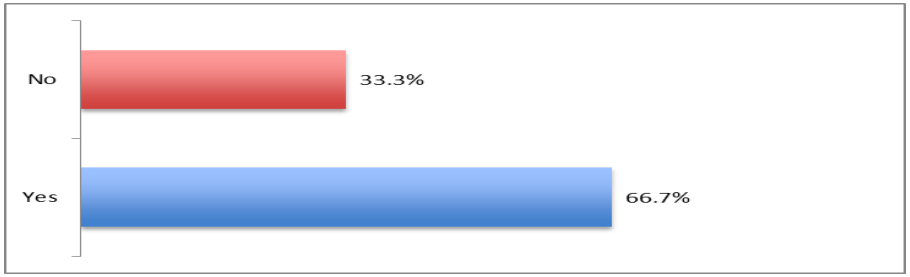
Main standards or guidelines used in digital forensics?



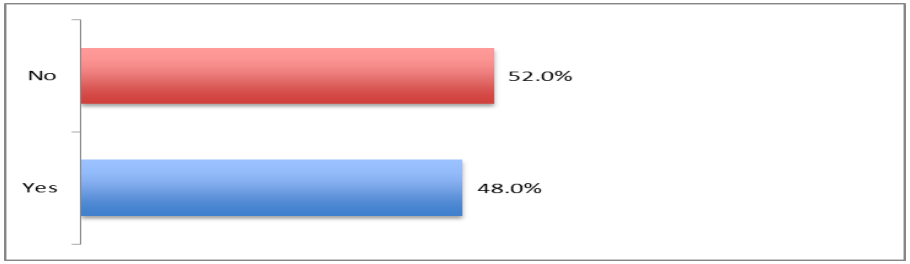
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

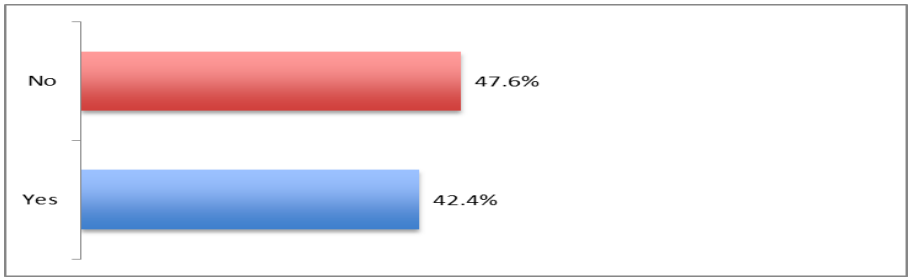
Training and Education



Continuous digital forensics education/training plan in place?



Use of e-learning to train digital forensics staff?



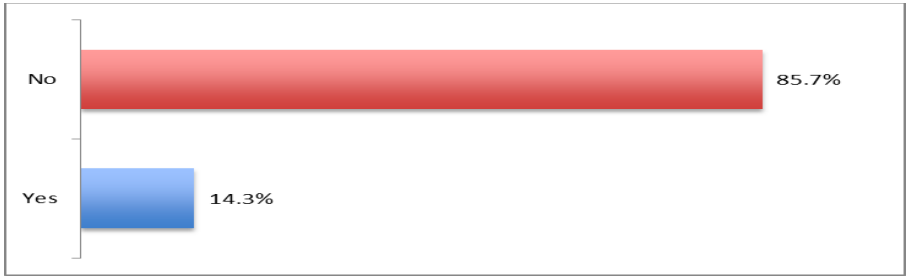
Personal development portfolio for staff?

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

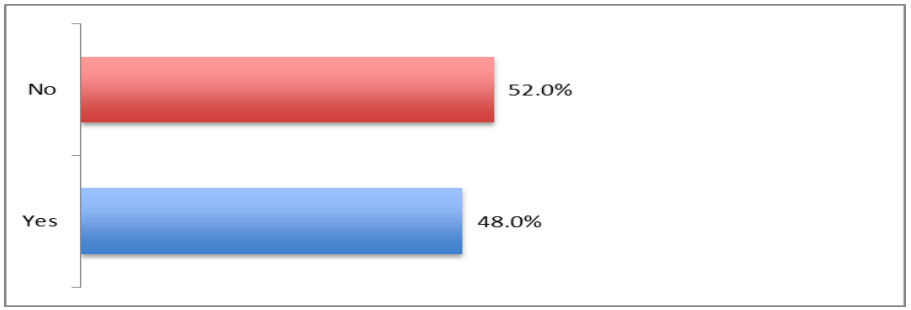
Key findings & Recommendations

Training and Education (cont'd)

Mentoring system in place?



Hand-over between outgoing and incoming digital forensics staff?

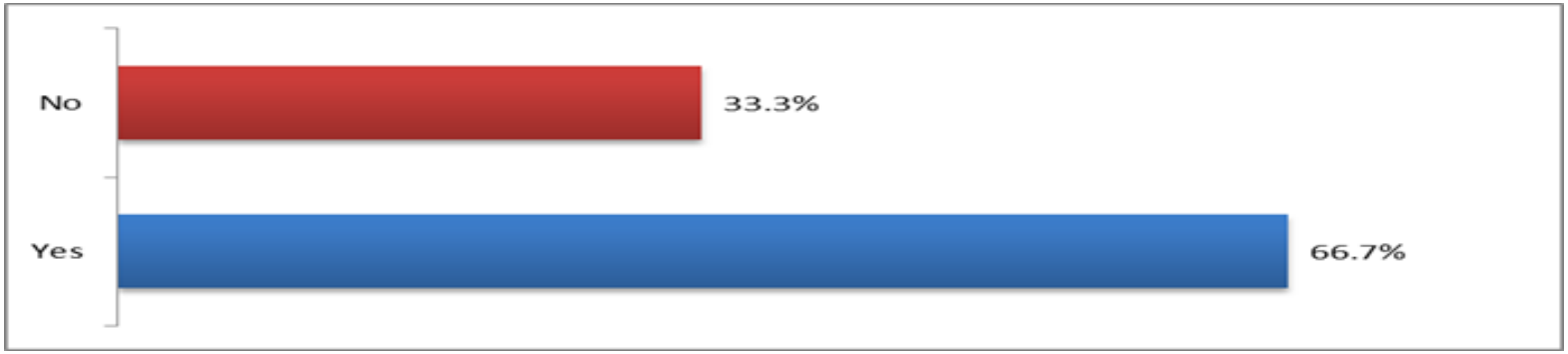


Further education and training considered during performance evaluations?

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

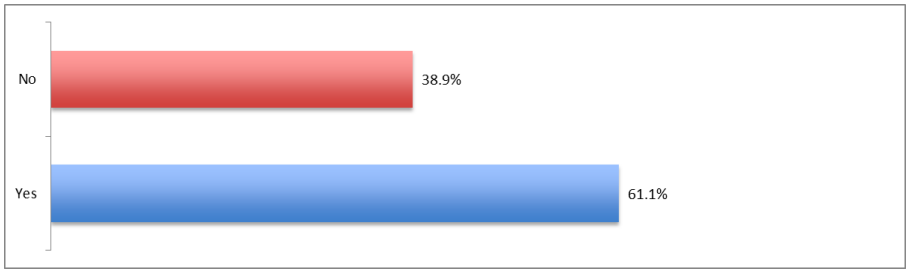
Do you use a reporting standard (incidents, case description, final reports, etc.)?



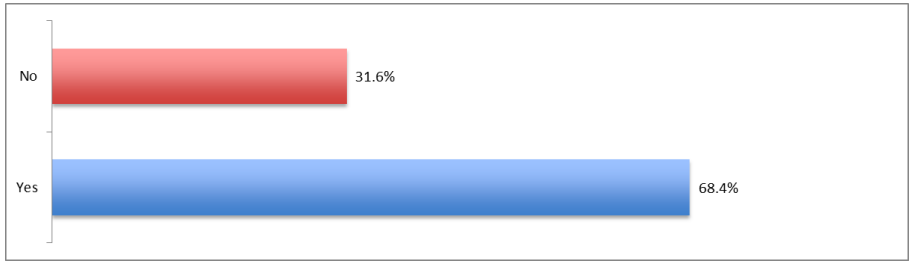
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

Tool Support



Do you use standardized digital forensics tools?

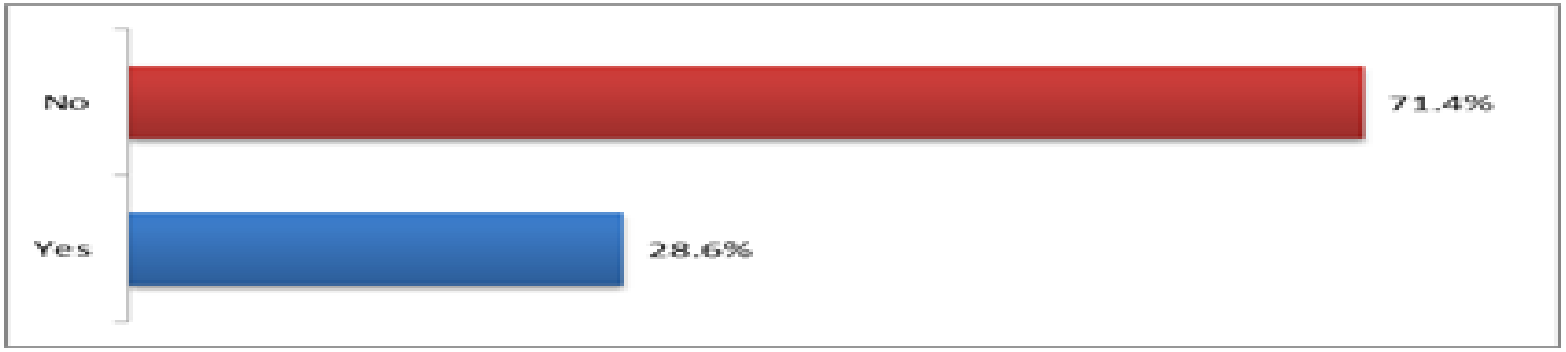


Do you use open-source digital forensics tools?

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

Do you have a Quality Management System in place?



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

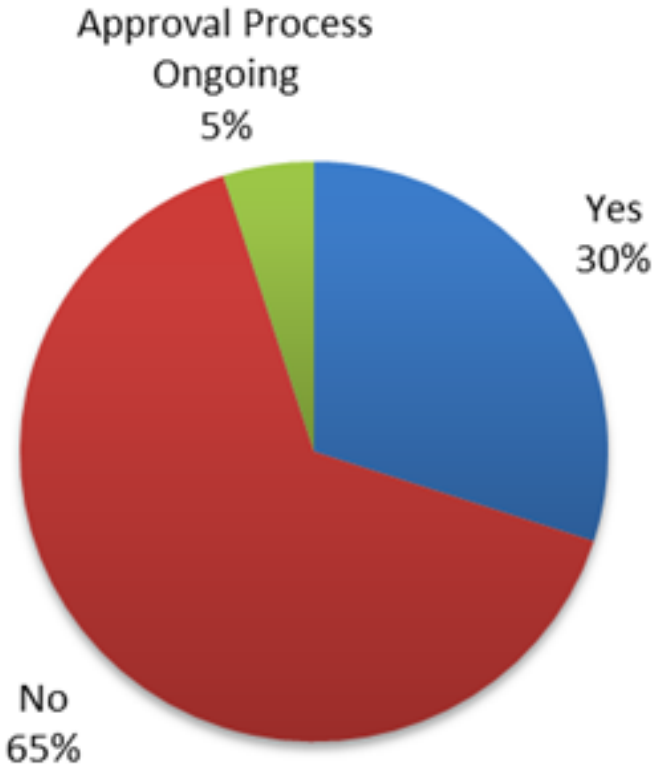
Key findings & Recommendations

Do you have a Knowledge Management Program in place?

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

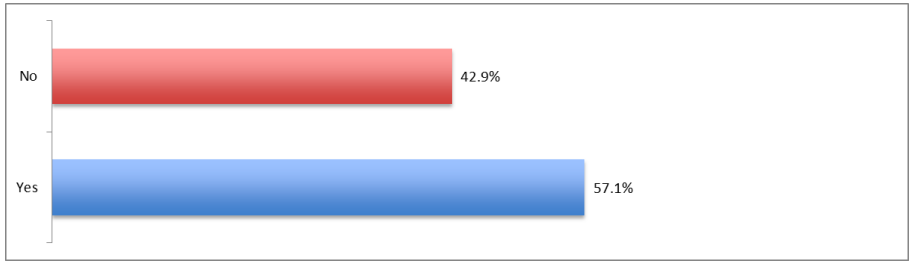
Are the digital forensics software tools that your agency uses 'court-approved'?



Key findings & Recommendations

Co-operation and PPPs

Co-operation with academia?

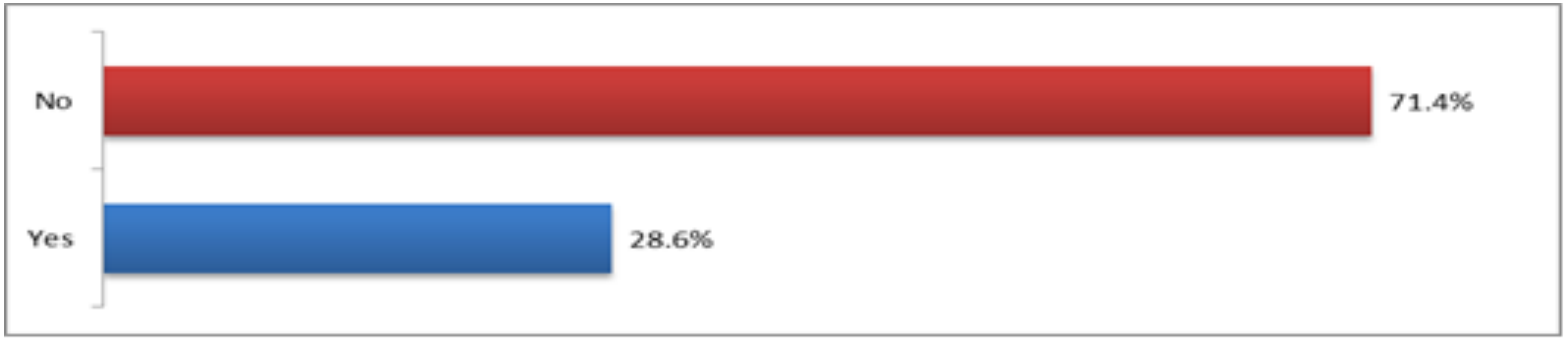


Co-operation with the private sector?

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

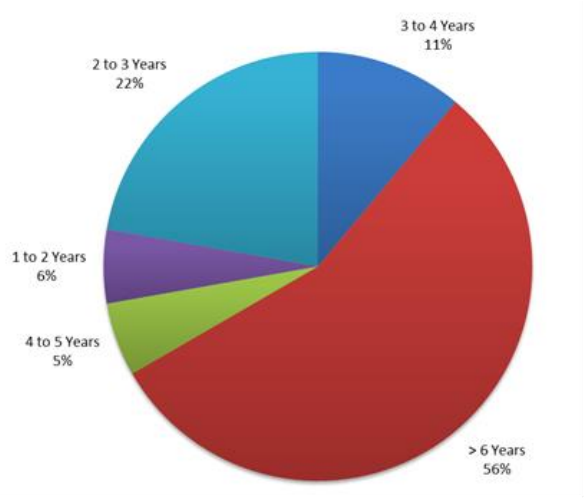
Do you have a digital forensics R&D unit?



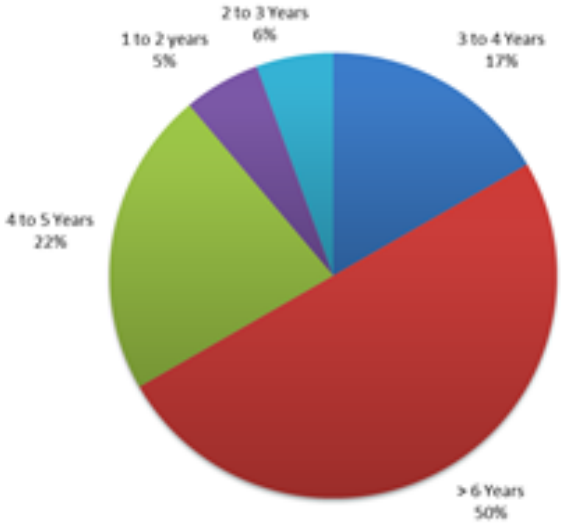
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

Average staff turnover



Digital forensic examiners

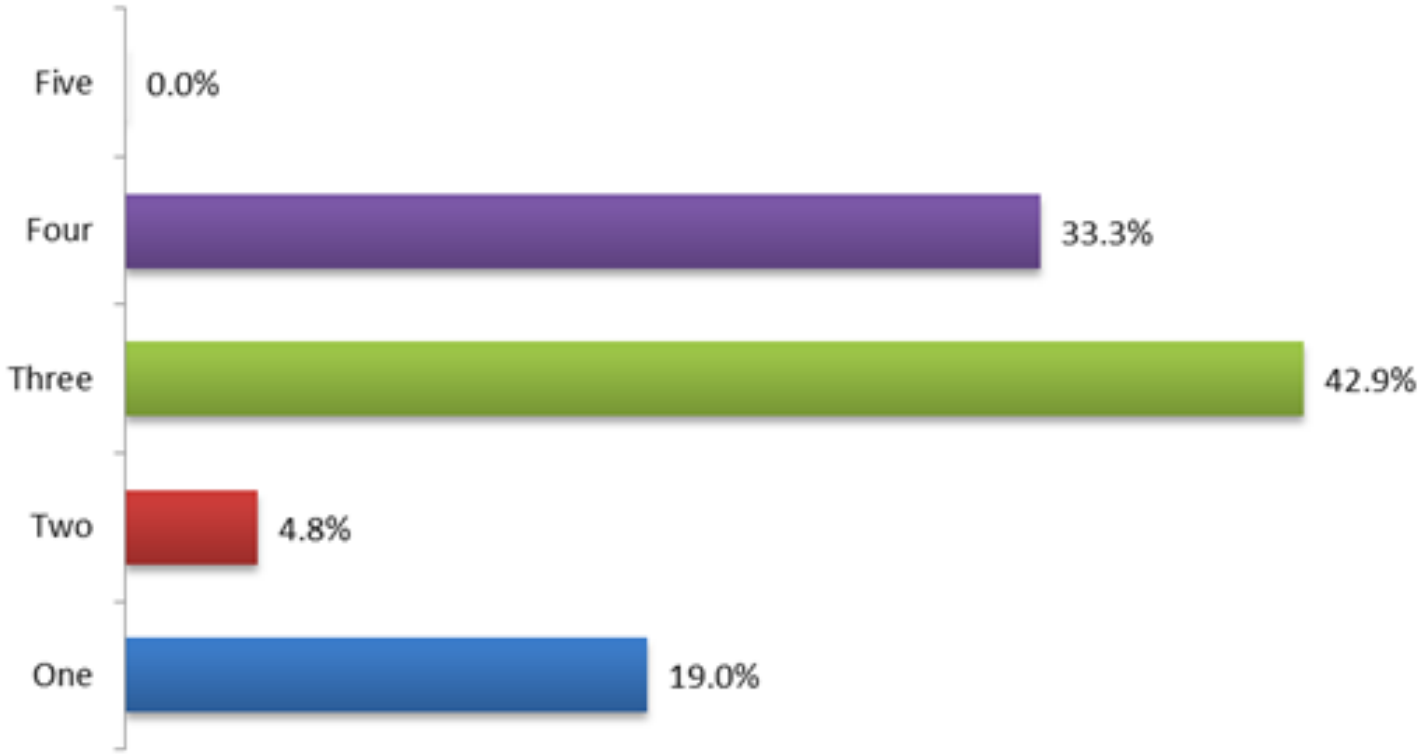


Digital forensic investigators

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

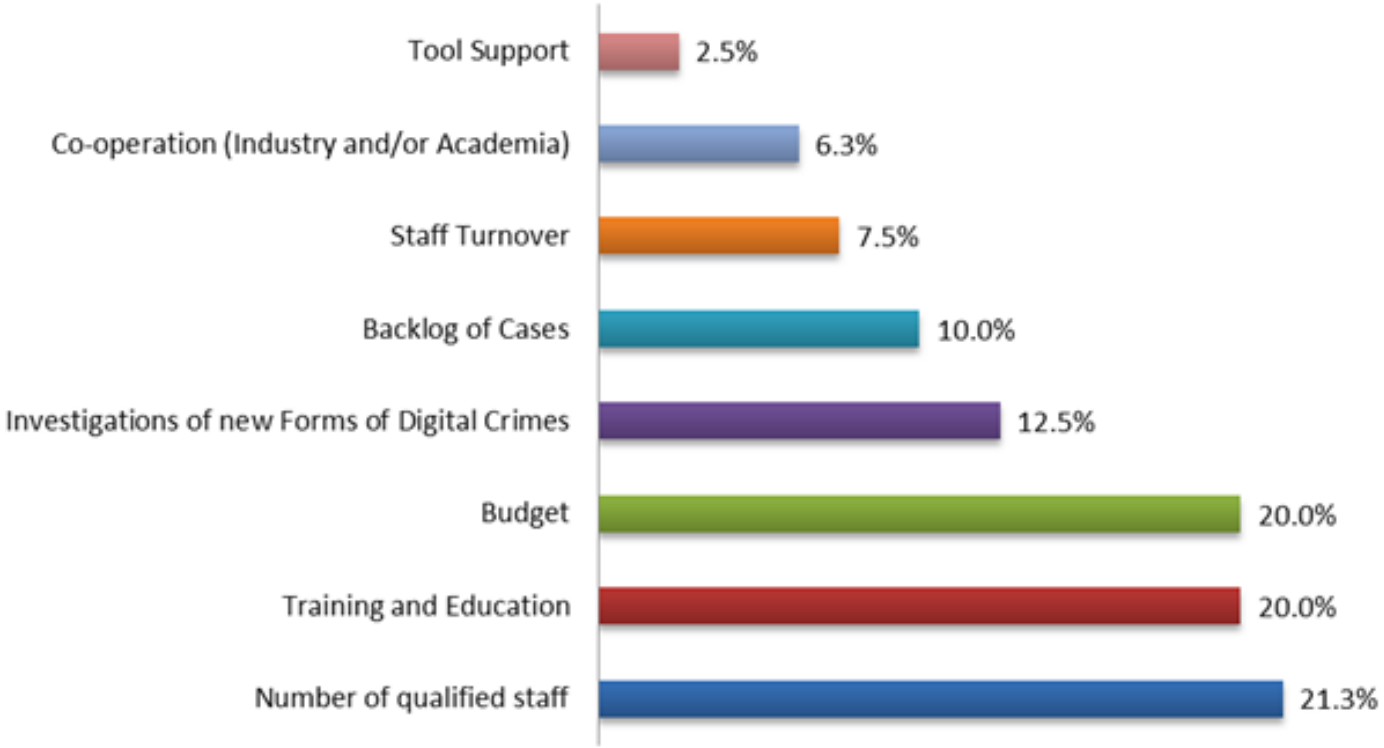
How would you rate your agency's robustness and resilience? (1 – Lowest 5 – Highest)



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Key findings & Recommendations

Greatest challenges in conducting digital investigations?



EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Future Research

- **Development of additional KPIs**
- **Digital forensics framework**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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

EUROPEAN CYBERCRIME CENTRE EC3 EUROPOL

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.**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

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, …**

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

Thank you

philipp.amann@europol.europa.eu