Digital Forensics

Thursday, 19th May 2016

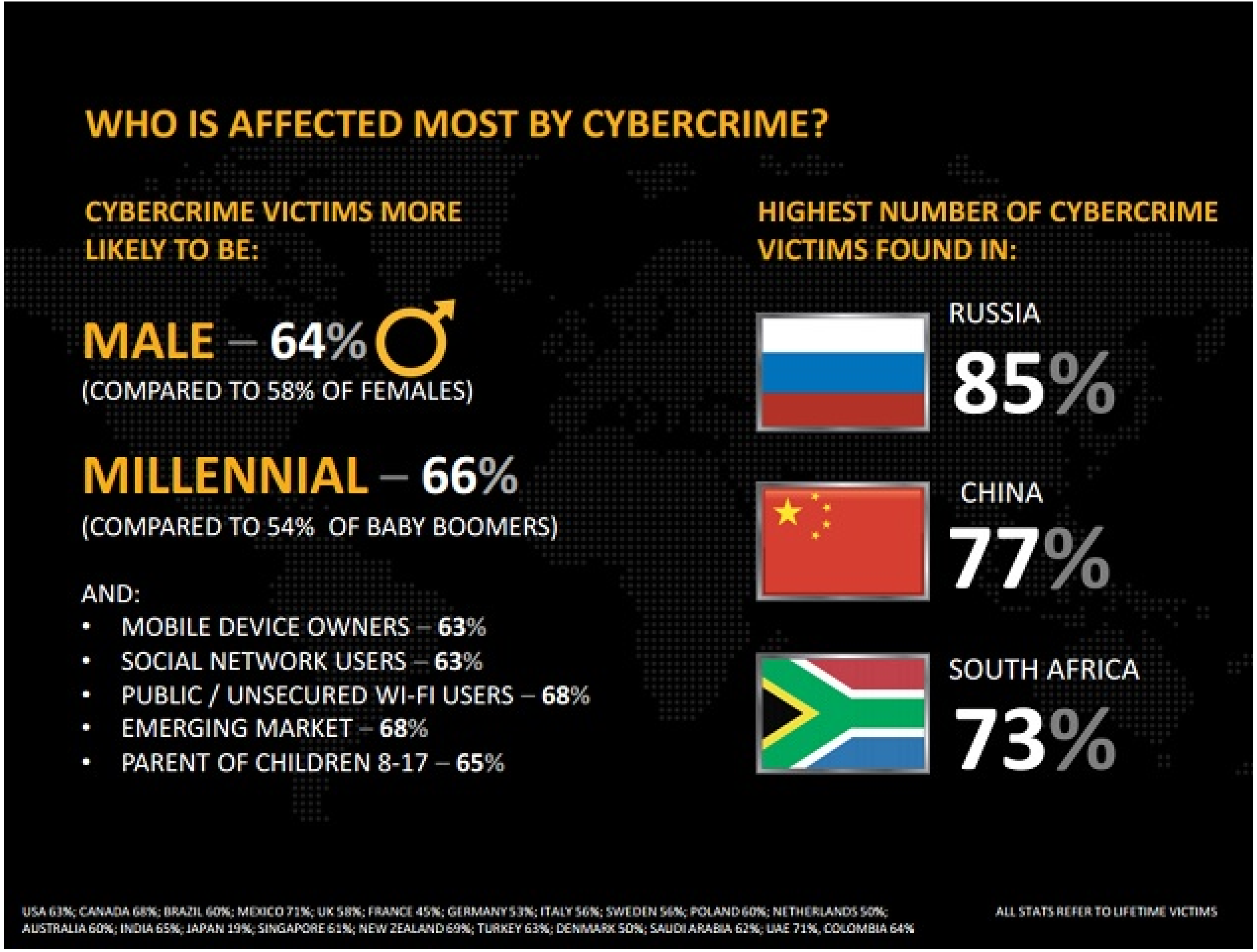
Roshan Harneker
roshan.harneker@uct.ac.za

ToC

- The cost of cybercrime
- A definition of Digital Forensics (DF)
- Importance of DF
- What can DF be used for?
- What is digital evidence
- Main DF areas
- Cloud Forensics
- DF Readiness
- Potential digital evidence sources
- Industry best practice
- Obstacles to obtaining digital evidence
- Legal and regulatory requirements
- Internal corporate demand
- Organisational challenges
- DF tools and skills

https://www.pilumdefense.com/digital-forensics-qa-session/

The cost of cybercrime



WHO IS AFFECTED MOST BY CYBERCRIME?

CYBERCRIME VICTIMS MORE LIKELY TO BE:

MALE – 64% ♂
(COMPARED TO 58% OF FEMALES)

MILLENNIAL – 66%
(COMPARED TO 54% OF BABY BOOMERS)

AND:

- MOBILE DEVICE OWNERS – 63%
- SOCIAL NETWORK USERS – 63%
- PUBLIC / UNSECURED WI-FI USERS – 68%
- EMERGING MARKET – 68%
- PARENT OF CHILDREN 8-17 – 65%

HIGHEST NUMBER OF CYBERCRIME VICTIMS FOUND IN:

RUSSIA 85%

CHINA 77%

SOUTH AFRICA 73%

USA 63%; CANADA 68%; BRAZIL 60%; MEXICO 71%; UK 58%; FRANCE 45%; GERMANY 53%; ITALY 56%; SWEDEN 56%; POLAND 60%; NETHERLANDS 50%; AUSTRALIA 60%; INDIA 65%; JAPAN 19%; SINGAPORE 61%; NEW ZEALAND 69%; TURKEY 63%; DENMARK 50%; SAUDI ARABIA 62%; UAE 71%, COLOMBIA 64%

ALL STATS REFER TO LIFETIME VICTIMS

http://www.pcmag.com/article2/0,2817,2425118,00.asp

- SA ranked 3rd in Norton Report
- Costs SA an estimated R5.8 billion annually

Digital Forensics – a definition

- The discovery and preservation of evidence in a digital format for proof of criminal behaviour and ultimately prosecution of criminal activity.
- Acquisition and scientific examination and analysis of data from computing devices in a manner allowing information to be used for a court of law.

Importance of DF

- Important tool for solving crimes committed with computers (*e.g.* phishing and bank fraud)
- Solving crimes where evidence may reside on a computer (*e.g.* money laundering and child exploitation)
- Forensic tools have also become a vital tool for Information Assurance because of their ability to reconstruct the evidence left by cyber attacks.

What can DF be used for?

- The collection, preservation, analysis, and presentation of digital evidence
- Admissible in a court of law
- Usable for disciplinary hearings
- Supporting data for internal incident reports

What is digital evidence?

In a DF context, it is data which:

- Helps reconstruct a time line of past events or activities
- Shows possession and/or handling of digital data
- Shows use/abuse of IT infrastructure & IT services
- Shows evidence of policy violation or illegal activity

Main areas of DF

- Computer forensics
- Network forensics
- Software forensics
- Live system forensics
- Mobile forensics
- Cloud forensics
- Forensic data analysis
- Database forensics

Cloud Forensics Considerations

- Can you collect the data yourself?
- Which laws and jurisdictions will apply?
- Can the disclosure of detail be compelled?
  - Preservation letters / litigation holds
- Be prepared for incidents

DF Readiness

- ability of an organisation to maximise potential to use digital evidence while minimising cost of an investigation
- achievement of an appropriate level of capability by an organization in order for it to be able to collect, preserve, protect and analyse digital evidence
- Ten Steps of Readiness – Rowlingson

Ten Steps: DF Readiness

1. Define business scenarios that require digital evidence.
2. Identify available sources and different types of potential evidence.
3. Determine evidence collection requirement.
4. Establish capability for securely gathering legally admissible evidence to meet requirement.
5. Establish policy for secure storage and handling of potential evidence.

Ten Steps: DF Readiness

6. Ensure monitoring is targeted to detect and deter major incidents.
7. Specify circumstances when escalation to full formal investigation should be launched.
8. Provide staff with incident awareness training
9. Document evidence-based case describing incident and its impact.
10. Ensure legal review to facilitate action in response to the incident.

Potential digital evidence sources

- Hard disks, tapes, external/removable media
- Network infrastructure logs (Firewall, IDS, proxy, etc.)
- Application, audit log files + email
- server content (shared folders, web servers, databases, etc.)
- Captured network traffic

Industry best practice / standards

- Rowlingson’s 10 steps of DF readiness
- ISO 17799 (2003)
- Information Assurance Advisory Council (IAAC)
  - guidelines for ensuring corporate forensic readiness (http://www.iaac.org.uk/media/1347/iaac-forensic-4th-edition.pdf)
- Published, peer reviewed papers
  - Digital Investigation Journal, International Journal of Digital Forensics & Incident Response (Elsevier) • International Journal of Digital Evidence (IJDE)

Obstacles to obtaining digital evidence

- Evidence is easy to destroy and can be difficult to obtain
  - starting PC updates hundreds of timestamps and modifies many files
  - attaching hard disk or USB stick will modify file system timestamps
  - volatile memory is lost when a machine is powered down
  - network traffic only exists on wire for milliseconds
  - intrusions and attacks may be cleverly devised and disguised
  - anti-forensic activity may prevent collection

Legal and regulatory requirements

- Country/region specific laws
- different countries have own laws and regulations which may require some form of forensic capability or readiness
- Regulated Industries
  - finance, healthcare, insurance, telecoms, etc. may have industry specific requirements
- Applicable to RSA
  - ECT Act, RICA, FICA, CAC Bill

Internal corporate demand

- DF can assist:
  - corporate legal teams with discovery and ensure compliance with local laws and regulations
  - corporate policies and standards compliance (company policies and standards & audit requirements and recommendations
  - HR: firing, termination, employee misconduct, disciplinary action)
  - IP: intellectual property abuse and/or infringement
  - IT: intrusion analysis , investigating IT policy violation, IT infrastructure abuse/misuse, logic bomb, virus/malware analysis, etc.
  - Using forensics for legitimate, but non-forensic purposes viz. verifying corporate disk wiping procedures , verifying disk/network encryption implementation, data recovery, legitimate password recovery requests, assist with obscure troubleshooting, IT architecture and design (provide forensic readiness input/feedback)

Organisational Challenges

- Team placement within the organisation:
  - IT / infosec / legal / compliance / CSIRT / SNOC / NOC / centralised or regional / in-house or outsourced?
- Internal competition/diversity of roles:
  - very large organisations may have multiple investigation teams
  - varying degrees of responsibility/involvement
- Authorisation to conduct investigations:
  - Does your organisation have a policy that ensures DF practitioners/investigators are able to collect and protect potentially sensitive data?
  - NDA signed?
  - Controlled access
- IT data retention policy
  - legal/regulatory requirements
  - IT incident response requirements
  - forensic & investigative recovery requirements

Organisational Challenges

- Establishing Forensics resources
  - trained forensics team
  - properly equipped forensics lab
  - outsourcing partners and/or external experts
- Management support
  - convincing management a forensic team or competency is needed/valuable to the organisation
  - emphasis on readiness
  - preventing even 1 high-cost court case alone could justify expense of such a team
- DF awareness
  - inclusion in work-flows and processes
  - having point of escalation, additional support
  - knowing a DF competence exists

DF tools and skills

- Staff training and skills maintenance
  - knowledge of proper methods and procedures
  - Important to ensure all methods followed are forensically sound and will stand up in a court of law
  - allowing time to learn about and understand new technologies
  - certified examiners (SANS 408 and 508 / GCFE etc.)
- Setting up a DF lab
  - forensics hardware (write blockers)
  - forensics software (commercial and open source)
  - systems for performing acquisition, analysis, and testing
  - old media drives and technologies

Thank You