Forensics in cybercrime cases

What happens to organizations that have to deal with a cyber-attack?

About me

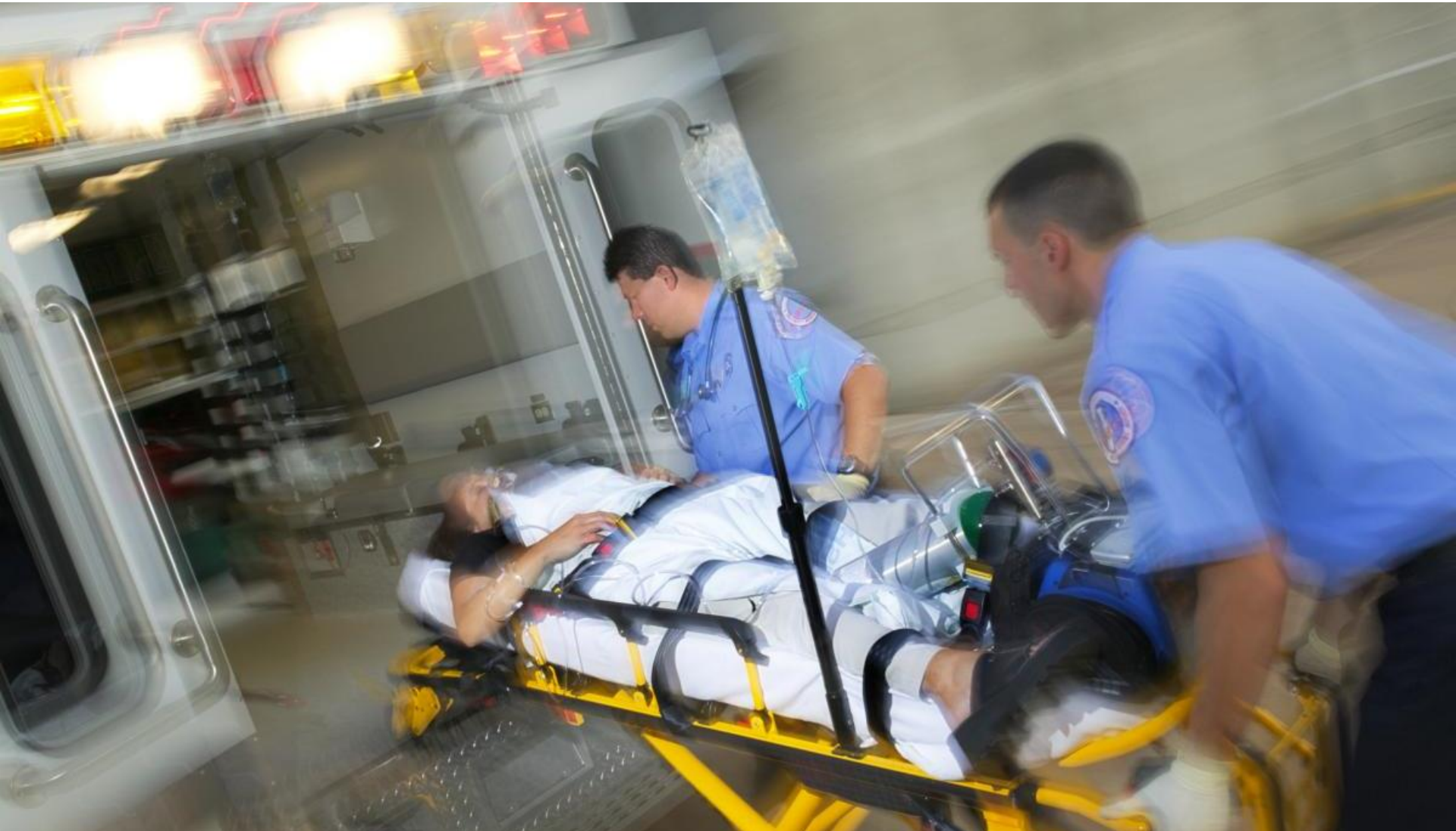
- Christian Prickaerts
  - prickaerts@fox-it.com

- My day job
  - In charge of DFIR @Fox-IT
  - Providing expert witness testimony
  - SANS Institute instructor

Digital forensics 15 years ago

Digital forensics anno 2014

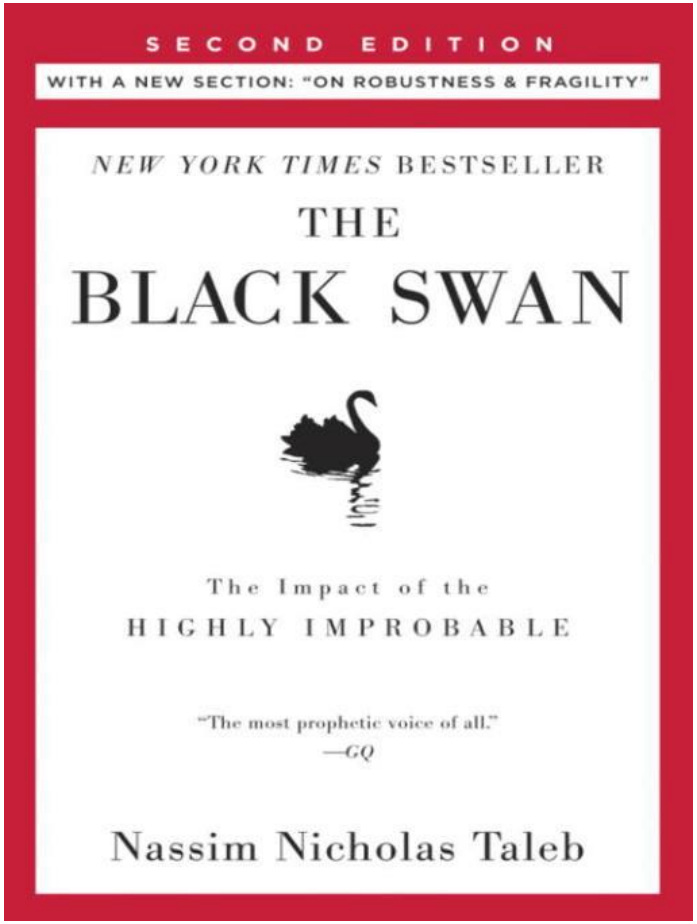
Role of digital forensics in IR?




OUR NETWORK HAS BEEN BREACHED

Black Swan

- High-impact
- Hard-to-predict
- Non-computable
- Psychological biases blinds



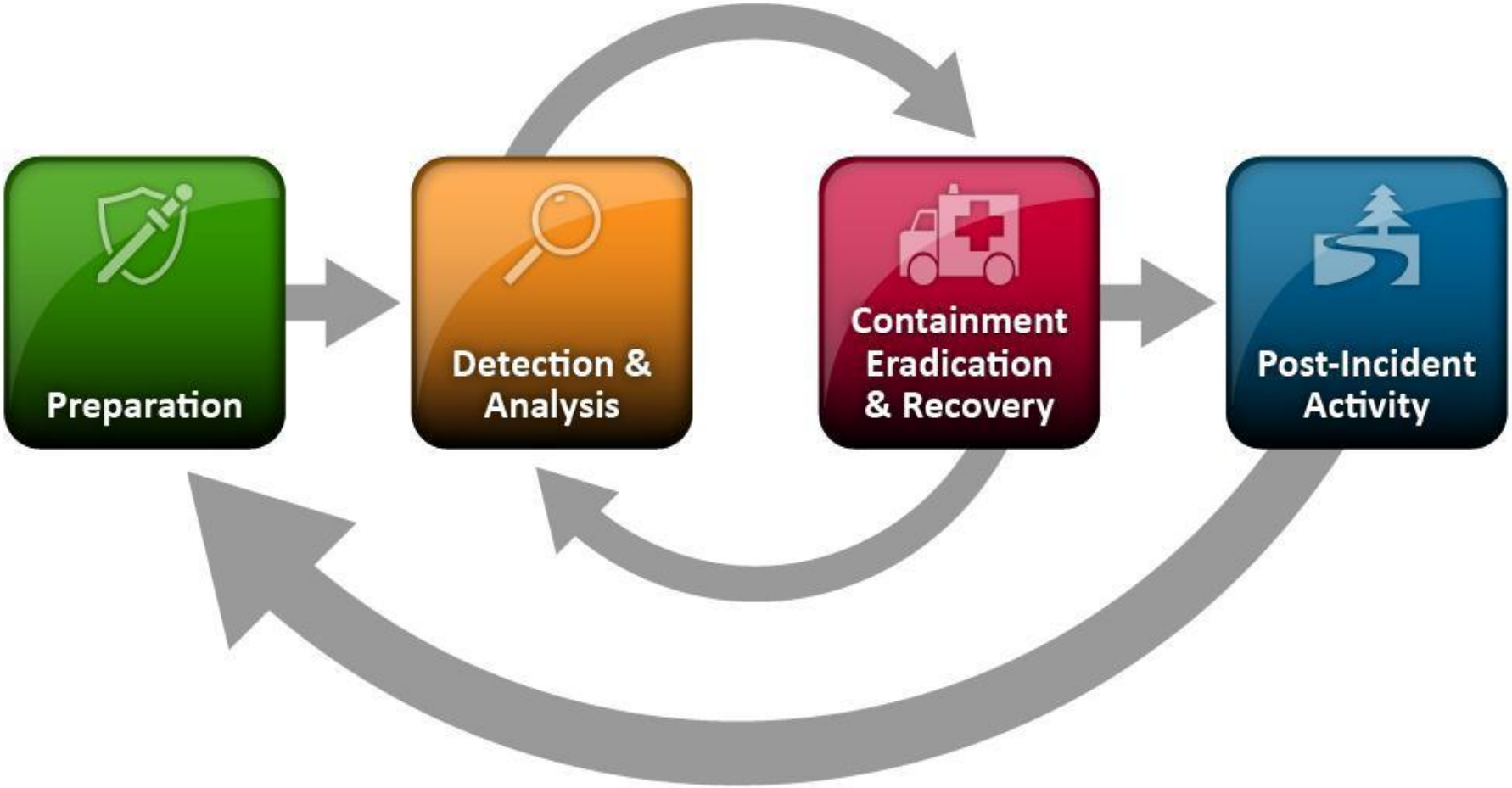

PANIC

Incident Response

- NIST's Computer Security Incident Handling Guide (SP800-61)

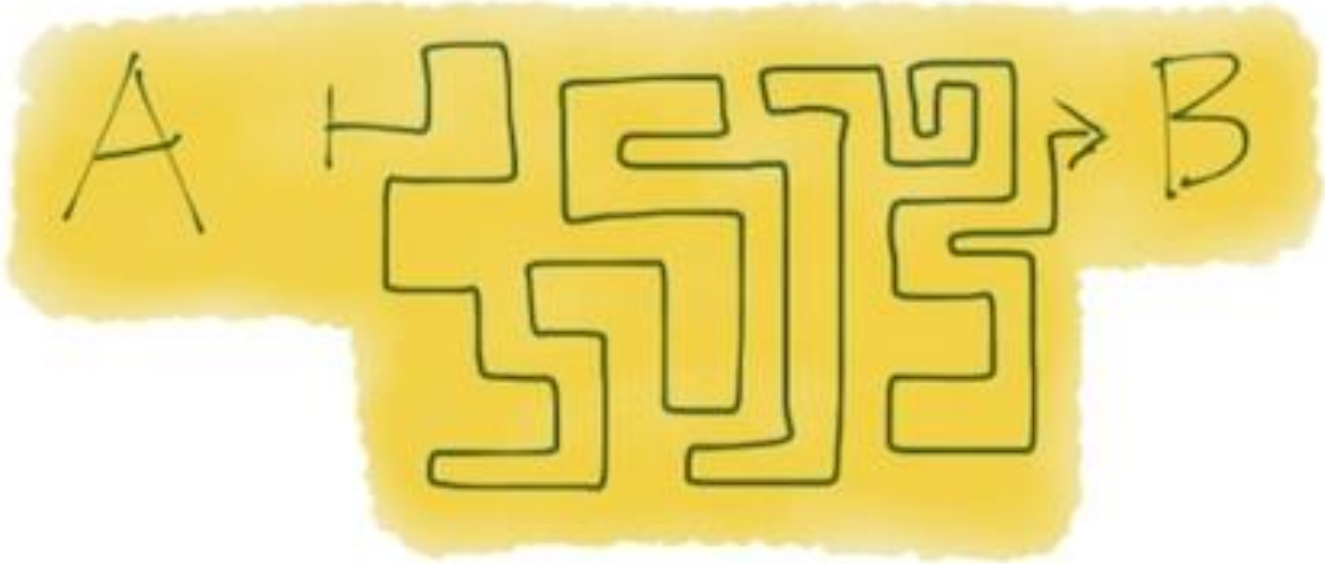
Guide to Integrating Forensic Techniques into Incident Response (SP800-86)

Incident Response lifecycle



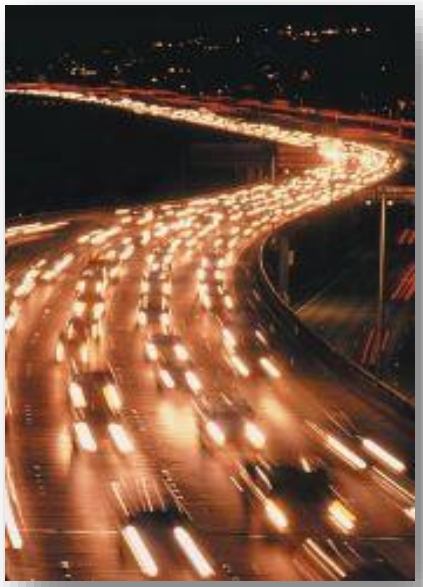
Theory:

Practice:



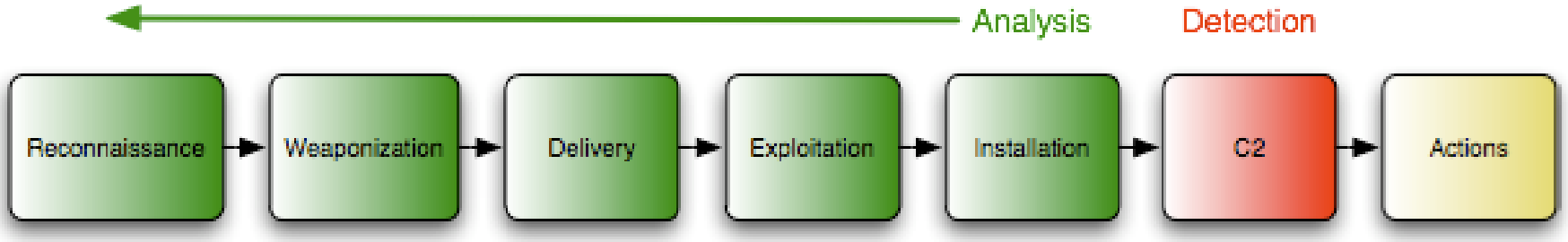
Digital forensics – the challenge

- Digital information is everywhere
  - Computer
  - Mobile devices
  - Network
  - External storage devices
  - Backup tapes
  - The cloud

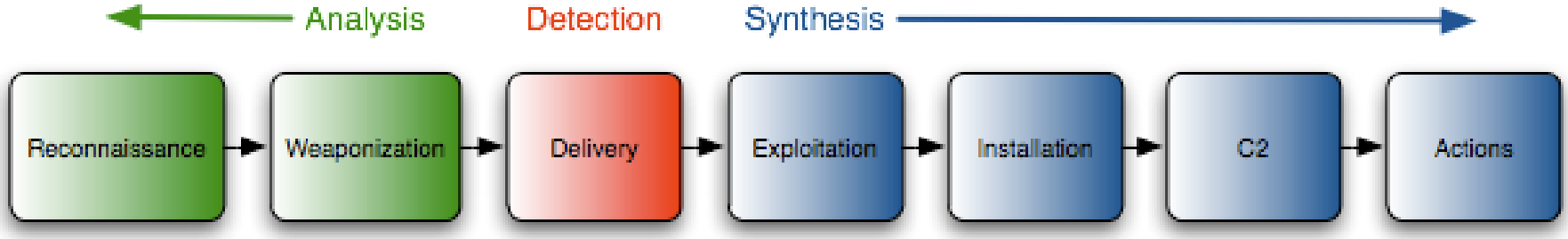


- Increasingly more data in many different formats
- Added challenges: duplicates, malformed data

Security Intelligence



Analysis of successful intrusion



Analysis and synthesis of unsuccessful intrusion

Michael Cloppert, 2009

Use the force

- Imaging all and always is *not* time efficient
- Provide intelligence quickly
  - Perform live forensic analysis
  - Using forensically sound tools
  - Combine
    - Network data
    - File system data
    - Operating system data
    - Application data


Manage your logs

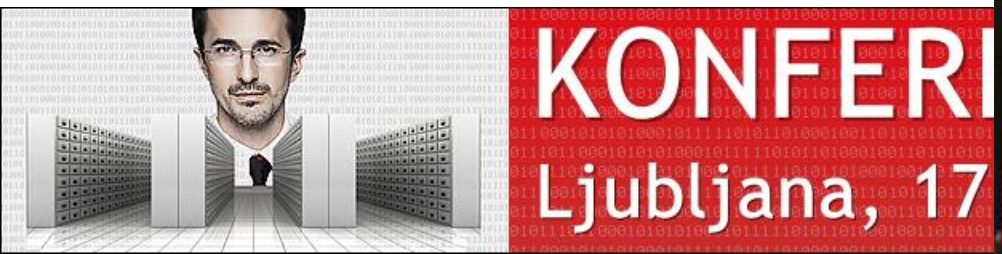
Data in your network

- Log files of network systems:
  - Firewall logs
  - IDS logs
  - VPN logs
  - Proxy logs
  - Active directory logs
  - DHCP logs

- Synchronize systems with central NTP system

A cunning plan.....

“Delete the logs and use a program like CCleaner to destroy possible relevant evidence to frustrate the forensic investigation”

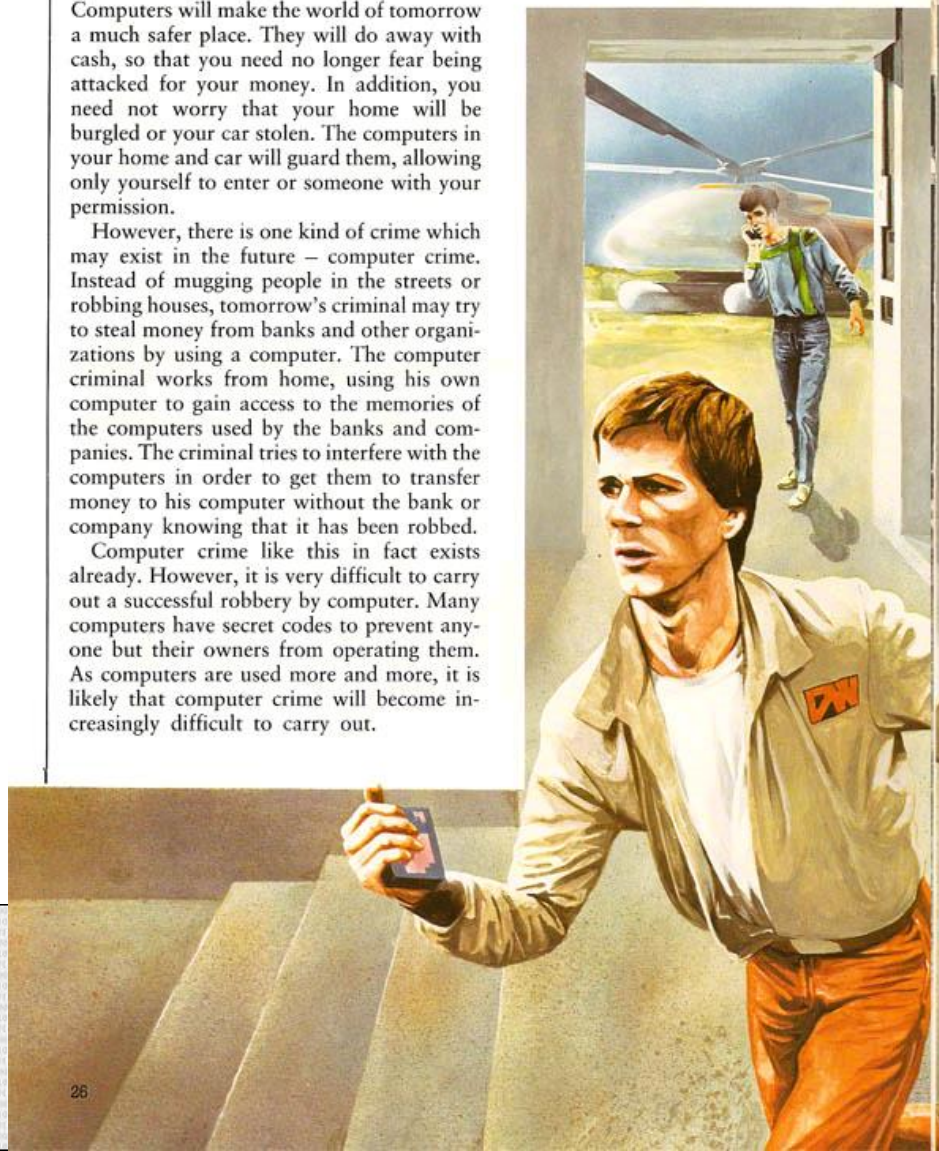


Computer criminals

Computers will make the world of tomorrow a much safer place. They will do away with cash, so that you need no longer fear being attacked for your money. In addition, you need not worry that your home will be burgled or your car stolen. The computers in your home and car will guard them, allowing only yourself to enter or someone with your permission.

However, there is one kind of crime which may exist in the future – computer crime. Instead of mugging people in the streets or robbing houses, tomorrow's criminal may try to steal money from banks and other organizations by using a computer. The computer criminal works from home, using his own computer to gain access to the memories of the computers used by the banks and companies. The criminal tries to interfere with the computers in order to get them to transfer money to his computer without the bank or company knowing that it has been robbed.

Computer crime like this in fact exists already. However, it is very difficult to carry out a successful robbery by computer. Many computers have secret codes to prevent anyone but their owners from operating them. As computers are used more and more, it is likely that computer crime will become increasingly difficult to carry out.



Modus Operandi

Nevertheless, a computer criminal may succeed now and then and the detectives of the future will have to be highly skilled computer operators. There will probably be police computer-fraud squads, specially trained to deal with computer crime. Here you can see a squad arriving at the home of a computer criminal and arresting him as he makes a dash for it. He is clutching a computer cassette that contains details of his computer crimes, and the police will need this as evidence to prove that he is guilty.

Digital forensics in court

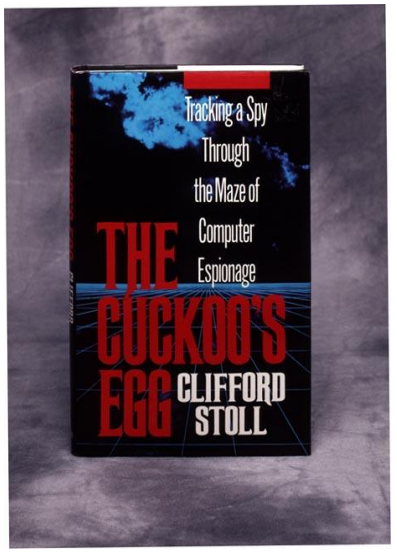
European Commission

- Upcoming (new) data-protection legislation

- Data breach **notification:**
  The drafted rules are similar to rules in relation to providers of public (electronic) communications services

- To be able to notify, one must know

First fully documented digital forensic investigation



- ***The Cuckoo's Egg***
- Written by Clifford Stoll

- The story:
  - Hacker active in defense networks
  - Unix sysadmin investigates the incident
  - Pioneer in digital forensics

Educate your staff

"If you think education is expensive, try ignorance."

Derek Bok, former president of Harvard

"It does not matter how slowly you go as long as you do not stop."

Confucius

FOX IT

Christian Prickaerts

prickaerts@fox-it.com