OWASP
The Open Web Application Security Project

Crime DOES Pay (Unless you get caught)

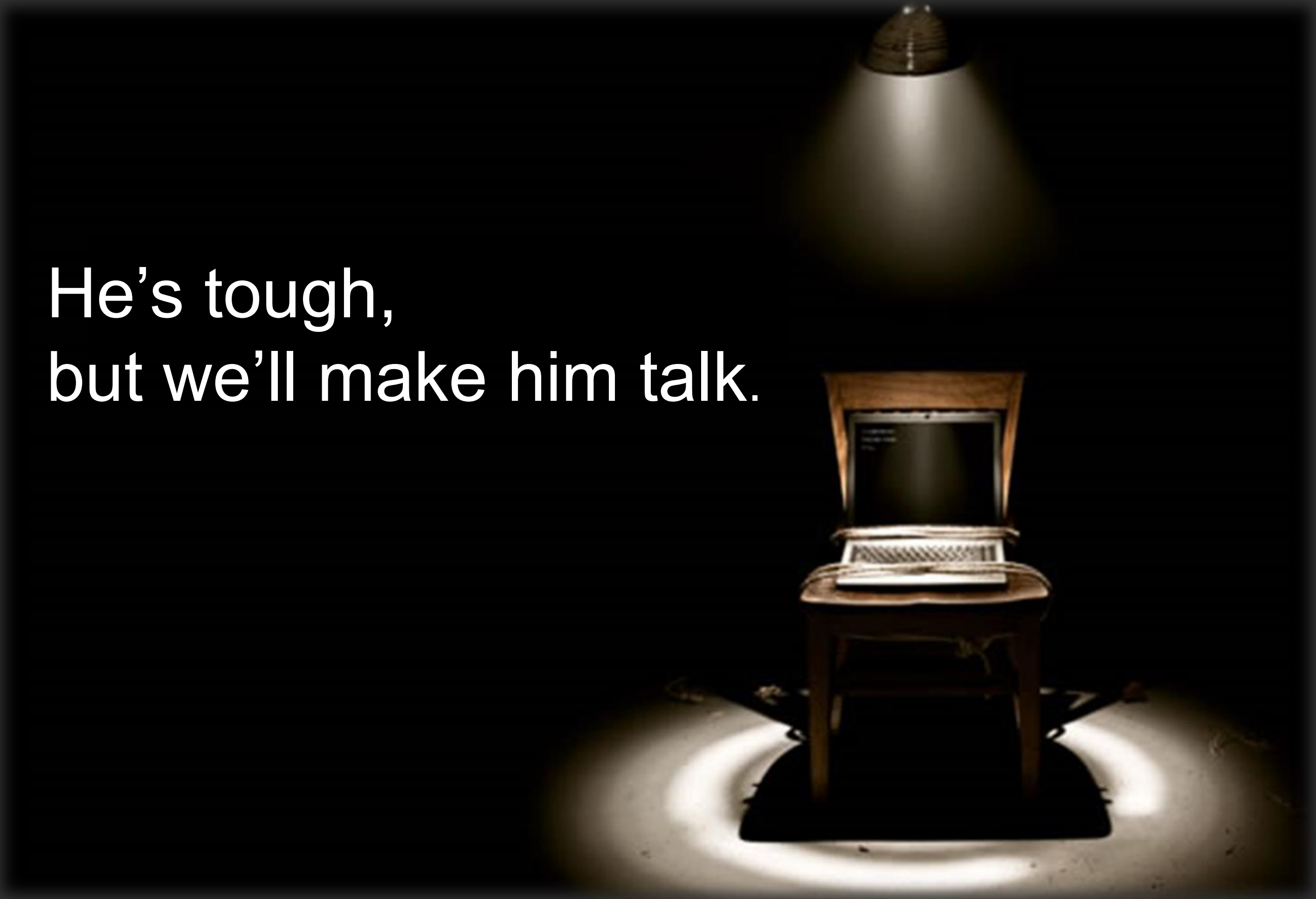
Renana Friedlich, IR & Forensic Team Leader
Hacktics Advanced Security Center,
Ernst & Young
February 2013

ERNST & YOUNG
Quality In Everything We Do

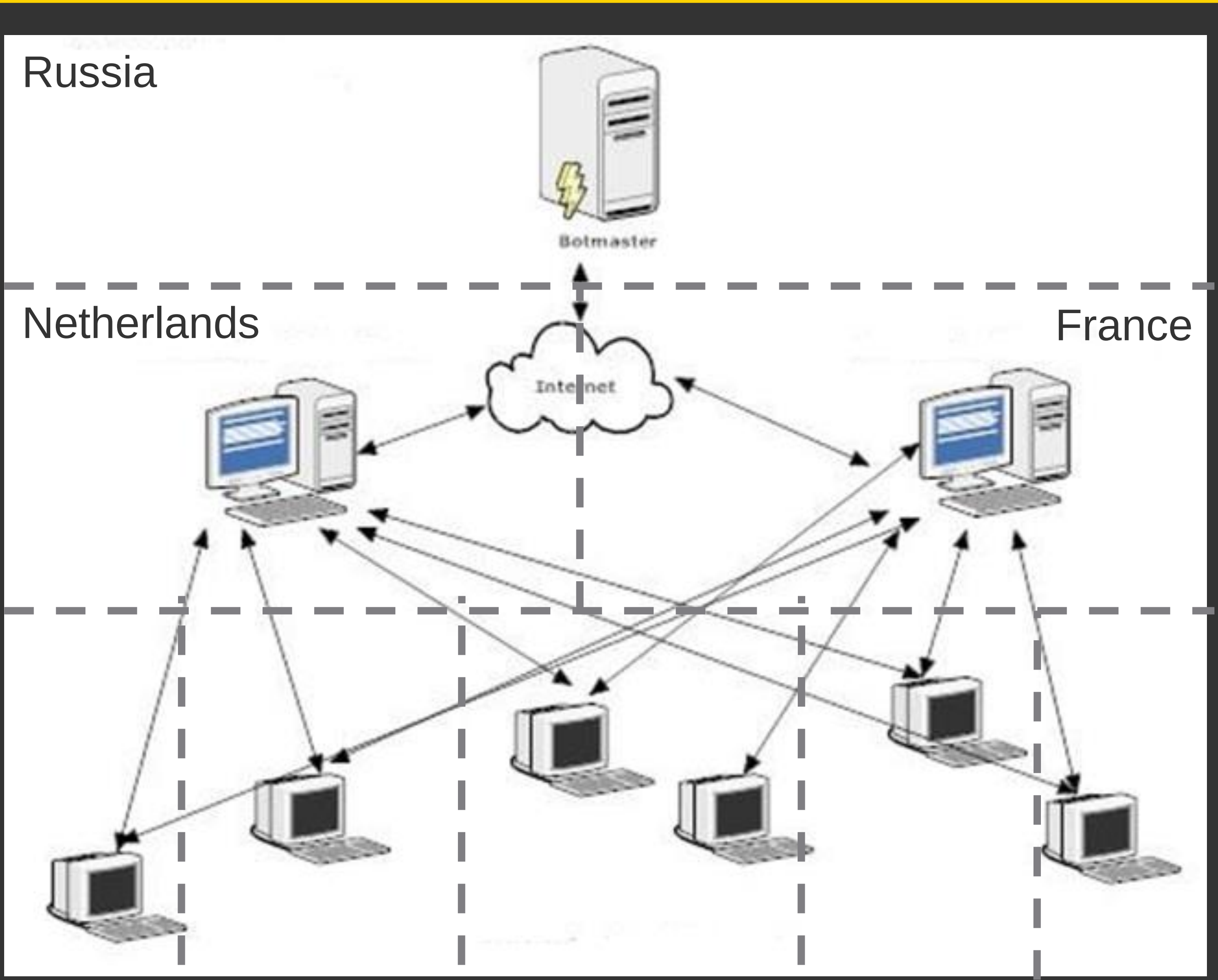
Traditional Forensics

CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS CRIME SCENE DO NOT CROSS

Digital Forensics



Example – Bredolab



Agenda

- Computer Crime Definition
- Crime Detection
- Dealing with an Incident
  - Jurisdiction
  - Punishment
- Case Studies
- Summary and Recommendations

Computer Crime Definition

- What name would best describe this type of offense?
- Is it a new form of crime?

Computer as a target

Computer as a weapon

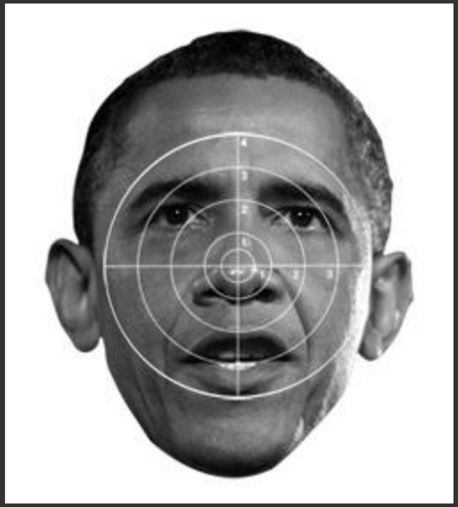
Rising Above the Noise Level

Vectors that may lead to detection:

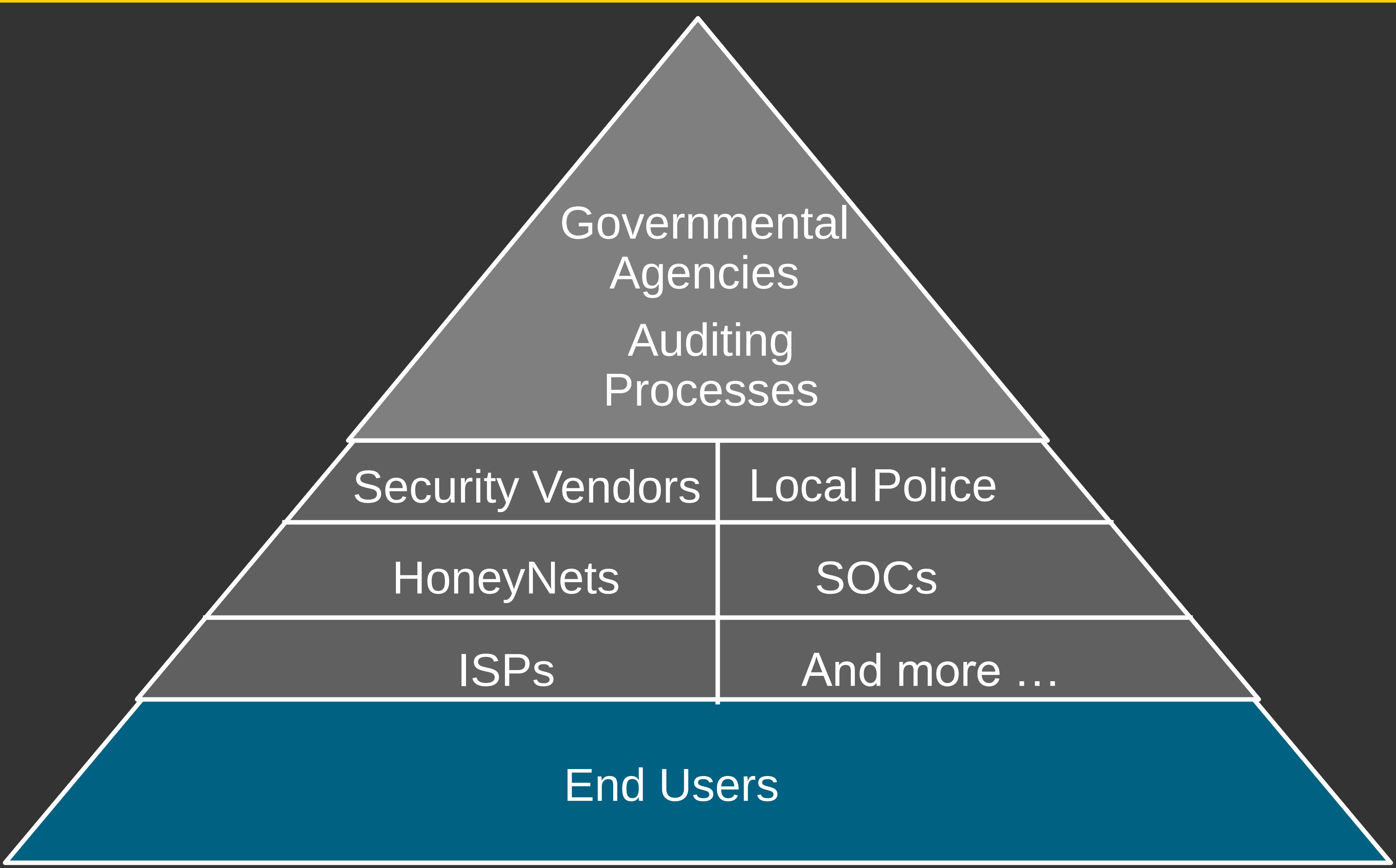
Security systems

Subject of attack

Proportions



Relevant Parties for Detection



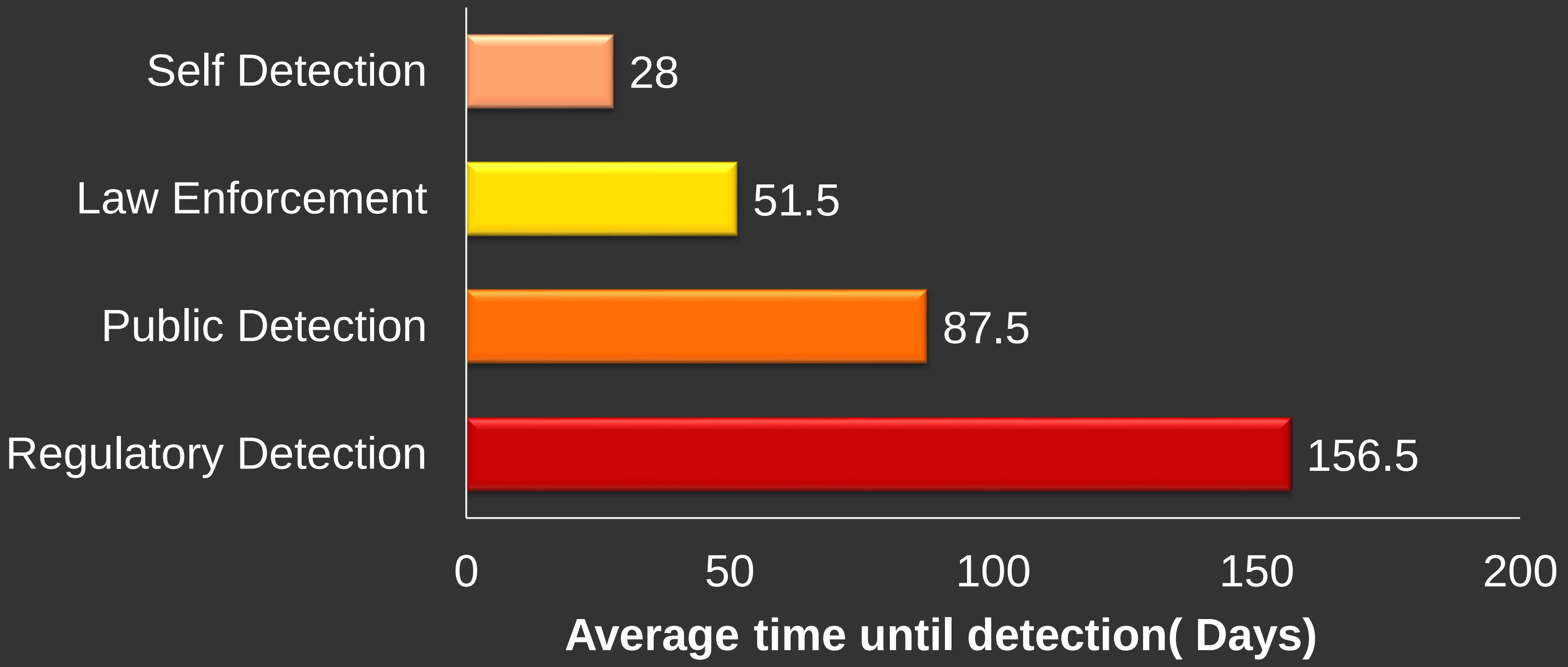
Top 10 Detected Incidents

- Verizon 2012 Data Breach Investigations Report

Rank @ Large Org.	Overall Rank	Attack	Category
1	3	Use of stolen login credentials	Hacking
2	6	Backdoor	Malware
3	7	Exploitation of backdoor C&C channel	Hacking
4	9	Tampering	Physical
5	1	Keylogger/Form-grabber/Spyware	Malware
6	11	Pretexting (classic social engineering)	Social
7	5	Brute force and dictionary attacks	Hacking
8	15	SQL injection	Hacking
9	20	Phishing (or any type of *ishing)	Social
10	22	C&C (listens for and executes commands)	Malware

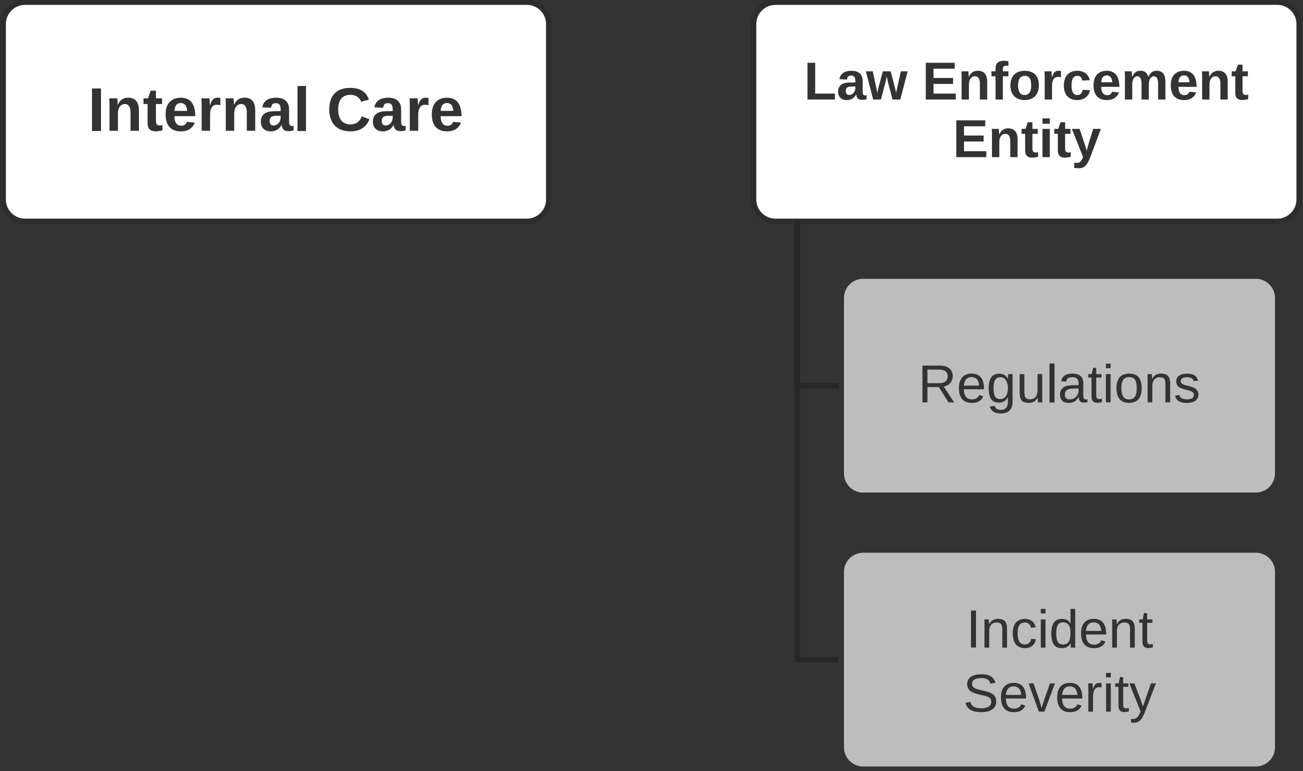
Duration Until the Incident is Discovered

Early detection heavily depends on the organization's security maturity level.

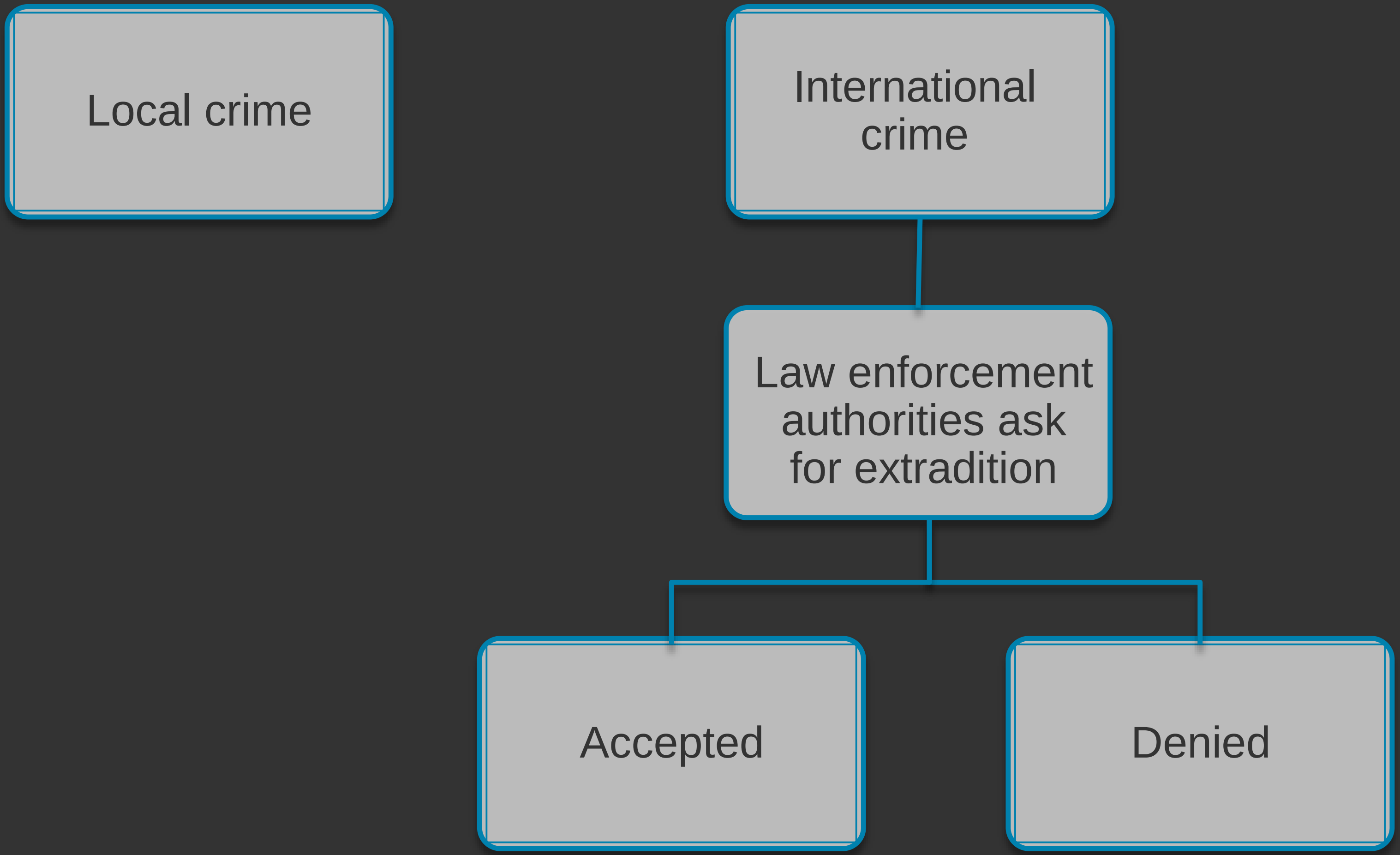


Dealing with an Incident

Common ways of dealing with an incident:



Jurisdiction



Punishment

The penalty usually depends on the following factors:

Financial damage

Current & potential damage

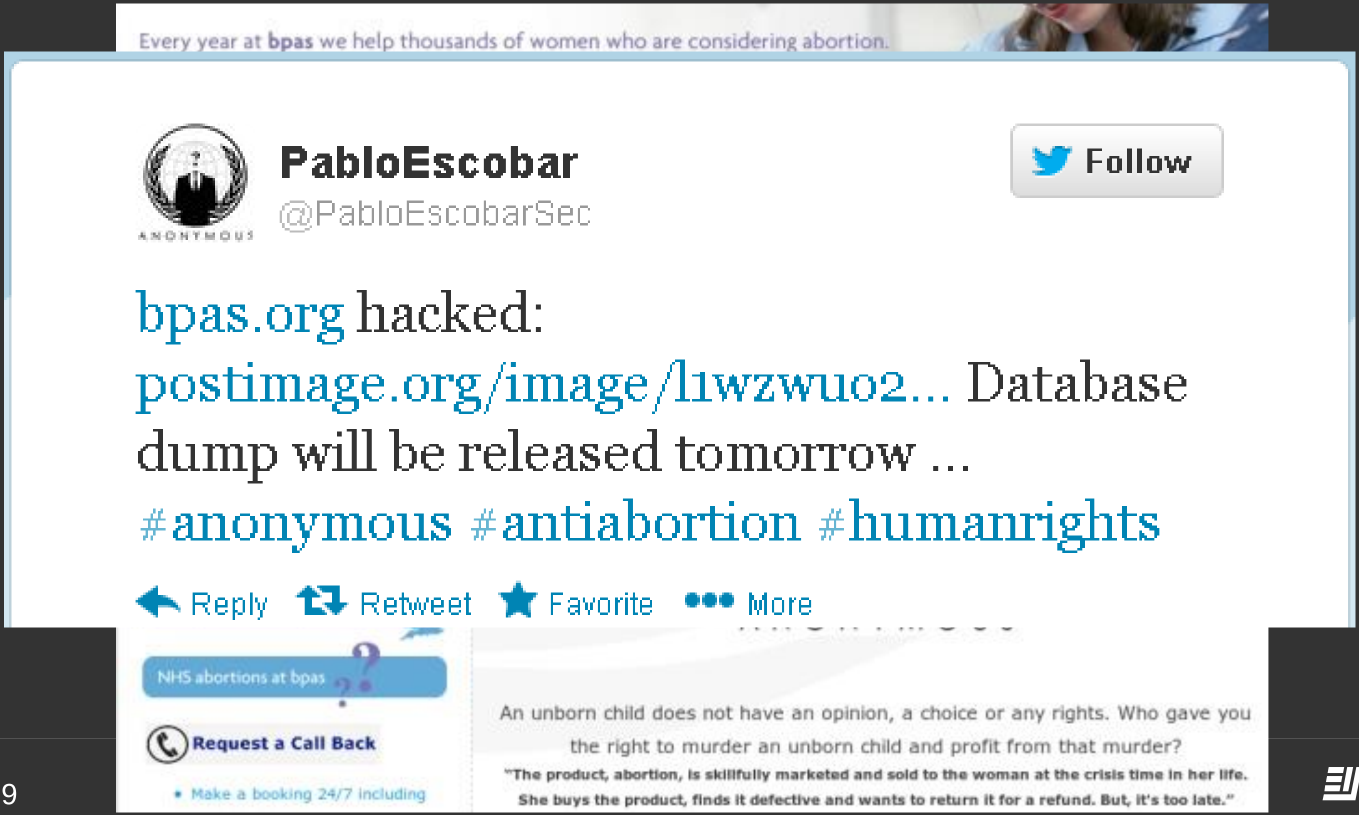
Offender intentions & personal gain

Case Studies

Case Study 1

- ▶ Attacker: Pablo Escobar (James Jeffery)

- ▶ Victim: Abortions website



Every year at bpas we help thousands of women who are considering abortion.

PabloEscobar
@PabloEscobarSec

bpas.org hacked: postimage.org/image/l1wzwu02… Database dump will be released tomorrow … #anonymous #antiabortion #humanrights

An unborn child does not have an opinion, a choice or any rights. Who gave you the right to murder an unborn child and profit from that murder?

"The product, abortion, is skillfully marketed and sold to the woman at the crisis time in her life. She buys the product, finds it defective and wants to return it for a refund. But, it's too late."

Case Study 2

- Attacker: Gary McKinnon

- Victim : USA military computers
  (“**The biggest military computer hack of all time**”)

- The US authorities tried to get an extradition

- Requested penalty: Up to 60 years in prison

Case Study 3

Case Study 3

Take 1

- Age – 19
- Arrested for hacking to computers at NASA, the Pentagon, and more.
- Didn’t try to get a hold of secrets, rather to prove that the systems were flawed.

1.5 years in prison

Take 2

- Age – 28
- Accused with charges of conspiracy and fraud.
- Increased or deleted cards limit, then sold the stolen credit card numbers in the black market.

3 years probation + $503,000 fine

Summary

- The chances of getting caught are slim.
- Even if an offender does get caught, there is a long way to go before he may stand trial.
- Since so “MANY” stand trial, penalty is disproportionate.

And the Conclusion Is …

Crime Does Pay …

Recommendations

Poor	Save logs
Moderate	Continuous log monitoring
Good	Build incident response capabilities

How good is your detection mechanism…?

Ernst & Young

Quality In Everything We Do

Thank you.

Renana Friedlich,
Incident response & forensic team leader
Renana.Friedlich@il.ey.com, 054- 2661260

ERNST & YOUNG
Quality In Everything We Do