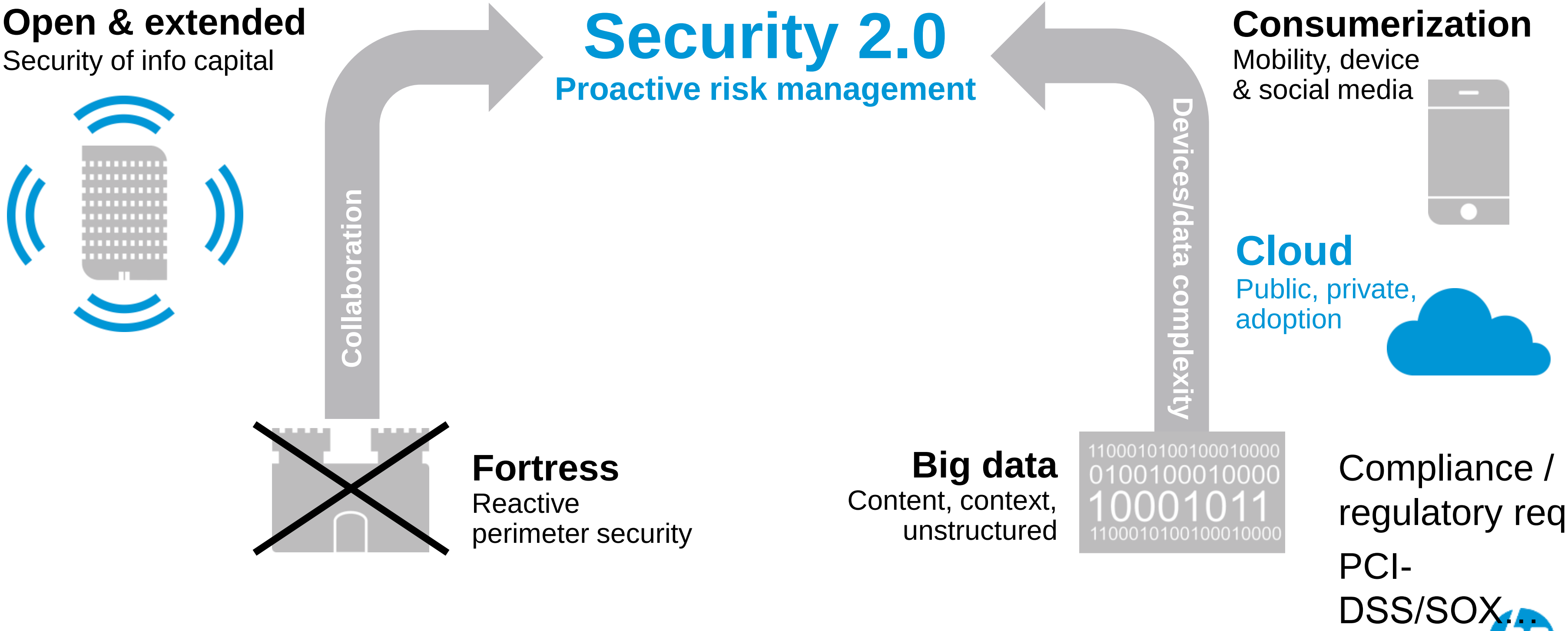
Theory and Practice

Peter Mikeska @ HP.com

2015/05

The security is in everything

90‘s vs Today



Open & extended
Security of info capital

Security 2.0
Proactive risk management

Consumerization
Mobility, device
& social media

Cloud
Public, private,
adoption

Fortress
Reactive
perimeter security

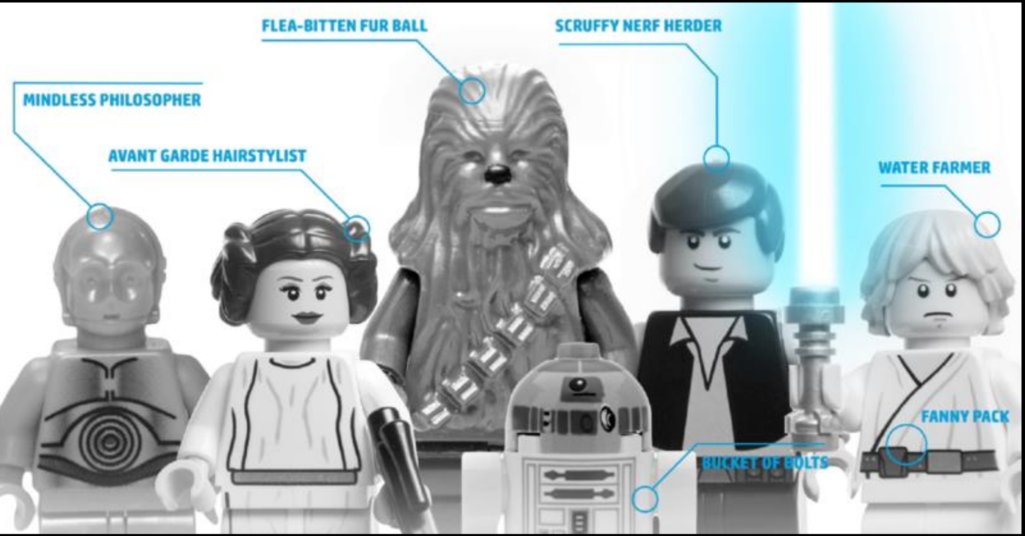
Big data
Content, context,
unstructured

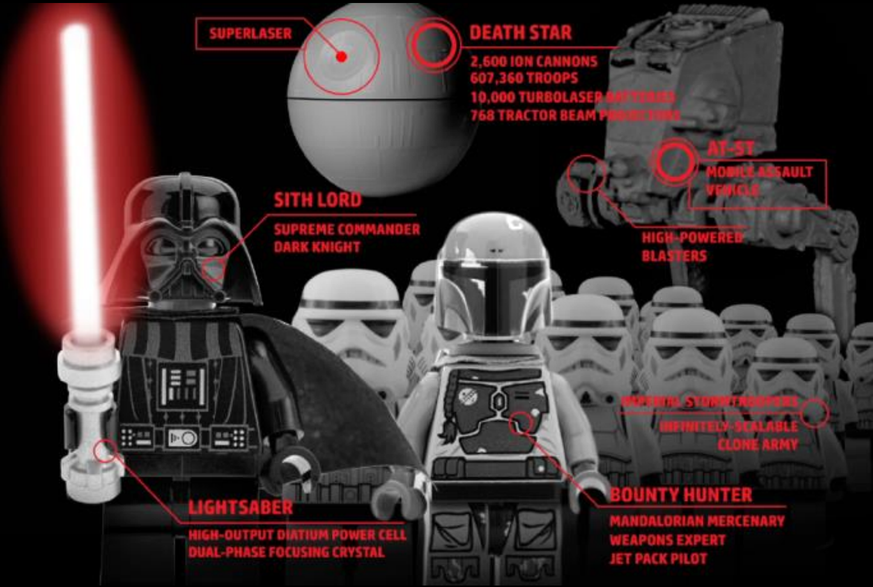
Compliance /
regulatory req

PCI-DSS/SOX…

Stop looking for the silver bullet, start thinking like a bad guy

Art Gilliland





©iStock.com/LeventKonuk

Let me introduce to you …

Let me introduce to you …

Let me introduce to you …

HACKTIVIST CYBERCRIMINAL NATION STATE

ORGANIZE

ORGANIZE

SPECIALIZE

ORGANIZE

SPECIALIZE

MONETIZE

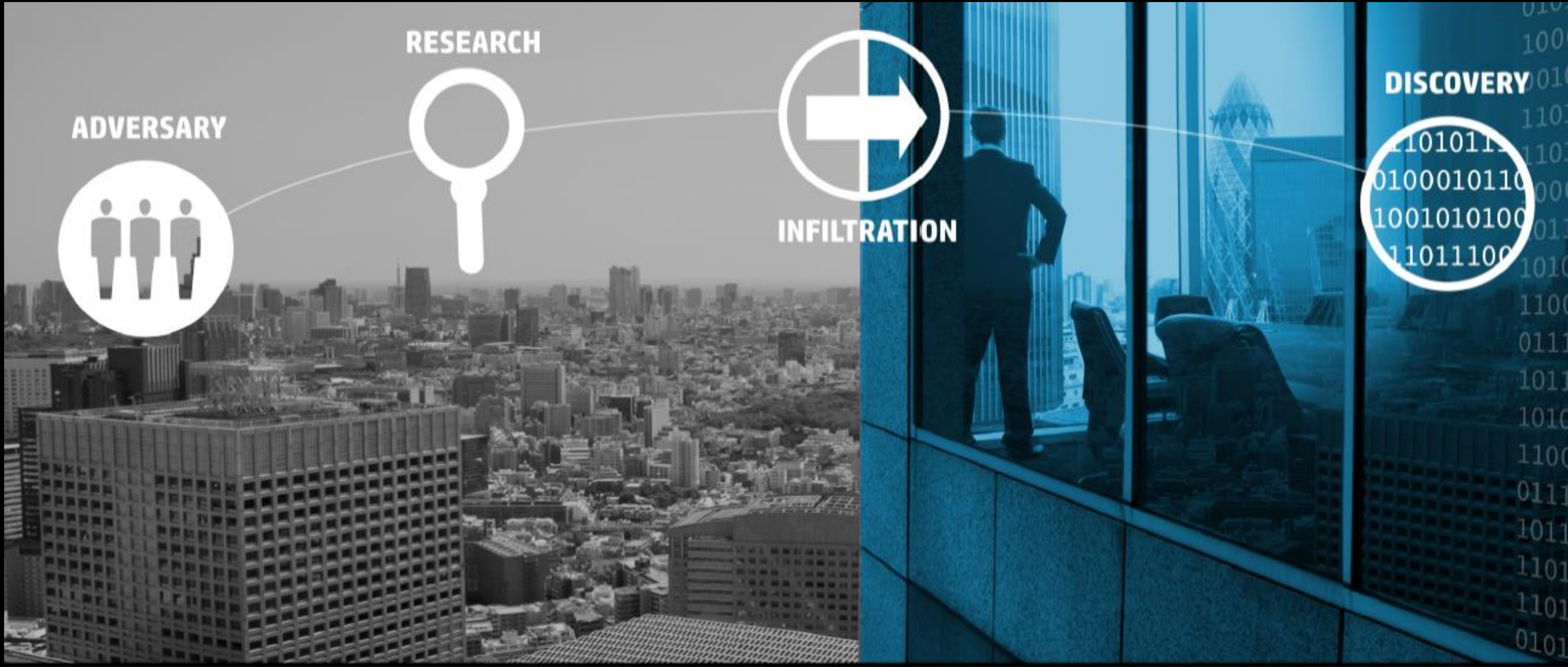
It’s wild world outside

It’s wild world outside

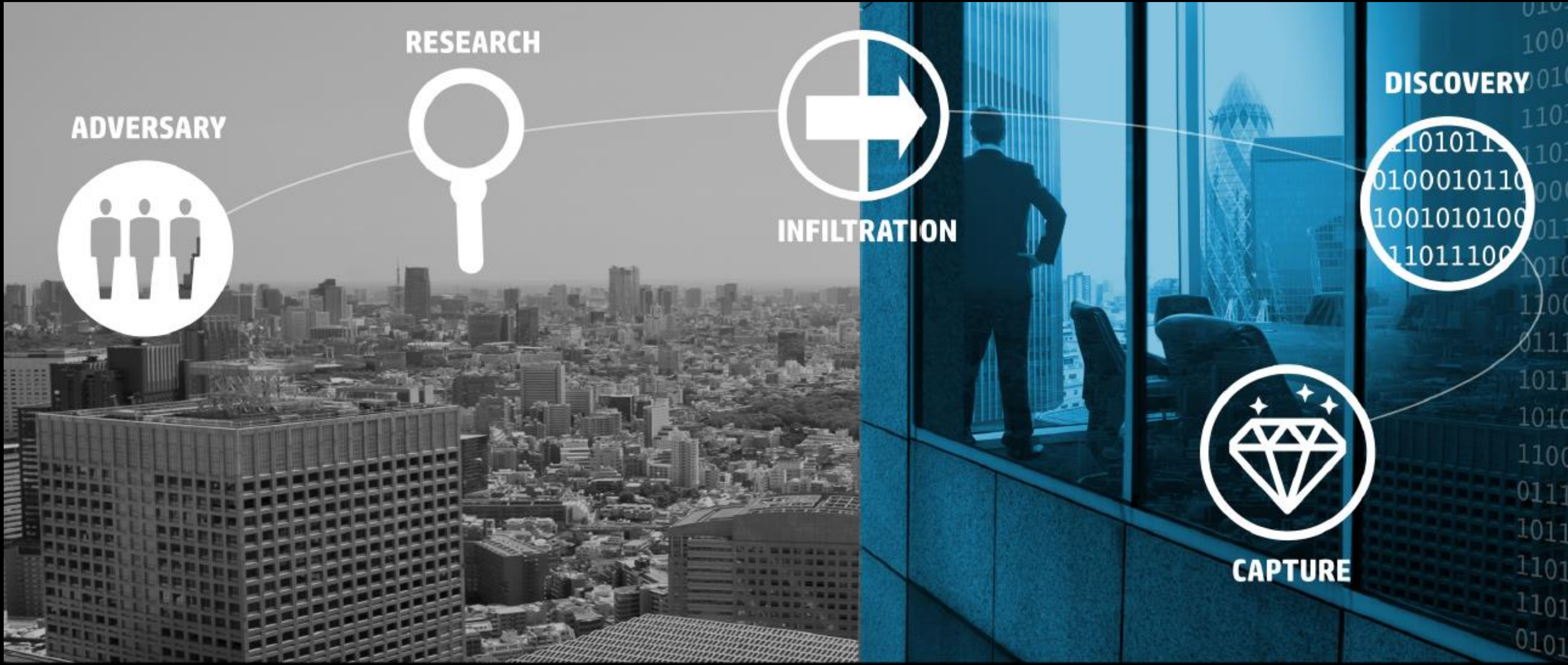
It’s wild world outside

ADVERSARY
RESEARCH
INFILTRATION

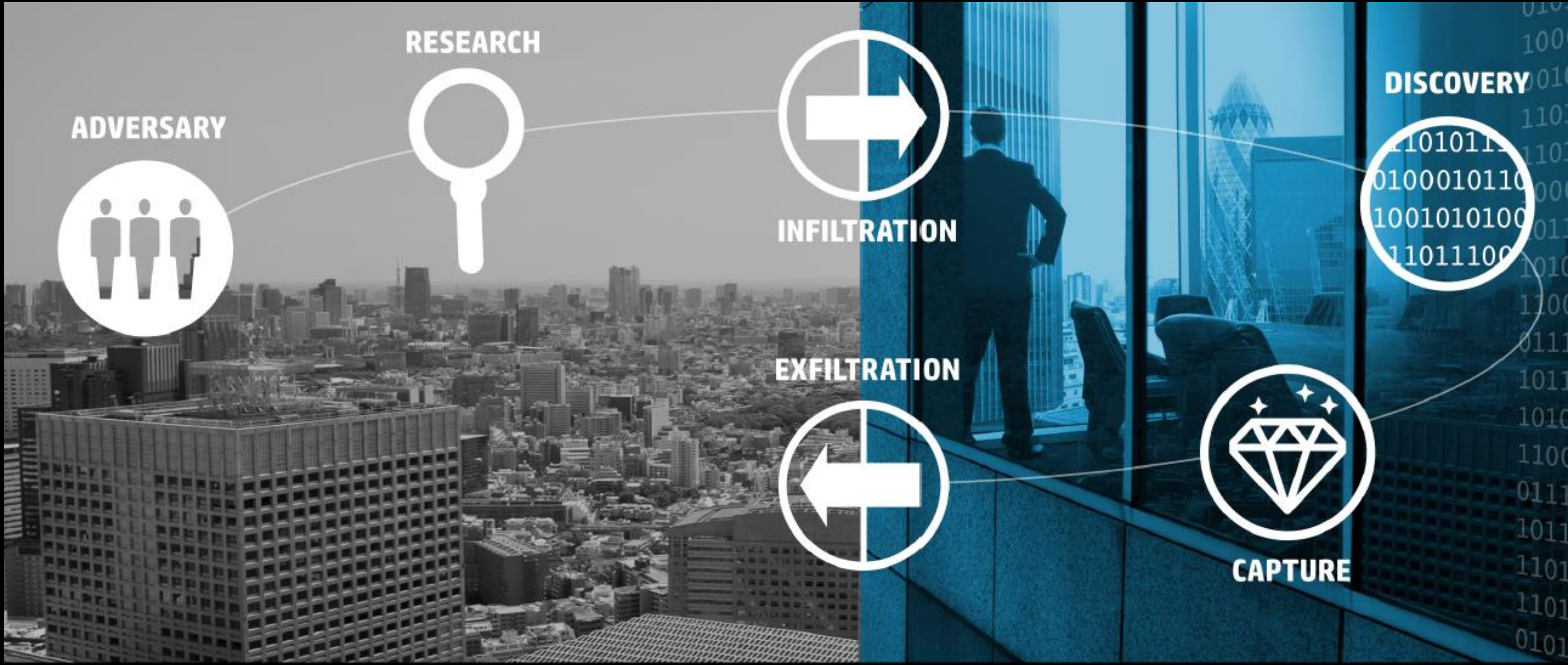
It’s wild world outside



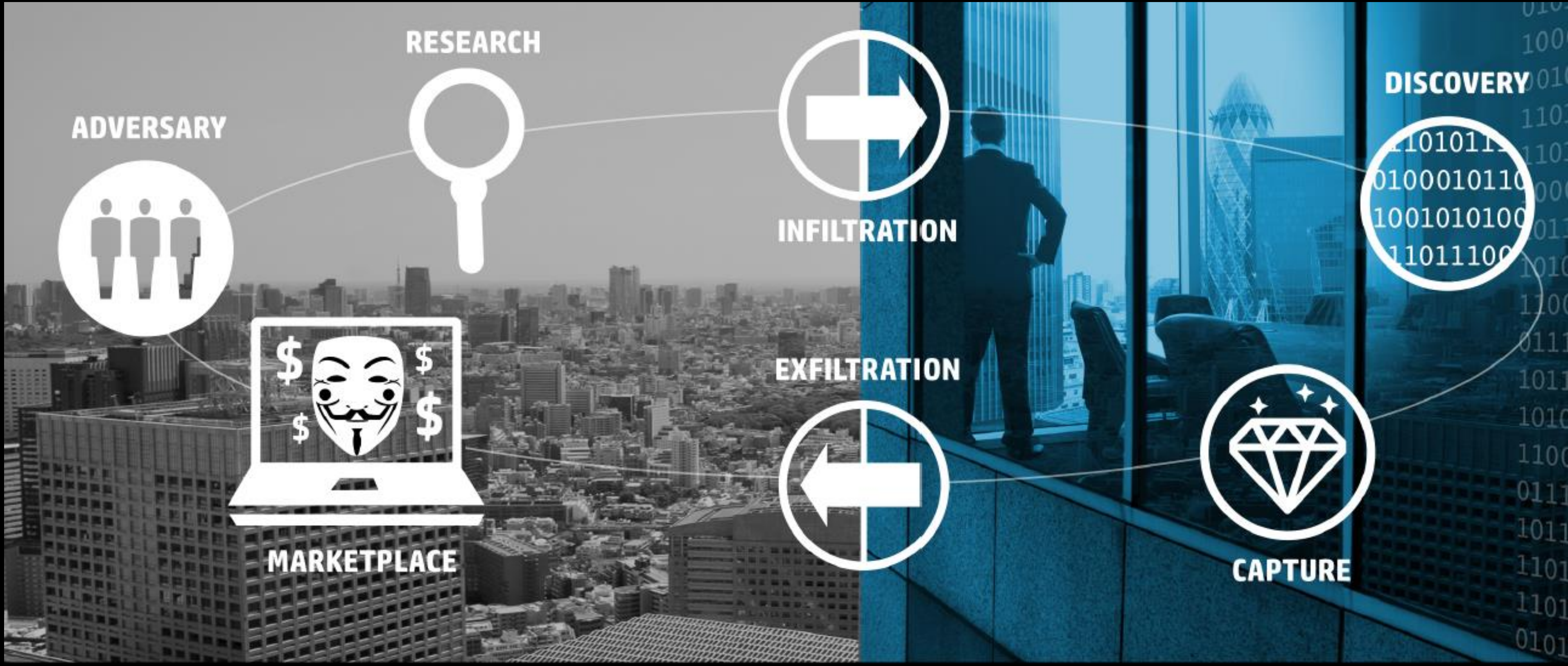
It’s wild world outside



It’s wild world outside



It’s wild world outside



$46 BILLION

Global Spend on Cyber Security

20% increase in **NUMBER OF BREACHES**

30% increase in cost of a single **BREACH**

They only need to be right

ONE TIME

We need to be right
EVERY TIME

High Profile Attack

Easy ? Script kiddies generation.

Example of a High-Profile Attack: RSA Data Breach

1

5:00 AM
Finance person receives a spearphishing email

2

8:30 AM
Opens to see 2012 Recruitment plan with .xls file

3

8:31 AM
RAT program downloaded utilizing Adobe Flash vulnerability

4

8:32 AM
Poison Ivy RAT is initiated

5

NEXT DAY / 12:01AM
NMAP scan to identify and classify network resources

6

OVER THE NEXT 10 DAYS
Collect data over a period of time

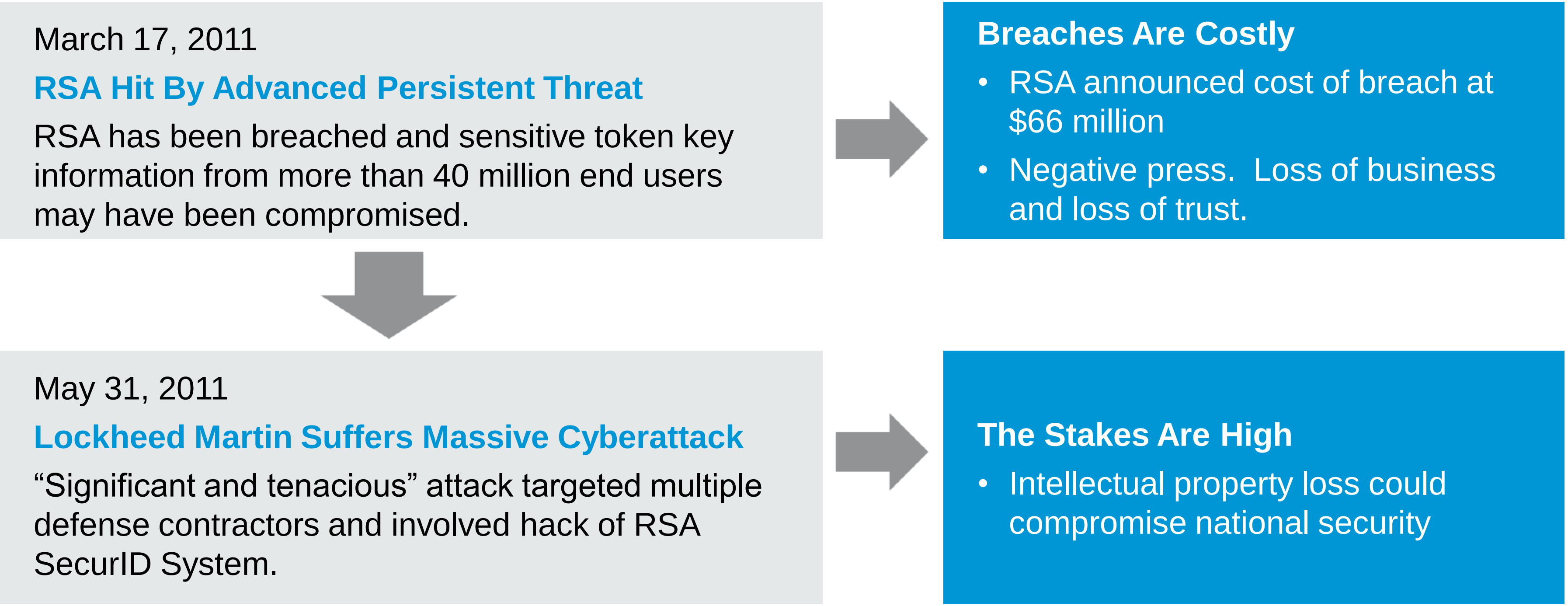
7

11TH DAY / 12:05 AM
Encrypt and ftp file to good.mincesur.com

8

12TH DAY
Attack hits the headlines

The Impact is Real…



March 17, 2011

RSA Hit By Advanced Persistent Threat

RSA has been breached and sensitive token key information from more than 40 million end users may have been compromised.

Breaches Are Costly

- RSA announced cost of breach at $66 million
- Negative press. Loss of business and loss of trust.

May 31, 2011

Lockheed Martin Suffers Massive Cyberattack

“Significant and tenacious” attack targeted multiple defense contractors and involved hack of RSA SecurID System.

The Stakes Are High

- Intellectual property loss could compromise national security

And RSA Was Not Alone…

United Nations
Cyber attack on United Nations leads to massive loss of information and posses huge economic threat.

Blackhole Exploit Injected into USPS Website
The website of U.S Postal Service serving up malware

360,000 accounts hacked in cyber attack; $2.7 million stolen.

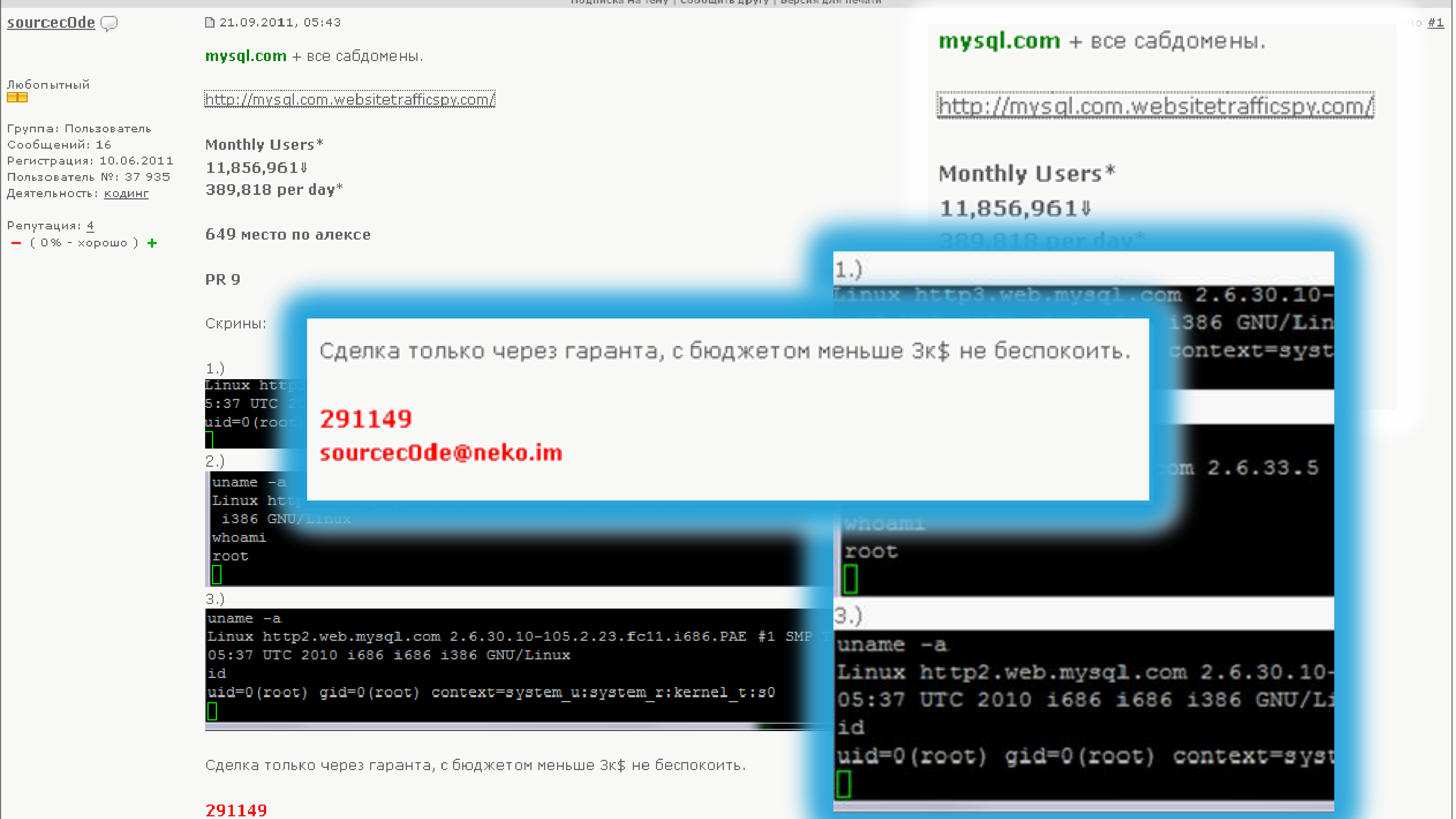
Barracuda Hit By Cyber Attack
Attacker grabbed the information using an SQL injection script

Sony PlayStation Network Down
77 million accounts at risk of data theft

Sony Online estimates 25 million customer accounts hacked.

Stuxnet Worm
Sophisticated worm attacks Siemen's SCADA industry control systems and Windows.

Directors Desk application breached,
Web-based collaboration and communications tool for senior executives and board members



sourcec0de

Любопытный

Группа: Пользователь
Сообщений: 16
Регистрация: 10.06.2011
Пользователь №: 37 935
Деятельность: кодинг

Репутация: 4
– (0% - хорошо) +

21.09.2011, 05:43

#1

mysql.com + все сабдомены.

http://mysql.com.websitetrafficspy.com/

Monthly Users*
11,856,961⇩
389,818 per day*

649 место по алексе

PR 9

Скрины:

1.)

```
Linux http
5:37 UTC 2
uid=0(root
```

2.)

```
uname -a
Linux http
 i386 GNU/Linux
whoami
root
```

3.)

```
uname -a
Linux http2.web.mysql.com 2.6.30.10-105.2.23.fc11.i686.PAE #1 SMP
05:37 UTC 2010 i686 i686 i386 GNU/Linux
id
uid=0(root) gid=0(root) context=system_u:system_r:kernel_t:s0
```

Сделка только через гаранта, с бюджетом меньше 3к$ не беспокоить.

291149

mysql.com + все сабдомены.

http://mysql.com.websitetrafficspy.com/

Monthly Users*
11,856,961⇩
389,818 per day*

1.)

```
Linux http3.web.mysql.com 2.6.30.10-
i386 GNU/Lin
context=syst
```

```
om 2.6.33.5
whoami
root
```

3.)

```
uname -a
Linux http2.web.mysql.com 2.6.30.10-
05:37 UTC 2010 i686 i686 i386 GNU/Li
id
uid=0(root) gid=0(root) context=syst
```

Сделка только через гаранта, с бюджетом меньше 3к$ не беспокоить.

291149
sourcec0de@neko.im

Attacker shopping list…

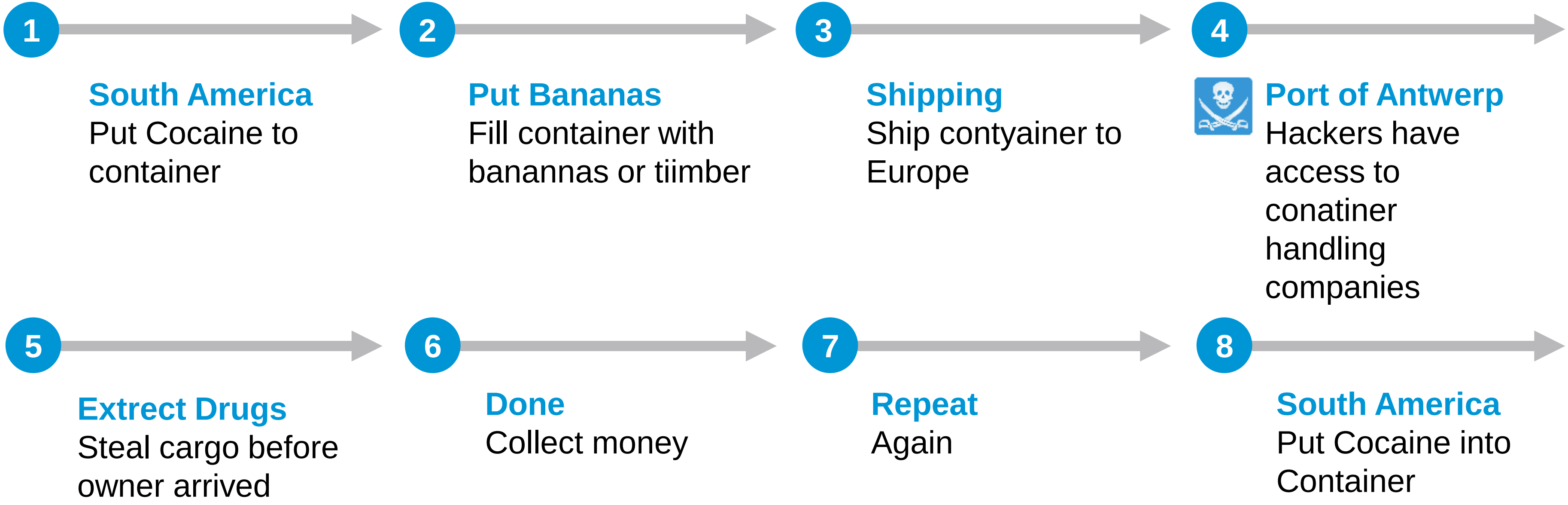
- **DDOS and black mail** for „rich websites“ or public agencies (Daňový portál v marci, Internet Banking na konci roka)
- **Card-botnet in bank** , automatic pay-order system, business model – buyer, botnet master, sales ... From 10k to 600k
- **0-day exploits** – remember RSA ?
- **XSS, SQL injection** – too many doors, so little time
- **Social engineering** – profiling by social site, get „language preference“ , insert malware into iframe in post

- .... Only credit card group make millions by year

Vanishing containers

Drugs smuggling

Drug trafficking in Antverp Port



1

South America
Put Cocaine to container

2

Put Bananas
Fill container with banannas or tiimber

3

Shipping
Ship contyainer to Europe

4

Port of Antwerp
Hackers have access to conatiner handling companies

5

Extrect Drugs
Steal cargo before owner arrived

6

Done
Collect money

7

Repeat
Again

8

South America
Put Cocaine into Container

Drug trafficking in Antverp Port – tech spec

Drug traffickers **recruited hackers** to breach IT systems that **controlled** the movement and location of containers

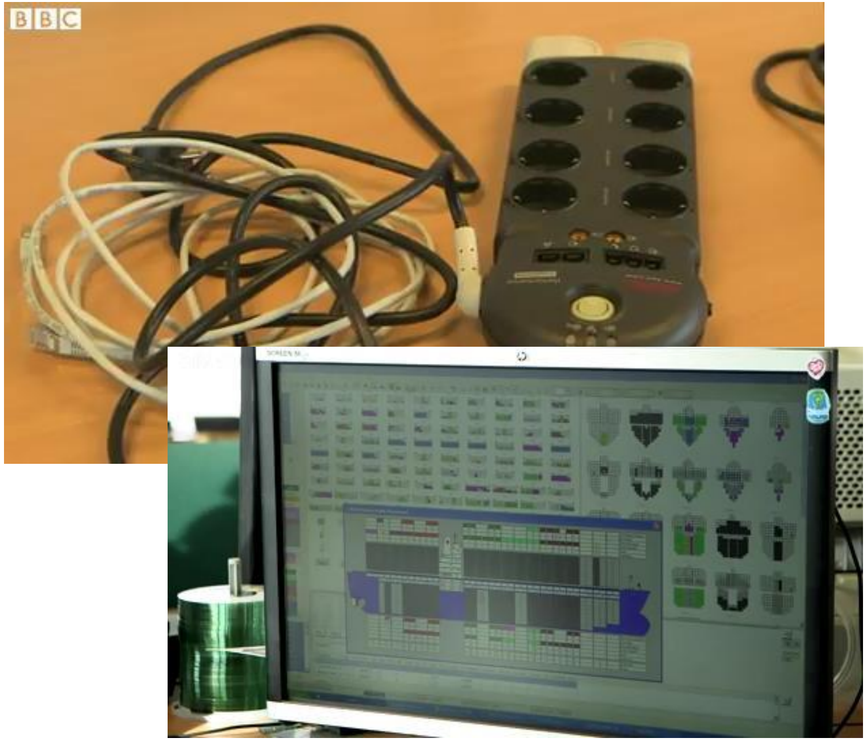
We have effectively a **service-orientated industry** where organised crime groups are paying for specialist hacking skills that they can acquire online

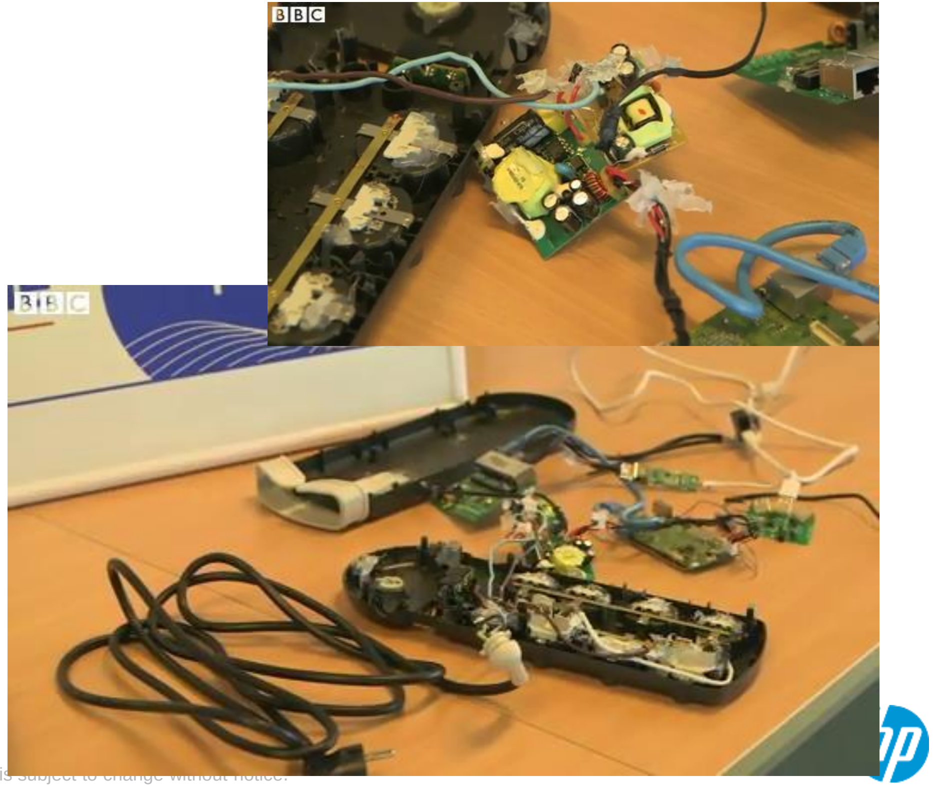
alleged plot demonstrates how the internet is being used as a "**freelance marketplace**" in which drug trafficking groups recruit hackers to help them carry out cyber-attacks "to order".

The case is an example of how **organised crime** is becoming more **enterprising**, especially online

Drug trafficking in Antverp Port – HW

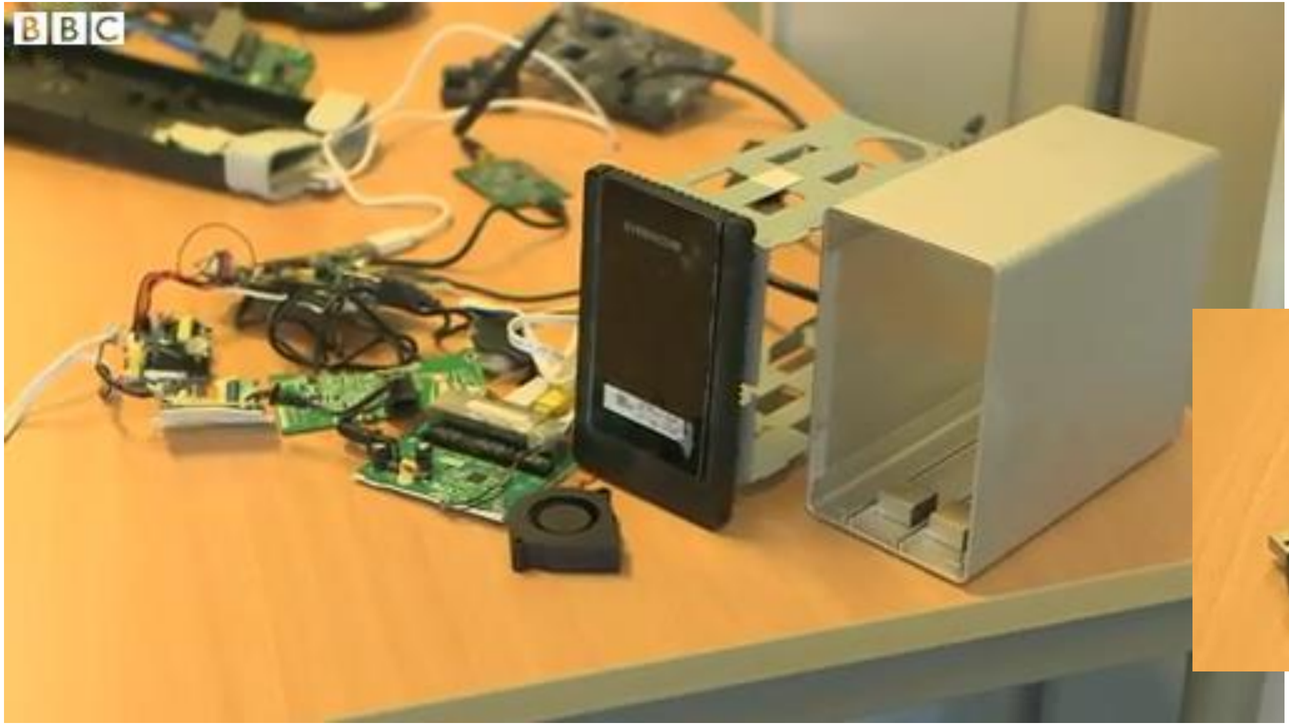
Brake into offices of shipping companies and installed devices

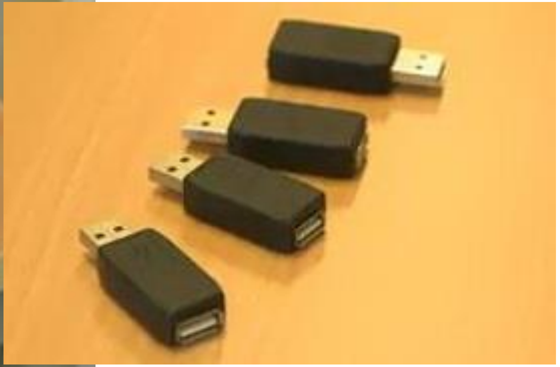




Drug trafficking in Antverp Port – HW part 2

Brake into offices of shipping companies and installed devices



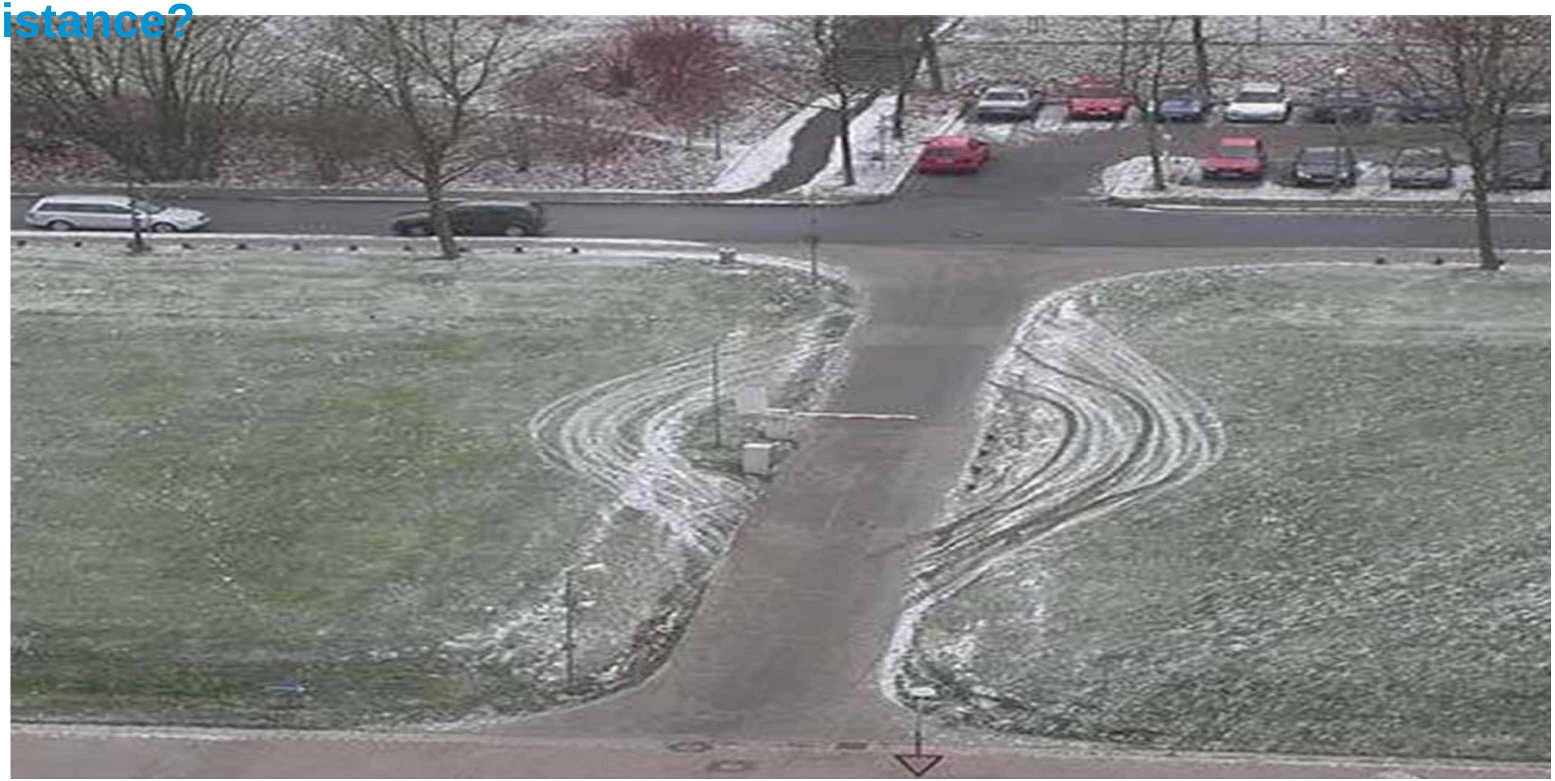


Is your security OK ?

If you feel SECURE , probably you just don‘t know what was stolen from you !

In theory, you are safe…

The path of least resistance?



IT Security project

It is like being married.

When its perfect, theres no thanks. When it goes wrong, boy you are in troubles!

Scope Management

includes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully.

Theory: Prepare equipment, install it and make it functional

Practice: Have no idea whats going on and how environment is depending on PCI-DSS compliance

Time Management

includes the processes required to manage the timely completion of the project.

Theory: In 3 months we are going live.

Practice: waiting, waiting, waiting .....

Cost Management

includes the processes involved in planning, estimating, budgeting, financing, funding, managing, and controlling costs so that the project can be completed within the approved budget.

Theory: We buy chepest version and few mandays. It must be enough.

Practice: Wanted full blown functionality, lot of custom coding .But, hey, its our customer, we can work for free

Human Resource Management

includes the processes that organize, manage, and lead the project team.

Theory: IT manager will be just fine.

Practice: Security manager hired in the middle of project, stating that security analyst will be hired at the end of delivery.

Risk Management

includes the processes of conducting risk management planning, identification, analysis, response planning, and controlling risk on a project

Theory: We will held meeting each week, taking risk log.

Practice: Bug and resource hunting.

When things go wrong

We should have thought of that

you already realise that the project could have been planned for or managed as a risk.

The shock of the unexpected

Top security operation center in public offices for rent.

after the initial shock, our job is to clean up as quickly and as well as we can, and then decide on the longer-term action

You may need a good lawyer

There is sensitive financial data breach, time to crawl years of emails, and documents to establish lines of defence in case negotiation fails

If one women deliver baby in 9 months, 9 women deliver in 1 month.

Thank you

Peter Mikeska (CiSA, CiSM, RHCE)

peter.mikeska@hp.com