WSIS 2015

Session 262 - Building trust

Geneva, 28 April 2015

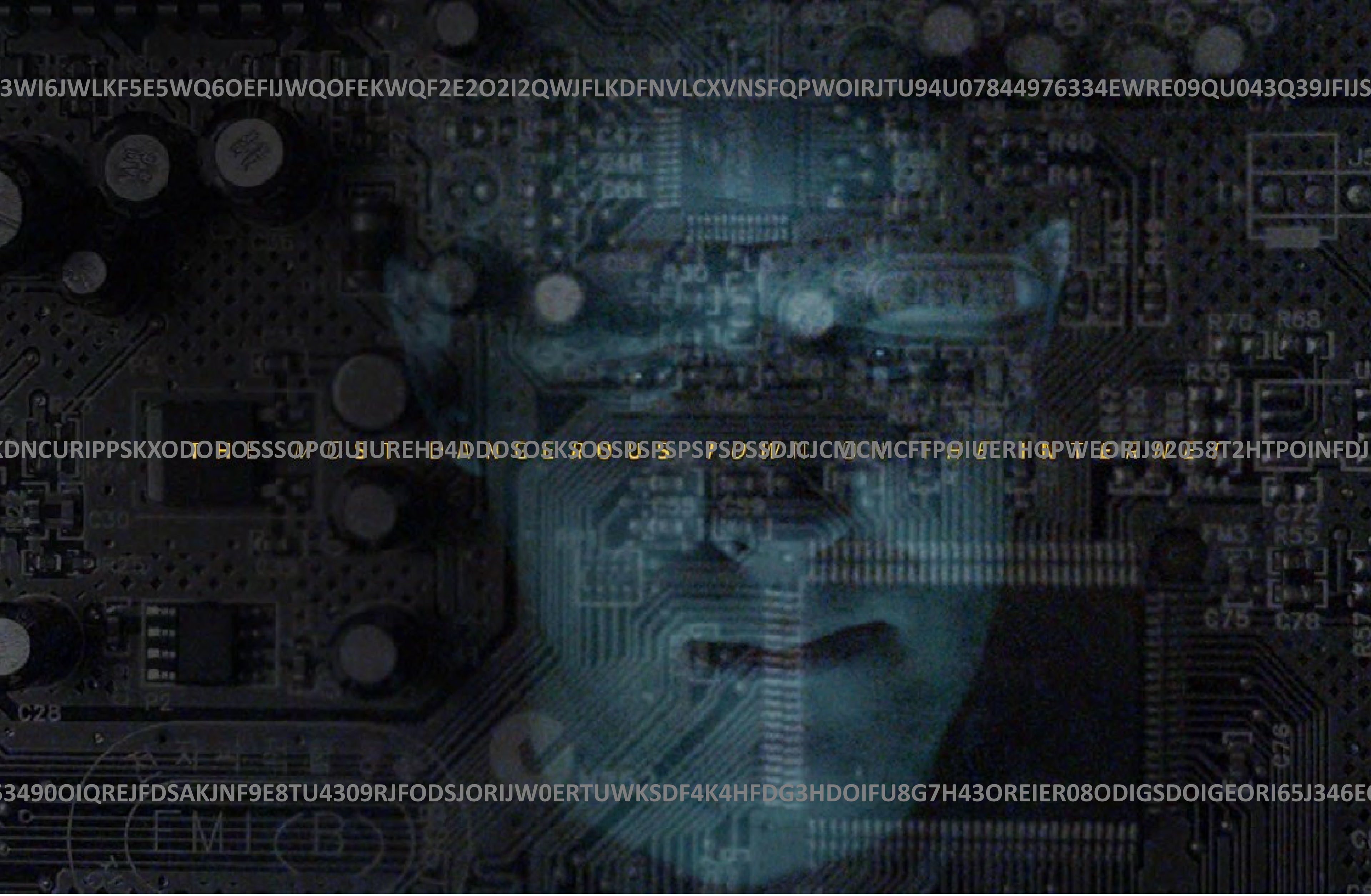
BALANCING CYBER-SECURITY AND PRIVACY

Giampiero Nanni

Government Affairs - Europe, Middle East, Africa

Symantec

giampiero_nanni@symantec.com


3WI6JWLKF5E5WQ6OEFIJWQOFEKWQF2E2O2I2QWJFLKDFNVLCXVNSFQPWOIRJTU94U07844976334EWRE09QU043Q39JFIJS
KDNCURIPPSKXODOHOSSSOPOIUUREHB4DDOSOSKSOOSPSPSPSPSPSSDJCJCMCMCFFPOIUERHGPWEORJ92058T2HTPOINFDJ
3490OIQREJFDSAKJNF9E8TU4309RJFODSJORIJW0ERTUWKSDF4K4HFDG3HDOIFU8G7H43OREIER08ODIGSDOIGEORI65J346E

Agenda

1 Threat landscape

2 Security

3 Privacy

4 Balance

1 Threat landscape

Are you ready for the next cyber-attack ?

Imagine… you have to tell the Board of Directors, that your organization has been compromised by an attack…

It took the attackers only **six minutes** to circumvent the perimeter defenses. From there, they achieved domain administrator privileges in **less than 12 hours.**In less than a week they **fully compromised** all 30 of our global domains.

They harvested **all our credentials**, giving them the ability to log in to the network **masquerading as any of us**. There was **no place** on our global network they could not go and only a handful of computers they did not have easy **access to**.

The attackers were in a position to electronically **transfer millions of dollars** out of our bank accounts through our accounts payable system.

They had **direct access** to our **manufacturing**

The information economy trends

Socialisation

IoT/ Hyper-connectivity

Mobility/

Platform proliferation

Cloud/

Virtualisation

Smart Infrastructure

Big Data

Data flow globalisation

The information economy risk

Risk level

Lloyd’s Risk Index 2013	
26 Energy security	39 Harmful effects of new technology
27 Demographic shift	40 Pandemic
28 Industrial/workplace accident	41= Abrupt regime change
29 Environmental liability	41= Riots and civil commotion
30 Sovereign debt	41= Flooding
31 Piracy	44 terrorism
32 Climate change	45 Windstorm
33 Water scarcity	46 Drought
34 Strikes and industrial action	47 Threats to biodiversity
35 Population growth	48 Earthquake
36 Expropriation of assets	49 Impact of space weather
37 Urbanisation	50 Volcanic eruption
38 Food security	

[redacted]

Risk level

Lloyd’s Risk Index 2013	
1 High taxation	14 Corporate liability
2 Loss of customers/cancelled orders	15= Major asset price volatility
3 Cyber risk	15= Poor/incomplete regulation
4 Price of material inputs	17 Fraud and corruption
5= Excessively strict regulation	18 Government spending cuts
5= Changing legislation	19 Theft of assets or IP
7 Inflation	20 Failed investment
8 Cost and availability of credit	21 Corporate governance failure
9 Rapid technological changes	22 Critical infrastructure failure
10 Currency fluctuation	23 Supply chain failure
11= Interest rate change	24 Increased protectionism
11= Talent and skills shortage	25 Insolvency risk
13 Reputational risk	

Symantec Internet Security Threat Report, Vol. 20

In 2014

- Nearly **ONE MILLION** new threats released

Every day

- More than 400 MILLION identities exposed
- Targeted attacks to large enterprise up **40%** (5 out of 6)
- **60%** of targeted attacks were against SMEs
- Crypto-ransomware up **4500%**
- **17%** Android mobile Apps are malware carriers
- E-mails still the preferred vector but social media fastly rising
- The « Internet of Things » is source of vulnerability (cars, medical equipment)
- Software download websites a new vehicle for hackers

[redacted]

Cyber-attackers
are leap-frogging defences
in ways organisations
lack insight to anticipate

Facts, not predictions

- Risk zero doesn’t exist
- Attacks will happen, some successfull (‘100K records from IRS’)
- Errors will occur, human or technical
- Insiders will be negligent or malicious (‘PA to CEO ’)
- Confidentiality, Integrity & Availability will be impacted
- It’s impossible to protect everything at the highest level
- All critical assets are not identified or even known
- Mobility is pervasive, Internet of Things
- There is no IT perimeter anymore
- « Social » is the new normal
- « Smart » is the new normal

2 Security

Security posture: PREPARE→PREVENT→DETECT→RESPOND

- Cyber-Security ≠ Antivirus
- Legislation/Regulation/Policy
- Establish authorities & stakeholders
- Acquire intelligence, monitor threats
- Establish response teams (CERT)
- Define procedures/processes
- Define Critical Infrastructure
- Coach people, build capacity
- Cooperate, share information – PPP
- Invest

What is Dragonfly?

- Dragonfly is
  - Ongoing cyberespionage campaign
  - Targeting the energy sector in Europe an
  - Stealing information
  - Capable of sabotage
- Targets
  - Electricity infrastructure
  - Electricity generation
  - Industrial equipment provi
  - Petroleum pipeline operat

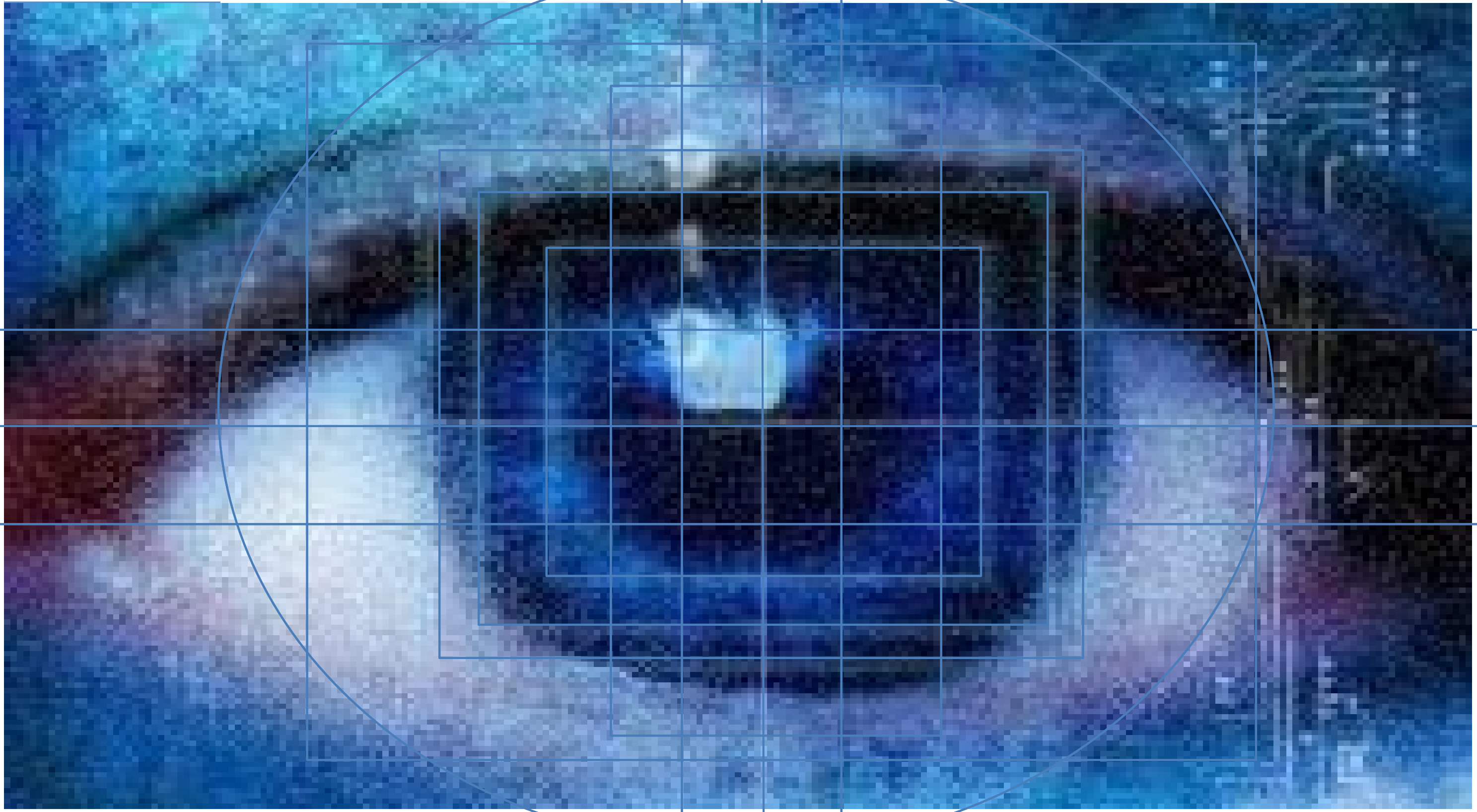
The Dragonfly group

- In operation since at least 2011
- Initially targeted defense and aviation companies in the US and Canada
- Shifted focus to US and European energy firms in early 2013
- Priorities appear to be:
  - Persistent access to targets
  - Information stealing
  - Sabotage
- Has the hallmarks of state sponsored op
- Appear to be operating in the UTC +4 tir

Dragonfly employs three attack vectors

- Spam emails
- Watering hole attacks
- Compromising third party sof [redacted]
  - Three ICS equipment providers
  - Malware inserted into the software bundles they had made available for download on their websites
  - Victims inadvertently downloaded “Trojanized” software when applying software updates
  - By targeting suppliers, attackers found “soft underbelly” that provided a path into bigger companies

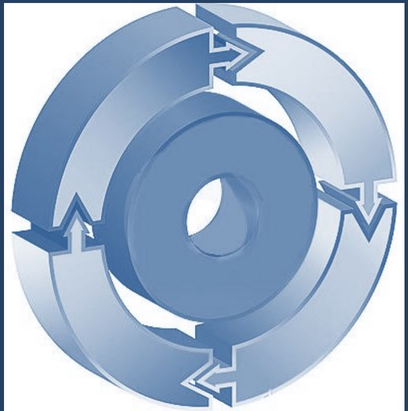
3 Privacy



Cyber-security must address 3 dimensions

PEOPLE

PROCESSES



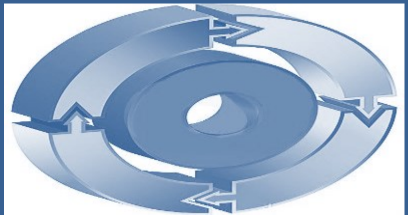
TECHNOLOGY

+1

Privacy

PEOPLE

PROCESS

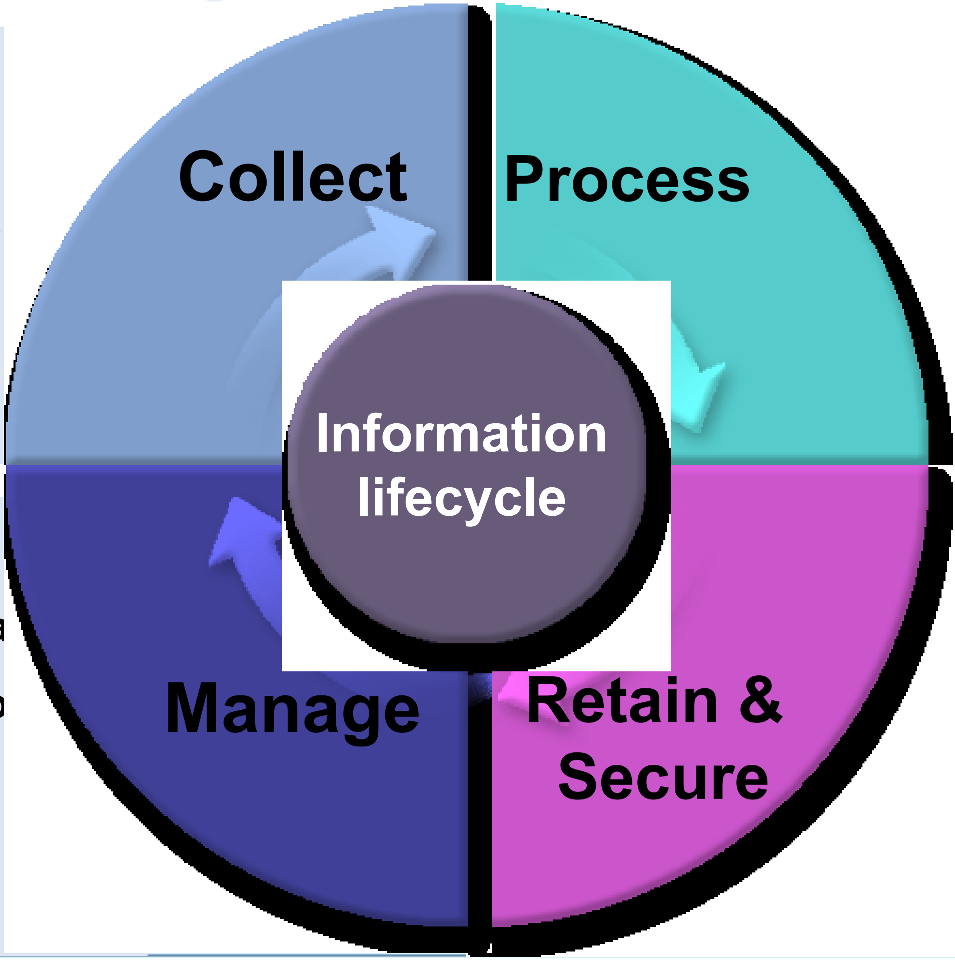


TECHNOLOGY

Information lifecycle - good data governance

Principles of data collection

- Fairly and lawfully
- Receiving individua consent
- Relevance
- Proportionality
- Types of data



Purpose limitation

- Specific data
- For specific purpose

ny changes need to be notified

Provide access

Right to rectify data

Data destruction po

Data transfers

Applicable rules

Retain

- Duration
- Types of data

Secure

- Technical measures

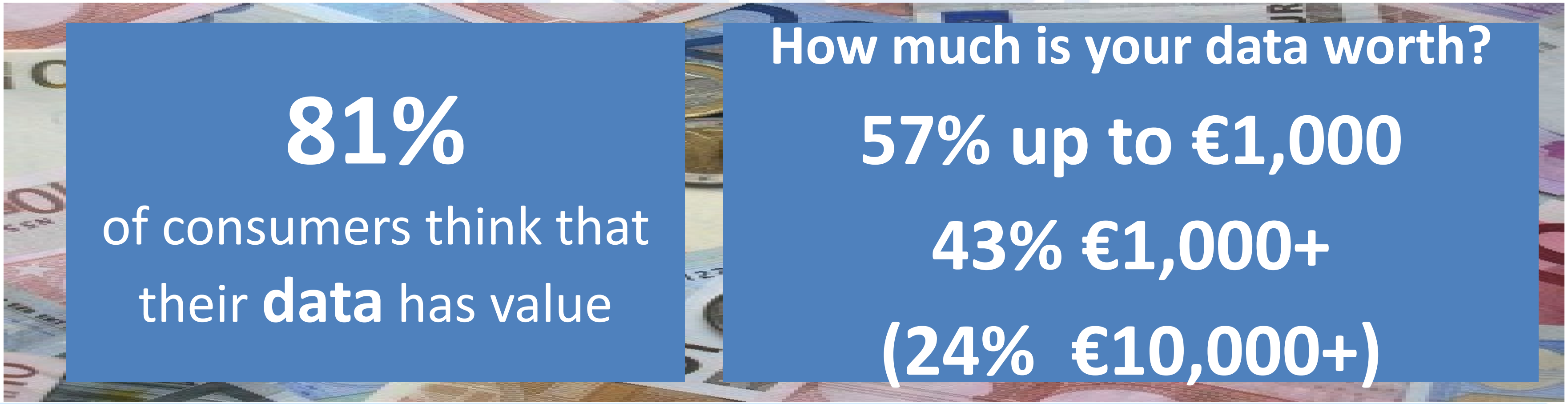
rganizational measures

- Data loss

[redacted]

The State of Privacy study

- In a digital economy data is the "new currency"
- Information protection generates value, enables growth
- Individual/Industry/Government/National Security interlinked.
- Changing European legislation
- Lack of ownership
- Business apathy
- Exponential growth of risk



81%

of consumers think that their **data** has value

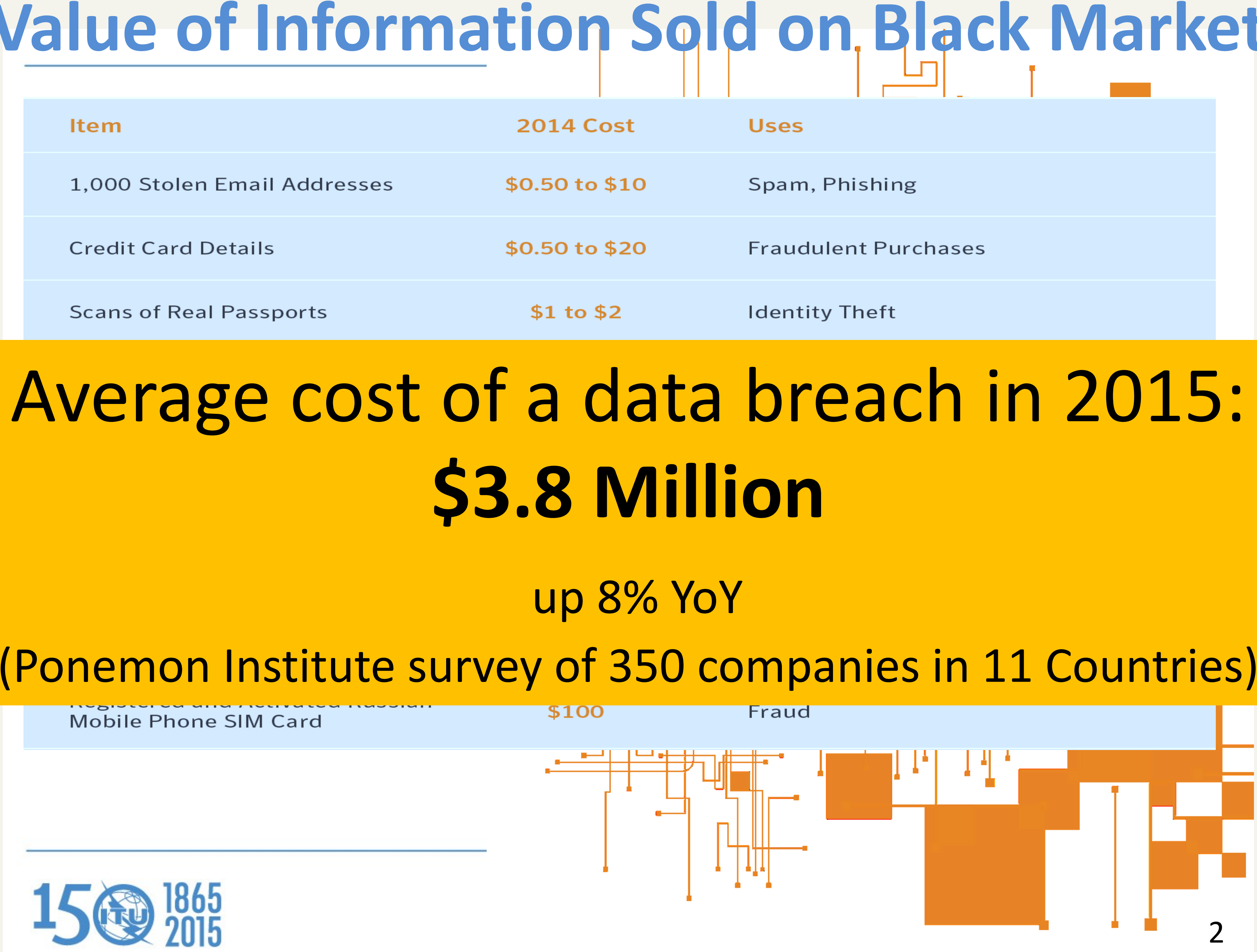
How much is your data worth?

57% up to €1,000

43% €1,000+

(24% €10,000+)

Value of Information Sold on Black Market



Item	2014 Cost	Uses
1,000 Stolen Email Addresses	$0.50 to $10	Spam, Phishing
Credit Card Details	$0.50 to $20	Fraudulent Purchases
Scans of Real Passports	$1 to $2	Identity Theft
Registered and Activated Russian Mobile Phone SIM Card	$100	Fraud

150 ITU 1865 2015

Average cost of a data breach in 2015:

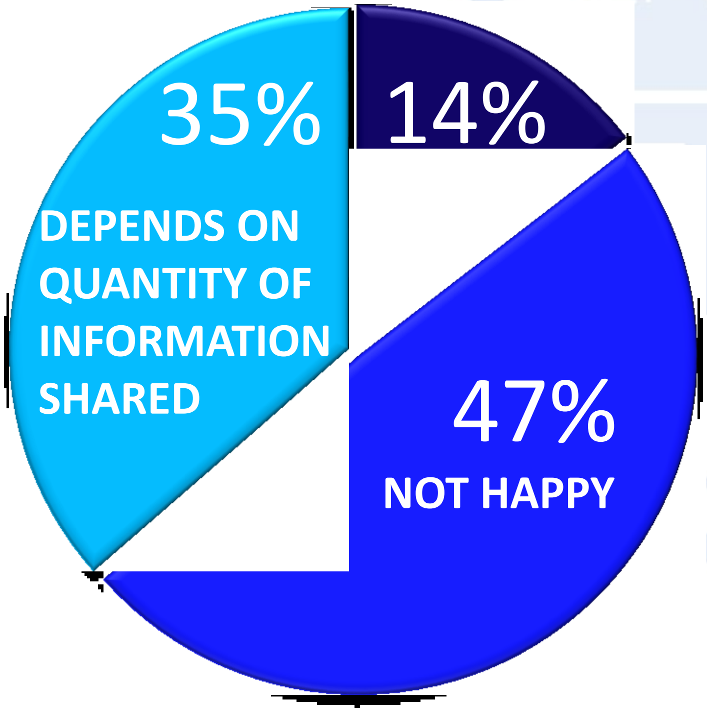
$3.8 Million

up 8% YoY

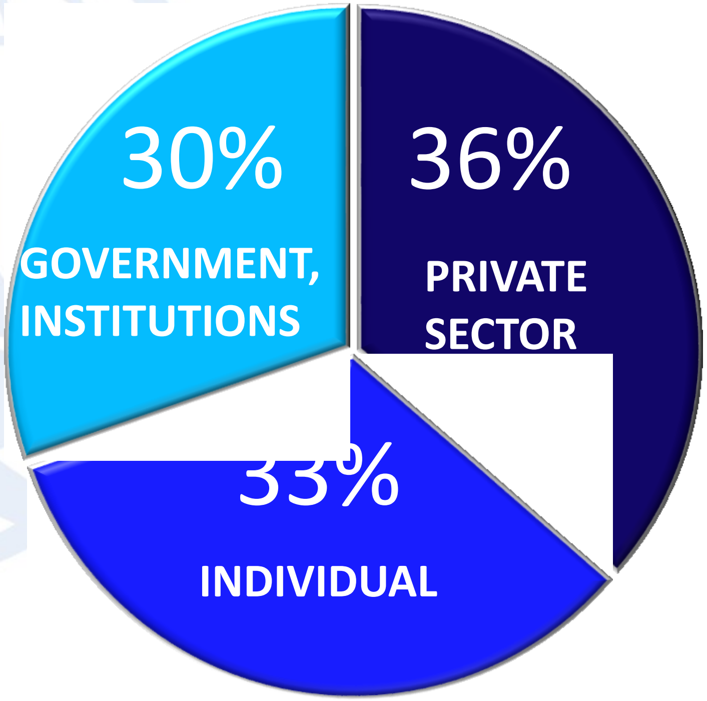
(Ponemon Institute survey of 350 companies in 11 Countries)

The State of Privacy study: Personal data

Almost half of people are not happy to share their personal data with third parties

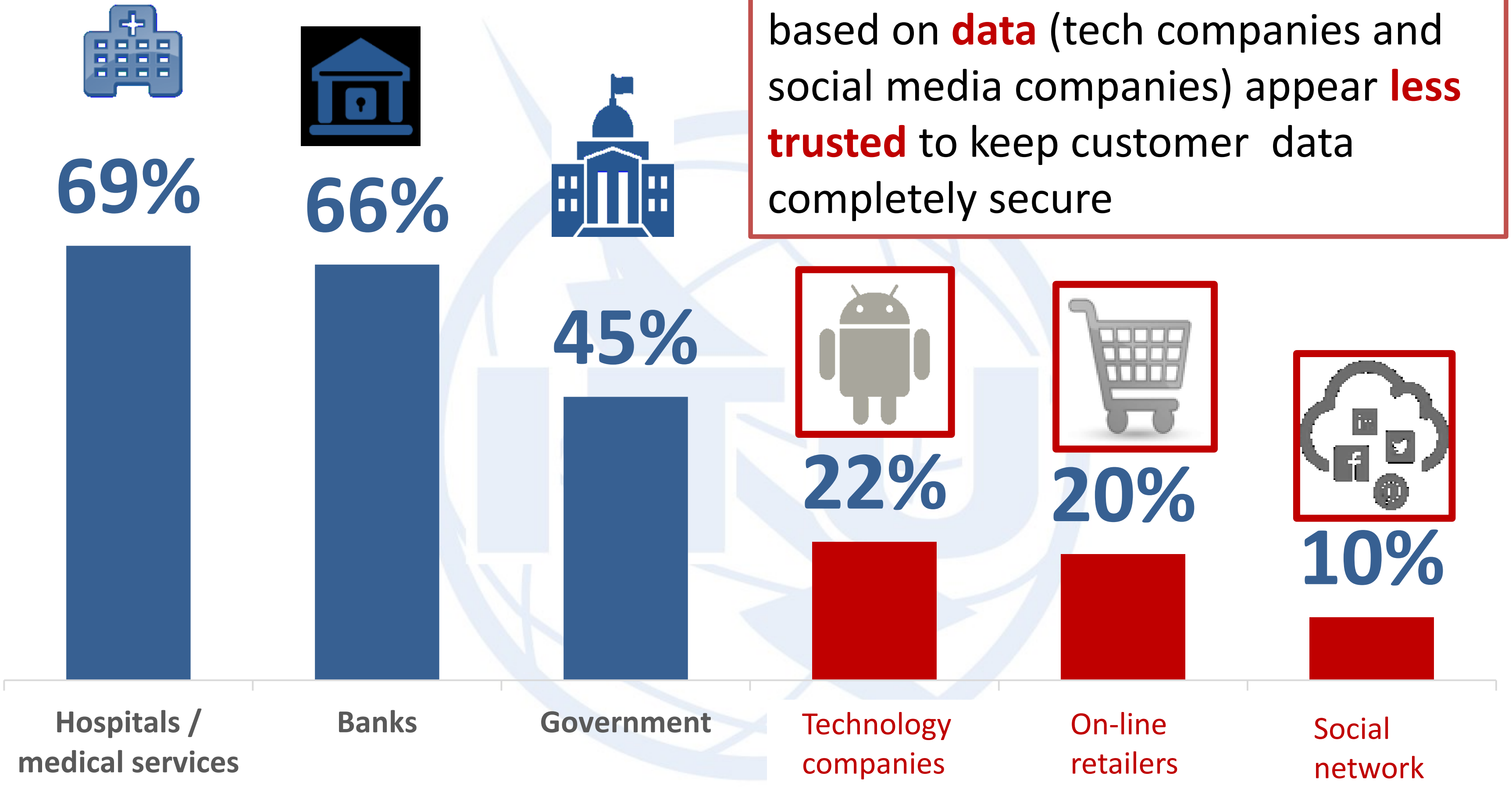


% of responsibility in protecting personal information



The State of Privacy study: Level of trust in organisations

Organisations with **business models** based on **data** (tech companies and social media companies) appear **less trusted** to keep customer data completely secure



Consumers will trade personal data in exchange for…

STORE DISCOUNT	33%
WIN A PRIZE	30%
FOR MONEY	30%
LOYALTY BENEFITS	29%
ACCESS to a FREE APP	17%

1 in **3**

give

false information

in order to protect their data

57%

avoid posting

their detail online

4 Balance

[redacted]

EU General Data Protection Regulation (GDPR)

“***Personal data*** shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity“

- Applicable to all industry of a certain size in all Countries
- Possibly to public sector - by Country discretion
- Regulates how personal data are collected, processed, retained and transferred
- Severe sanctions

PRIVACY

- Privacy is the new “Green”
- Emotional and highly political
- Snowden effect
- Reputational risk
- Legal risk
- Moral issues
- Customer expectations and rights

DATA

- Collection is fair and lawful
- Collection is for a specific purpose
- Collection is proportionate, limited in time and for the minimum amount necessary
- Data is accurate and is protected
- Data transfer is regulated

Network & Information Security (NIS)

Obligation for EU Member States:

- Establish national cybersecurity strategies
- Build incident response capabilities
- Share information with each other

Obligation for industry:

- In key sectors (energy, transport, finance, health, and possibly some large scale public clouds) to manage cyber risk and notify cybersecurity breaches;
- Obligation for industry to share information with their governments

Change

in

Business model

The security vs. privacy dilemma

"My government will work to reduce the threat from nuclear weapons, cyber attacks and terrorism."

[redacted]

Q&A

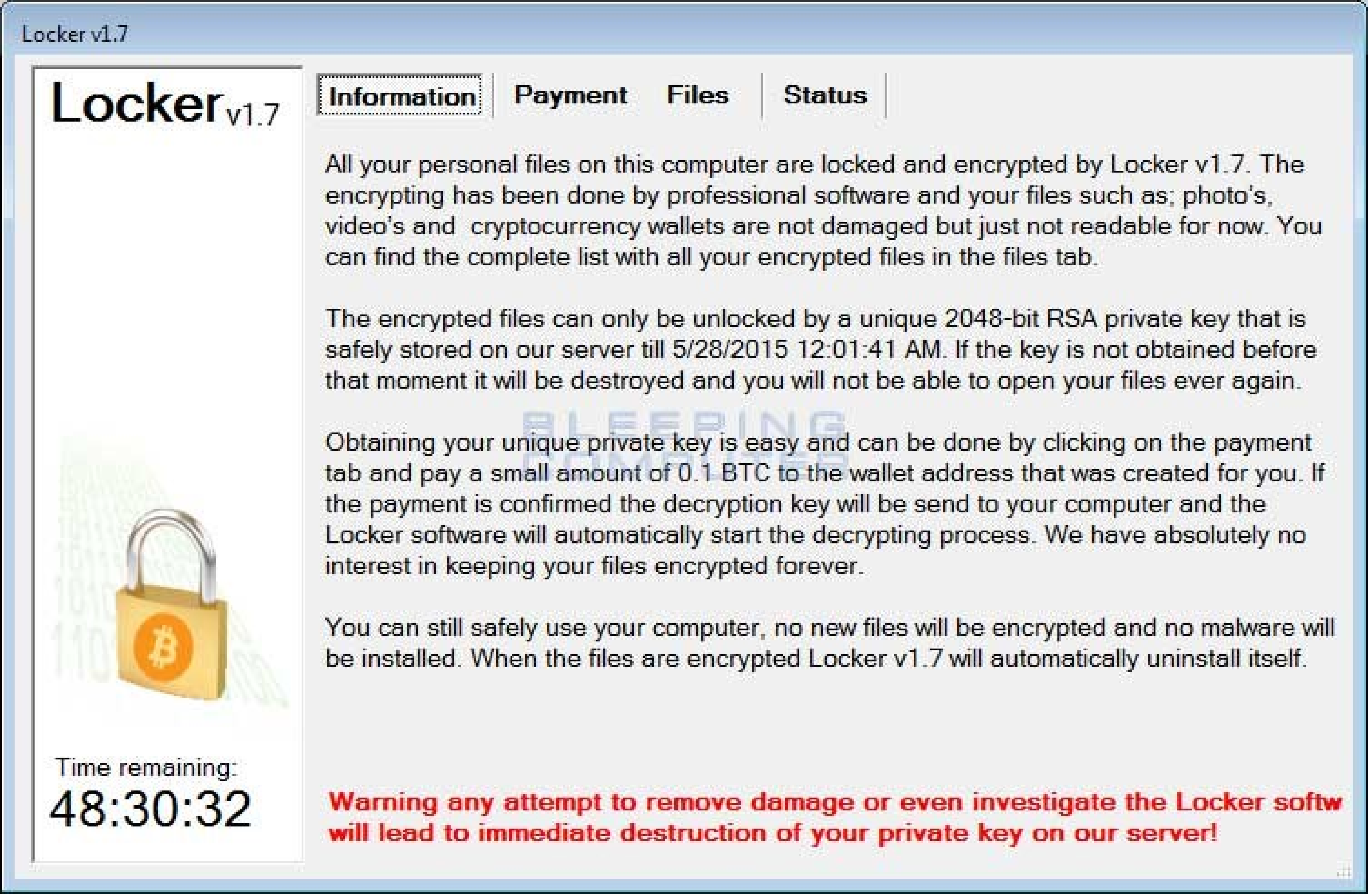
Thank you!

Giampiero Nanni

Government Affairs - Europe, Middle East, Africa

giampiero_nanni@symantec.com

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.



All your personal files on this computer are locked and encrypted by Locker v1.7. The encrypting has been done by professional software and your files such as; photo's, video's and cryptocurrency wallets are not damaged but just not readable for now. You can find the complete list with all your encrypted files in the files tab.

The encrypted files can only be unlocked by a unique 2048-bit RSA private key that is safely stored on our server till 5/28/2015 12:01:41 AM. If the key is not obtained before that moment it will be destroyed and you will not be able to open your files ever again.

Obtaining your unique private key is easy and can be done by clicking on the payment tab and pay a small amount of 0.1 BTC to the wallet address that was created for you. If the payment is confirmed the decryption key will be send to your computer and the Locker software will automatically start the decrypting process. We have absolutely no interest in keeping your files encrypted forever.

You can still safely use your computer, no new files will be encrypted and no malware will be installed. When the files are encrypted Locker v1.7 will automatically uninstall itself.

Time remaining:
48:30:32

Warning any attempt to remove damage or even investigate the Locker softw will lead to immediate destruction of your private key on our server!