OSY.SSI[2019][1]

Table of Contents

Security: a definition?

Information-related risks

Risks and Mitigation

An asymmetric relation

Threats, targets and adversaries

- Threat exposure

Dynamics and Macro-scale

A definition?

Security invokes strategies to deal with (information-related) risks.

What it's all about...

« Private information is practically the source of every large modern fortune. »

– Oscar Wilde, *An Ideal Husband*, Act I.

What it's all about...

> « Private information is practically the source of every large modern fortune. »
>
> – Oscar Wilde, *An Ideal Husband*, Act I.

Information shapes power relationships.
That is why we care about it.

What it's all about...

« Private information is practically the source of every large modern fortune. »

– Oscar Wilde, *An Ideal Husband*, Act I.

Information shapes power relationships.
That is why we care about it. But really it's just a means to an end.

What it's all about

I'm going to argue something you may find puzzling:

Security isn't about protecting things or avoiding incidents.

To see that, we must look at how it fits in the bigger picture.

Part I
The Classical Security Theory

Classical Security Theory, cheatsheet

It is based around three key notions that we'll start discussing right now:

- Informational Risk
- Access control
- Models and properties

Table of Contents

Security: a definition?

Information-related risks

Risks and Mitigation

An asymmetric relation

Threats, targets and adversaries

- Threat exposure

Dynamics and Macro-scale

Technology is great, it makes our lives easier sometimes.

But there’s no such thing as a free meal.

Risks

What is “risk”?

Incident:

- Example : A meteor hits the Earth, destroying all forms of life.

Risks

What is “risk”?

Incident:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won’t.

Risks

What is “risk”?

Incident:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won’t.

Risk measures the expected loss caused by incidents

Risks

What is “risk”?

Incident:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won’t.

Risk measures the expected loss caused by incidents

$$\text{Risk} = \mathbb{E}\left[\text{cost}\right] = \sum_{\text{danger}} \text{probability of occurence} \times \text{cost}$$

Risks

What is “risk”?

Incident:

- Example : A meteor hits the Earth, destroying all forms of life.

There are many dangers: some we will meet, some we won’t.

Risk measures the expected loss caused by incidents

$$\text{Risk} = \mathbb{E}\left[\text{cost}\right] = \sum_{\text{danger}} \text{probability of occurence} \times \text{cost}$$

Question: what terms do we know in that equation?

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability
- Integrity

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability
- Integrity
- Confidentiality

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability
- Integrity
- Confidentiality
- Hijacking

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability
- Integrity
- Confidentiality
- Hijacking
- etc.

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability
- Integrity
- Confidentiality
- Hijacking
- etc.

(The first three: CIA). REMEMBER THIS.

Risks and threats

Risk analysis 101

Information-related risks fall in several categories

- Availability
- Integrity
- Confidentiality
- Hijacking
- etc.

(The first three: CIA). REMEMBER THIS.

Risk analysis is the process of:

- Identifying key dangers
- Measuring the associated cost

This results in a *risk profile*.

Note : cost might include more than money. (or can it).

Table of Contents

- Security: a definition?
- Information-related risks
- Risks and Mitigation
- An asymmetric relation
- Threats, targets and adversaries
  - Threat exposure
- Dynamics and Macro-scale

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

Information security in a nutshell:

Risks and mitigation

Risk management 101

Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

Information security in a nutshell: <u>REMEMBER THIS.</u>

Risks and mitigation

Risk management 101

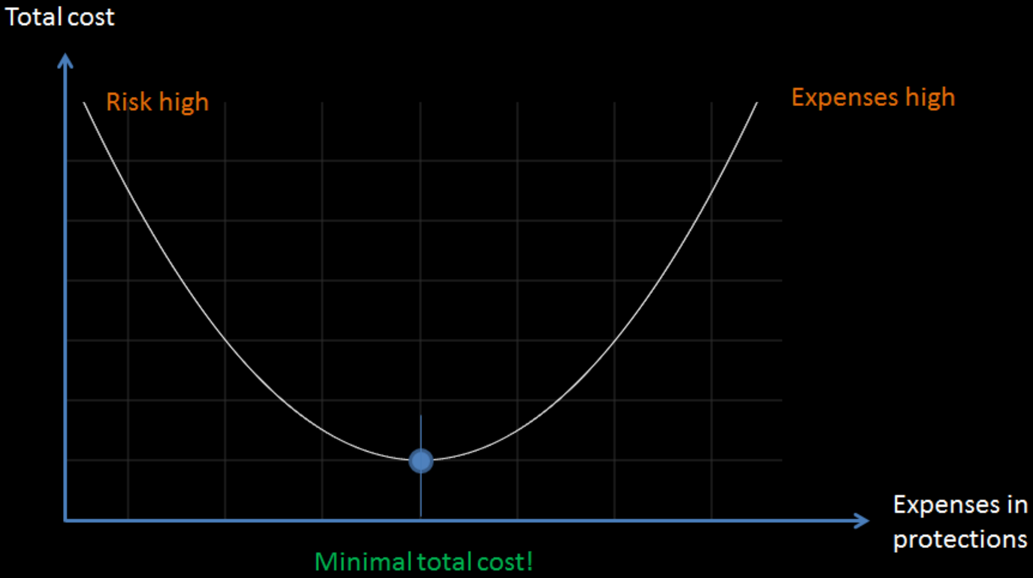
Facing risks, different paths can be taken:

- **Avoiding** : run away. fast. don't look back.
- **Transfer** : throw the hot potato to someone else (assurance,...) ;
- **Control** : take care of the threat (repel, fix, detect) ;
- **Accept** : shit happens, just pay the price.

Each of these options has a cost.

Information security in a nutshell: REMEMBER THIS.
Goal 1: Know the risks.
Goal 2: Minimise the costs.

Risks and mitigation



Security is trying to stop losing money

Three important consequences REMEMBER THIS:

- The expression “perfect security” is probably meaningless
- Within a budget, you have to choose what to protect and what to leave open
- “Being secure” is also meaningless unless we specify
    - against what specific incident or family of incidents
    - to what extent the protection holds

Marketing and corporate talk about this is a mental cancer.

Table of Contents

Security: a definition?

Information-related risks

Risks and Mitigation

An asymmetric relation

Threats, targets and adversaries

- Threat exposure

Dynamics and Macro-scale

The “victim’s” point of view

Risks, actually

Net and direct losses

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

Indirect losses

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

Indirect losses

2014 Zurich Insurance : 46000 identities leaked, the company was fined £2.3M

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

Indirect losses

2014 Zurich Insurance : 46000 identities leaked, the company was fined £2.3M

2014 Apple ‘Fappening’ : 100+ accounts compromised, stock option plummets

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

Indirect losses

2014 Zurich Insurance : 46000 identities leaked, the company was fined £2.3M

2014 Apple ‘Fappening’ : 100+ accounts compromised, stock option plummets

2009 Google (+40 other large US-based tech firms) : IP stolen 2009

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

Indirect losses

2014 Zurich Insurance : 46000 identities leaked, the company was fined £2.3M

2014 Apple ‘Fappening’ : 100+ accounts compromised, stock option plummets

2009 Google (+40 other large US-based tech firms) : IP stolen 2009

2009 Stuxnet : nuclear sabotage in 2009

The “victim’s” point of view

Risks, actually

Net and direct losses

- About \$ 10^{11} per year over the world (Source: McAfee)
- More than 3 G€/yr for Germany alone (Source: BMWi)
- More than M€ *per intrusion* in the USA in 2013 (Source: Ponemon/Symantec)

Indirect losses

2014 Zurich Insurance : 46000 identities leaked, the company was fined £2.3M

2014 Apple ‘Fappening’ : 100+ accounts compromised, stock option plummets

2009 Google (+40 other large US-based tech firms) : IP stolen 2009

2009 Stuxnet : nuclear sabotage in 2009

Fines, reputation, prosecution, destruction, etc. are at stake, too.

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)
- Ideology

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)
- Ideology
- Power or Coercion

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)
- Ideology
- Power or Coercion
- Ego

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)
- Ideology
- Power or Coercion
- Ego

In short: **MICE**.

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)
- Ideology
- Power or Coercion
- Ego

In short: **MICE**.

On certain black markets, a complete identity leak (a “DOX”) is worth around 4000€.

The “attacker’s” side

Motivations and risks

The main motivations for cybercriminals are thought to be:

- Money (by far the most powerful incentive)
- Ideology
- Power or Coercion
- Ego

In short: **MICE**.

On certain black markets, a complete identity leak (a “DOX”) is worth around 4000€. This should be put in perspective with the ∼30k leaks/incident in 2013 (Source: Ponemon/Symantec).

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)
- Organisations having a high symbolic value (religious, political, ...)

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)
- Organisations having a high symbolic value (religious, political, ...)
- High-profile individuals

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)
- Organisations having a high symbolic value (religious, political, ...)
- High-profile individuals

In the process of attacking these targets, there is oftentimes collateral damage done:

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)
- Organisations having a high symbolic value (religious, political, ...)
- High-profile individuals

In the process of attacking these targets, there is oftentimes collateral damage done:

- Low-profile individuals

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)
- Organisations having a high symbolic value (religious, political, ...)
- High-profile individuals

In the process of attacking these targets, there is oftentimes collateral damage done:

- Low-profile individuals
- Small and medium businesses

The “attacker’s” side

Main targets

The main targets are those most likely to satisfy the motivations discussed previously:

- Industrialised countries: USA, Western Europe, Russian Federation, China, ...
- High value-added industries (banks, etc.)
- Organisations having a high symbolic value (religious, political, ...)
- High-profile individuals

In the process of attacking these targets, there is oftentimes collateral damage done:

- Low-profile individuals
- Small and medium businesses
- NGOs, associations

Unlike larger organisations, those are rarely prepared and cannot efficiently face such an attack.

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

- Direct steal (Swift, Target, bitcoin), ransom (WannaCry), credit...

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

- Direct steal (Swift, Target, bitcoin), ransom (WannaCry), credit...
- Selling something that's profitable to the buyer: IP, blueprints, photos, financial info...

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

- Direct steal (Swift, Target, bitcoin), ransom (WannaCry), credit...
- Selling something that's profitable to the buyer: IP, blueprints, photos, financial info...
- Selling nuisance: degradation of/paralysing a competitor...

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

- Direct steal (Swift, Target, bitcoin), ransom (WannaCry), credit...
- Selling something that's profitable to the buyer: IP, blueprints, photos, financial info...
- Selling nuisance: degradation of/paralysing a competitor...
- Selling something the buyer can use to cause nuisance: vulnerabilities...

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

- Direct steal (Swift, Target, bitcoin), ransom (WannaCry), credit...
- Selling something that's profitable to the buyer: IP, blueprints, photos, financial info...
- Selling nuisance: degradation of/paralysing a competitor...
- Selling something the buyer can use to cause nuisance: vulnerabilities...
- Using info to get more or better info: keys (SecurID), blackmail...

Does crime pay?

How to get rich with information? Wherefore comes its value/price?

- Direct steal (Swift, Target, bitcoin), ransom (WannaCry), credit...
- Selling something that's profitable to the buyer: IP, blueprints, photos, financial info...
- Selling nuisance: degradation of/paralysing a competitor...
- Selling something the buyer can use to cause nuisance: vulnerabilities...
- Using info to get more or better info: keys (SecurID), blackmail...

Every middleman/middlewoman takes a percentage, hence prices increase.

Example: a PAN only can be sold 240 EUR in Europe.

Question : Who's buying?

Risks and threats

Criminology 101

Risks do not fall from the sky

Risks and threats

Criminology 101

Risks do not fall from the sky (well, most of the time)

Risks and threats

Criminology 101

Risks do not fall from the sky (well, most of the time)

We will almost exclusively consider *adversarial* situations, where the danger is cause by an *active, reactive, cunning* opponent trying to undermine our operations.

Risks and threats

Criminology 101

Risks do not fall from the sky (well, most of the time)

We will almost exclusively consider *adversarial* situations, where the danger is cause by an *active, reactive, cunning* opponent trying to undermine our operations.

As a consequence, risk analysis requires a good understanding of the *threat landscape* and *adversary models*.

Table of Contents

Security: a definition?

Information-related risks

Risks and Mitigation

An asymmetric relation

Threats, targets and adversaries

- Threat exposure

Dynamics and Macro-scale

Refining risk analysis

In order to get a finer picture of the risk profile, we will mostly use:

- A threat exposure model
- Adversary models

(It's not perfect, but it'll help)

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)
- We **embody** something an adversary may despise (religion, capitalism, nuclear power...)

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)
- We **embody** something an adversary may despise (religion, capitalism, nuclear power...)
- We **give in** to opportunism due to carelessness.

Threat exposure

The “No Sharks on Mt Everest principe”

A *threat* is something that produces danger.
The probability of encountering a danger is modulated by *threat exposure*.

Threat exposure increases, and therefore risk increases, in situations where:

- We are **close** to the threat source
- We **own** something that an adversary may envy (money, IP, fame, ...)
- We **embody** something an adversary may despise (religion, capitalism, nuclear power...)
- We **give in** to opportunism due to carelessness.

The risk profile can be refined to take into account a specific exposure situation, therefore enabling to better focus investments.

Threat exposure: an example

How is shaped the IT threat landscape for :

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?
- Hospitals and clinics?

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?
- Hospitals and clinics?
- Schools, universities, museums?

Threat exposure: an example

How is shaped the IT threat landscape for :

- Financial institutions?
- Large software companies (Adobe, Google, Facebook...)?
- GMO-producing firms? Car companies?
- Nuclear plants?
- Hospitals and clinics?
- Schools, universities, museums?

Table of Contents

Security: a definition?

Information-related risks

Risks and Mitigation

An asymmetric relation

Threats, targets and adversaries

- Threat exposure

Dynamics and Macro-scale

What drives it all

- Micro-level: *economical incentives* → Economics
- Macro-level: *political goals* → Geopolitics

What drives it all

- Micro-level: *economical incentives* → Economics
- Macro-level: *political goals* → Geopolitics

Security is a chess game where technology is the board and pieces.

What drives it all

- Micro-level: *economical incentives* → Economics
- Macro-level: *political goals* → Geopolitics

Security is a chess game where technology is the board and pieces.

We'll talk about strategies a bit later.

Know thy enemy: Demographics of cybercriminality

Q: What does the average cybercriminal look like?

Know thy enemy: Demographics of cybercriminality

Q: What does the average cybercriminal look like?

A: Like anyone else.

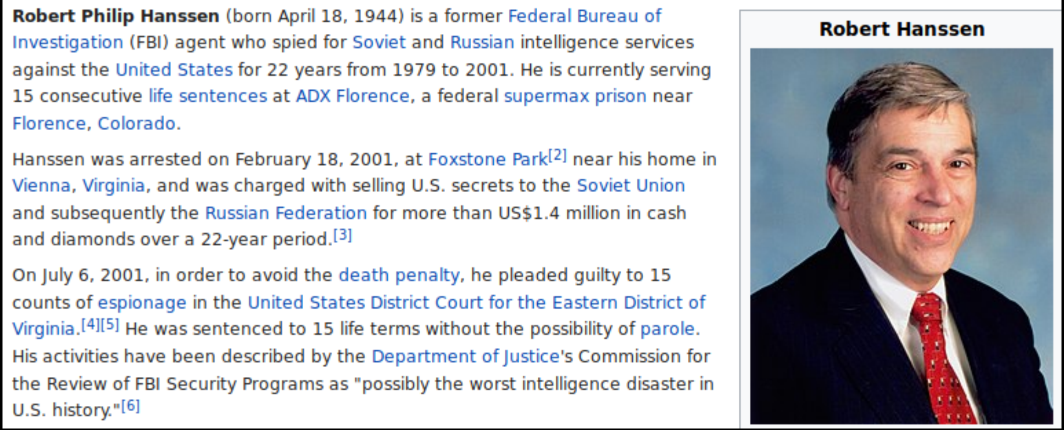
In about 50% of cases, she is an employee of the organisation she attacks.

Know thy enemy: Demographics of cybercriminality

Q: What does the average cybercriminal look like?

A: Like anyone else.

In about 50% of cases, she is an employee of the organisation she attacks.



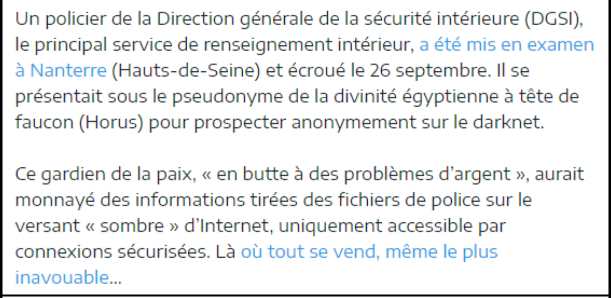
Robert Philip Hanssen (born April 18, 1944) is a former Federal Bureau of Investigation (FBI) agent who spied for Soviet and Russian intelligence services against the United States for 22 years from 1979 to 2001. He is currently serving 15 consecutive life sentences at ADX Florence, a federal supermax prison near Florence, Colorado.

Hanssen was arrested on February 18, 2001, at Foxstone Park[2] near his home in Vienna, Virginia, and was charged with selling U.S. secrets to the Soviet Union and subsequently the Russian Federation for more than US$1.4 million in cash and diamonds over a 22-year period.[3]

On July 6, 2001, in order to avoid the death penalty, he pleaded guilty to 15 counts of espionage in the United States District Court for the Eastern District of Virginia.[4][5] He was sentenced to 15 life terms without the possibility of parole. His activities have been described by the Department of Justice's Commission for the Review of FBI Security Programs as "possibly the worst intelligence disaster in U.S. history."[6]

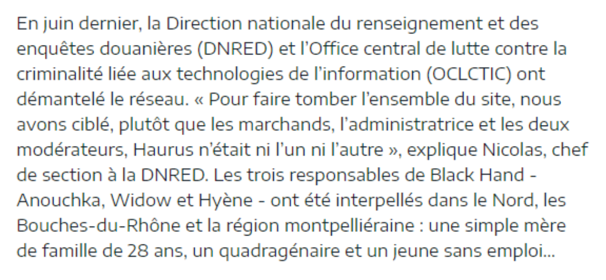
Robert Hanssen

Know thy enemy: Demographics of cybercriminality



Un policier de la Direction générale de la sécurité intérieure (DGSI), le principal service de renseignement intérieur, a été mis en examen à Nanterre (Hauts-de-Seine) et écroué le 26 septembre. Il se présentait sous le pseudonyme de la divinité égyptienne à tête de faucon (Horus) pour prospecter anonymement sur le darknet.

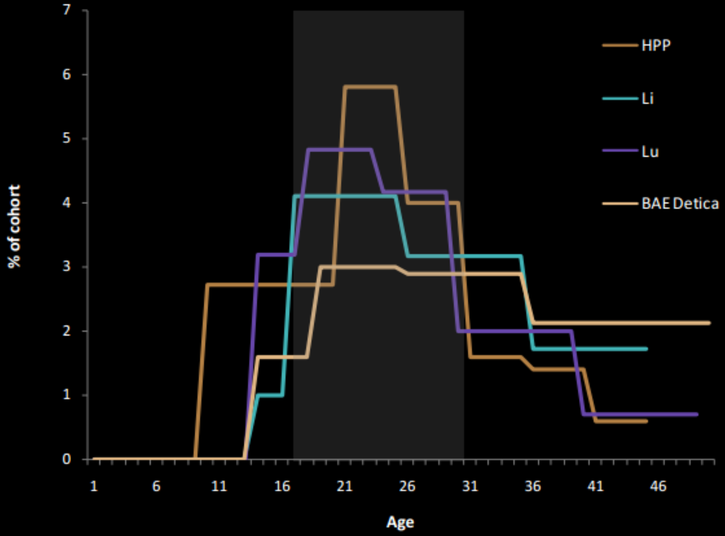
Ce gardien de la paix, « en butte à des problèmes d'argent », aurait monnayé des informations tirées des fichiers de police sur le versant « sombre » d'Internet, uniquement accessible par connexions sécurisées. Là où tout se vend, même le plus inavouable...



En juin dernier, la Direction nationale du renseignement et des enquêtes douanières (DNRED) et l'Office central de lutte contre la criminalité liée aux technologies de l'information (OCLCTIC) ont démantelé le réseau. « Pour faire tomber l'ensemble du site, nous avons ciblé, plutôt que les marchands, l'administratrice et les deux modérateurs, Haurus n'était ni l'un ni l'autre », explique Nicolas, chef de section à la DNRED. Les trois responsables de Black Hand - Anouchka, Widow et Hyène - ont été interpellés dans le Nord, les Bouches-du-Rhône et la région montpelliéraine : une simple mère de famille de 28 ans, un quadragénaire et un jeune sans emploi...

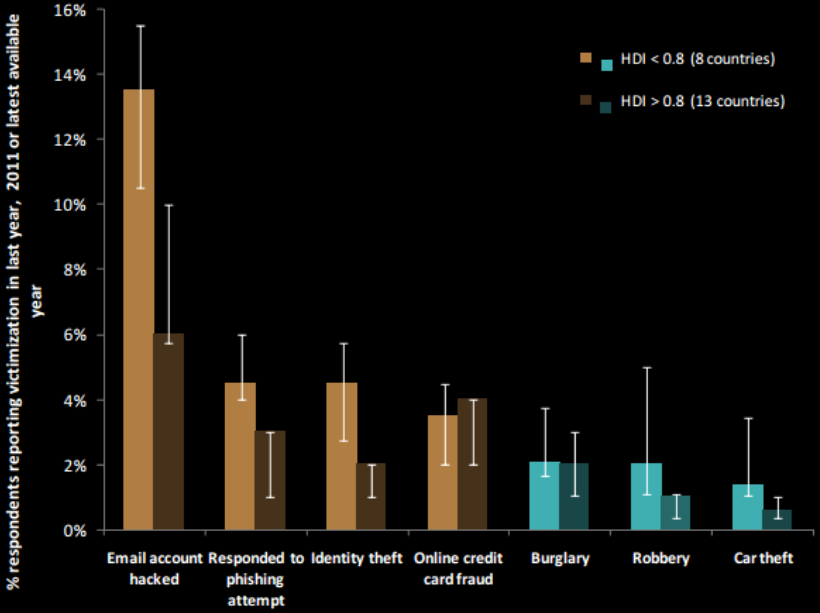
Know thy enemy: Demographics of cybercriminality

In the 50 other %,



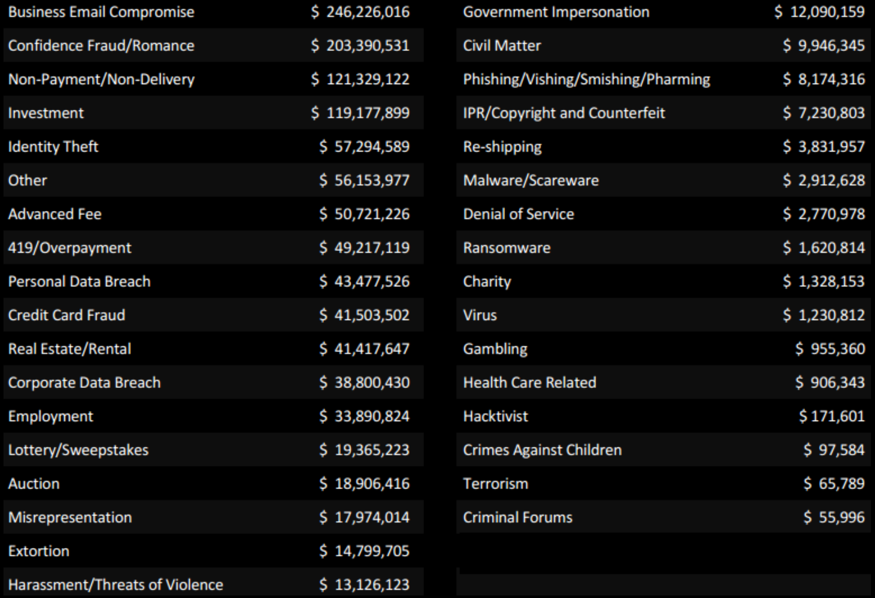
Source: UNODC elaboration of HPP, Li, Lu and BAE Detica

“Cyber”-crime ?



Source: UNODC elaboration of Norton Cybercrime Report and crime victimization surveys.

"Cyber"-victims?

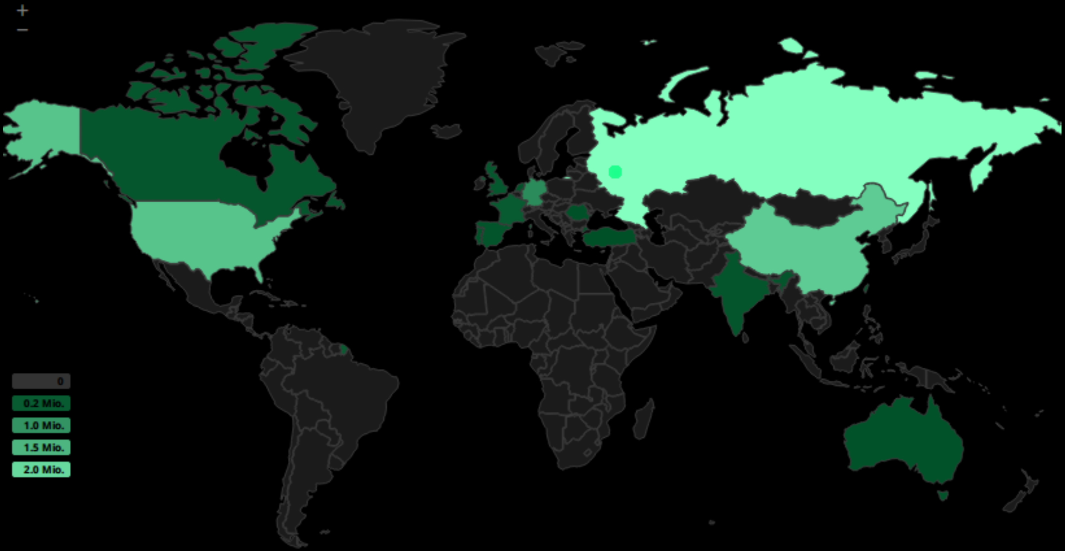


Business Email Compromise	$ 246,226,016	Government Impersonation	$ 12,090,159
Confidence Fraud/Romance	$ 203,390,531	Civil Matter	$ 9,946,345
Non-Payment/Non-Delivery	$ 121,329,122	Phishing/Vishing/Smishing/Pharming	$ 8,174,316
Investment	$ 119,177,899	IPR/Copyright and Counterfeit	$ 7,230,803
Identity Theft	$ 57,294,589	Re-shipping	$ 3,831,957
Other	$ 56,153,977	Malware/Scareware	$ 2,912,628
Advanced Fee	$ 50,721,226	Denial of Service	$ 2,770,978
419/Overpayment	$ 49,217,119	Ransomware	$ 1,620,814
Personal Data Breach	$ 43,477,526	Charity	$ 1,328,153
Credit Card Fraud	$ 41,503,502	Virus	$ 1,230,812
Real Estate/Rental	$ 41,417,647	Gambling	$ 955,360
Corporate Data Breach	$ 38,800,430	Health Care Related	$ 906,343
Employment	$ 33,890,824	Hacktivist	$ 171,601
Lottery/Sweepstakes	$ 19,365,223	Crimes Against Children	$ 97,584
Auction	$ 18,906,416	Terrorism	$ 65,789
Misrepresentation	$ 17,974,014	Criminal Forums	$ 55,996
Extortion	$ 14,799,705		
Harassment/Threats of Violence	$ 13,126,123		

Victim loss per crime type in 2015. Source: FBI.

Geopolitics

Inter-state cyberwars



Source of attacks against Germany as of 09.2014 (source : honeymap)

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning):

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning):

- United States of America

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning):

- United States of America
- China

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning):

- United States of America
- China
- Russian Federation

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning):

- United States of America
- China
- Russian Federation

They also happen to be the top 3 targets.

Inter-state cyberwars

The invisible casualties

Top 3 attackers (as of this morning):

- United States of America
- China
- Russian Federation

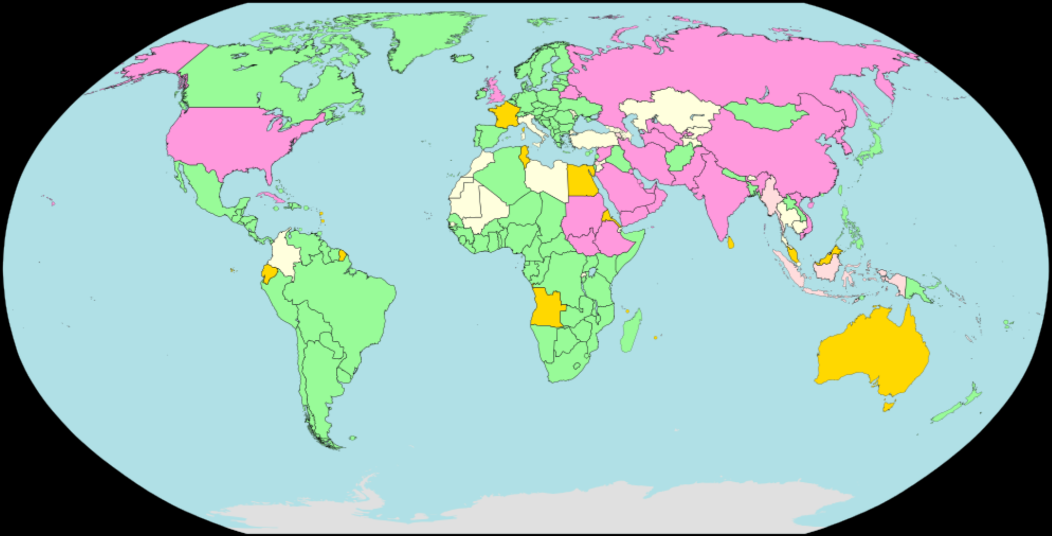
They also happen to be the top 3 targets.

You can check out `http://www.digitalattackmap.com/` or `http://map.ipviking.com/` for a nice, but misleading, view

Two factors: covert wars (metal-cold war) and internal attacks.

Intra-state cyberwars

They are not Charlie



Hindrances to freedom of information, surveillance and censorship in 2014 (source : Reporters sans Frontières)

Cyberwarfare

Since 2006 (Operation Olympic Games), all nation states engage at some level in economic and diplomatic operations through the abuse of vulnerabilities in information systems, which can escalate to physical destruction.

The targets of these attacks are not necessarily military installations. In the last few years, this phenomenon has grown to represent a large fraction of all attacks, and the prime threat to large organisations.

OK so what do we do?

The market is rigged against us, so what can we do?

- Punitive: make criminals pay for it
  - Penalise commercial exploitation of stolen data (e.g. forgery, exclusivity rights, copyright...) ?
  - Penalise abuse of sensitive or personal data (e.g. GDPR) ?
  - Penalise intrusion, even when no data was stolen or altered (L323) ?
  - Penalise more (LPM) ? Penalise preventively ? Setup international laws (e.g. Budapest, Wassenaar) ? Prosecute more and better?
  - Force manufacturers to internalise the cost of security?
- Preventive: make it hard/uninteresting to be a criminal
  - Design better technology or use it appropriately? ← **Crypto/Security**
  - Don't teach security (Australia)?
  - Defuse data by making it less useful ?
  - Reduce unemployment in some parts of the world?

Pause

||

See you in 10