OSY.SSI[2015][2]

Economy, part I

Table of Contents

The “victim’s” point of view

The “attacker’s” side

Economy

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 Geur/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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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 Geur/yr for Germany alone (Source: BMWi)
- More than Meur *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.

Table of Contents

The “victim’s” point of view

The “attacker’s” side

Economy

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 4000eur.

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 4000eur.
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.

Table of Contents

The “victim’s” point of view

The “attacker’s” side

Economy

Economy

The governing equation: predator-prey, part I

Attackers have to invest efforts so as to succeed.

Economy

The governing equation: predator-prey, part I

Attackers have to invest efforts so as to succeed. However, attacking is itself a risky business.

Economy

The governing equation: predator-prey, part I

Attackers have to invest efforts so as to succeed. However, attacking is itself a risky business.
On the attackers' side, the expected gain of a certain campaign is computed as:

$$\text{Gain} = \text{Loot} - \text{Investment} - \text{Risk}$$

In most cases, the low risk and high loot value make it worth the investment.

Economy

The governing equation: predator-prey, part II

On the defender's side, investments aim at protecting against risks.

Economy

The governing equation: predator-prey, part II

On the defender's side, investments aim at protecting against risks.

Too little spent on protection, and risks prevail.

Economy

The governing equation: predator-prey, part II

On the defender's side, investments aim at protecting against risks. Too little spent on protection, and risks prevail. Too much spent on protection, and money is lost.

Economy

The governing equation: predator-prey, part II

On the defender's side, investments aim at protecting against risks. Too little spent on protection, and risks prevail. Too much spent on protection, and money is lost.

There is a *sweet spot* where the defender spends just the right amount.

Economy

The governing equation: predator-prey, part II

On the defender's side, investments aim at protecting against risks. Too little spent on protection, and risks prevail. Too much spent on protection, and money is lost.

There is a *sweet spot* where the defender spends just the right amount.

The mathematical Gordon-Loeb model gives a simple estimation of that value:

$$\text{Optimal investment in protection} \simeq \frac{1}{e}\text{Risk}$$

Economy

The governing equation: predator-prey, part III

If attackers decide to attack, they increase the risk for the defender.

Economy

The governing equation: predator-prey, part III

If attackers decide to attack, they increase the risk for the defender.

However, the defender cannot influence the attacker's equation.

Economy

The governing equation: predator-prey, part III

If attackers decide to attack, they increase the risk for the defender.

However, the defender cannot influence the attacker's equation.

This is the first *fundamental economic asymmetry* between attackers and defenders.

Furthermore, the gains of the attacker are generally unrelated to the losses of the defender. This is the second fundamental economic asymmetry.

Economy

What these asymmetries mean

1. That a defender is *passive* w.r.t. threats.

Economy

What these asymmetries mean

1. That a defender is *passive* w.r.t. threats.
   - Curbing criminality requires *external, active* operations.
2. That there will always be temptation for fraud, like it or not.