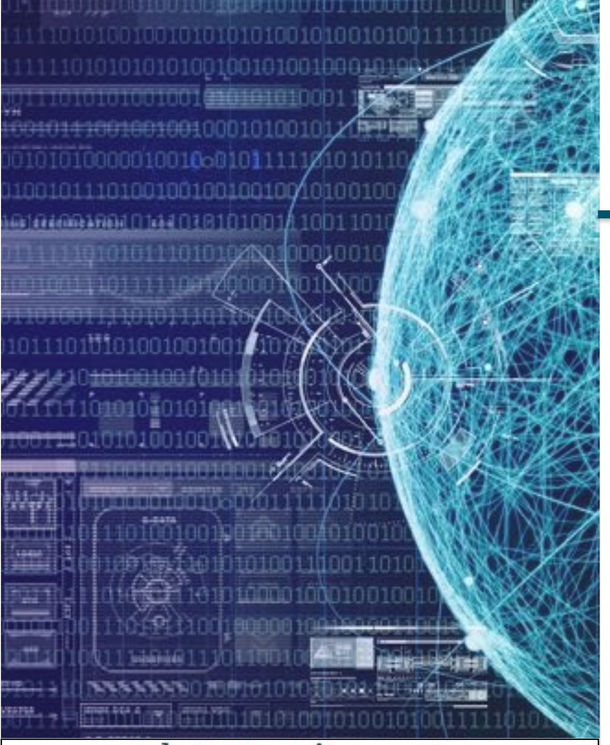


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

CyberSecuritySoton.org [w]

@CybSecSoton [fb & tw]

UNIVERSITY OF Southampton

# COMP6224 (2016)
# week 6: Economics

Vladimiro Sassone
Cyber Security Centre
University of Southampton

"often systems fail because of misplaced economic incentives: the people who could protect a system are not the ones who suffer the cost of failure" (Bruce Schneier)

Investing in cyber security

**Table 9-1. Influences on Cybersecurity Investment Strategy (adapted from [ROW06])**

| Categories of Influence | Average Percentage Across Organizations |
|---|---|
| Regulatory requirement | 30.1 % |
| Network history or information technology staff knowledge | 18.9 % |
| Client requirement or request | 16.2 % |
| Result of internal or external audit | 12.4 % |
| Response to current events, such as media attention | 8.2 % |
| Response to compromised internal security | 7.3 % |
| Reaction to external mandate or request | 5.0 % |
| Other | 1.7 % |

# how to decide how much to invest?

A **business case** for a given expenditure is a proposal that justifies the use of resources. It usually includes the following items:

- a description of the problem or need to be addressed by the expenditure
- a list of possible solutions
- constraints on solving the problem
- a list of underlying assumptions
- analysis of each alternative, including risks, costs, and benefits
- a summary of why the proposed investment is good for the organisation

- Need data on risks and costs of incidents:
  - data => models => projections/predictions

# considering all aspects

Evaluation of an existing or proposed investment in technology should be reported in several ways at once to form a "balanced scorecard":

- from a *customer* view, addressing issues such as customer satisfaction
- from an *operational* view, looking at an organisation's core competencies
- from a *financial* view, considering measures such as return on investment or share price
- from an *improvement* view, assessing how the investment will affect market leadership and added value

It is typical for companies to focus exclusively on return on investment, in part because the other views are less tangible.

# determining economic value

## Net present value (NPV)

present value of the investment minus value initial investment: compares a £ today with a £ in the future, taking all into account (project, inflation, returns,…)

## Internal rate of return (IRR)

equals the return rate (% of return from investment) that makes NPV equal to zero

## Return on Investment (ROI)

(profit last period) / (investment required to generate it)

# determining economic value

## Net present value (NPV)

present value of the investment minus value initial investment: compares a £ today with a £ in the future, taking all into account (project, inflation, returns,…)

## Internal rate of return (IRR)

equals the return rate (% of return from investment) that makes NPV equal to zero

ROI looks back at performance of investment
NPV and IRR look at likely future performance

CSI/FBI computer security survey (2005):
ROI: 38% IRR: 19% NPV: 18%

## Return on Investment (ROI)

(profit last period) / (investment required to generate it)

# NPV makes good sense

**Example**:

rationale for spending 100 units today suggests a benefit of 200 units five years from now. To assess the overall project benefit, we must adjust the 200 units for inflation and the interest or growth the firm would gain on the 100 units over five years.

Suppose 100 units invested traditionally yield 170 units in five years. Then the present value of the proposed project is only 30 units (200 - 170)

**Formula to estimate NPV:**

# NPV makes good sense

**Example**:

rationale for spending 100 units today suggests a benefit of 200 units five years from now. To assess the overall project benefit, we must adjust the 200 units for inflation and the interest or growth the firm would gain on the 100 units over five years.

Suppose 100 units invested traditionally yield 170 units in five years. Then the present value of the proposed project is only 30 units (200 - 170)

**Formula to estimate NPV:**

$$-C_0 + \sum_{t=1}^{n} (B_t - C_t)/(1+k)^t$$

# NPV example

The chief security officer is considering protecting its networks by:

1. buy an off-the-shelf intrusion detection system: large initial procurement cost, high returns (based on avoided work), but the off-the-shelf product must be replaced after 3 years
2. build own intrusion detection system with a reusable design: considerable up-front costs for design and documentation, but product's life will be longer.

# NPV example

The chief security officer is considering protecting its networks by:

1. buy an off-the-shelf intrusion detection system: large initial procurement cost, high returns (based on avoided work), but the off-the-shelf product must be replaced after 3 years
2. build own intrusion detection system with a reusable design: considerable up-front costs for design and documentation, but product's life will be longer.

**Table 9-2. Net Present Value Calculation for Two Alternatives**

| Cash Flows | Choice 1: Buy IDS Software | Choice 2: Build IDS Software |
|---|---|---|
| *Initial Investment* | -$9,000 | -$4,000 |
| *Year 1* | $5,000 | -$2,000 |
| *Year 2* | $6,000 | $2,000 |
| *Year 3* | $7,000 | $4,500 |
| *Year 4* | -$4,000 | $6,000 |
| Sum of all cash flows | $5,000 | $6,500 |
| NPV at 15% | $2,200 | $2,162 |

# difficult to estimate costs fairly

the number of factors is huge, the effects are vast

eg, for the intrusion system the number of (false) alarms triggered has direct impact on the staff you need to hire:

better system => higher investment => lower running costs

it may be difficult to separate security effects from more general ones, e.g. improved efficiency, functionality, access to assets, etc…

# four elements to cost/benefit analysis

UNIVERSITY OF Southampton

**Revenue:**

increased security => increased trust => increased revenue

**Costs:**

broader than purchase, installation, operation, maintenance:
includes savings; cost avoidance; efficiency; effectiveness

**Compliance:**

with regulations, laws, …:
avoids fines, court cases, bad publicity, lost business, …

**Risk:**

consequences of not implementing security:
loss of market share, productivity, legal exposure

Possible approach: establish baseline of cost, then sample and measure to determine if and how security changes the baseline…

# Very hard, but must be done!

**Issues**: *prevention, detection, mitigation, recovery*: in order to have meaningful (quantitative) risk assessment, one needs models, and models must be derived from data.

**Data** must be: *accurate, consistent, timely, reliable*.

Need to estimate:

- number/types of assets needing protection
- number/types of vulnerabilities in a system
- number/types of likely threats in a system

The book provides some interesting survey as source of data; do not forget we have seen recent data from Mandiant too.

# key findings from some surveys

- Viruses are the largest source of financial loss. Unauthorised access showed dramatic gains, replacing denial of service as the second greatest source of loss.
- The total dollar amount of financial loss from cyber crime is decreasing.
- The reporting of intrusions continues to decrease, for fear of negative publicity.
- Only 87 percent of respondents conduct security audits, up from 82 percent in the previous survey.
- Only 35 percent of respondents experienced attacks that affected the confidentiality, availability, or integrity of their networks or data systems in 2005, compared with 49 percent in 2004 and 42 percent in 2003.
- The level of insider attacks has remained constant over three years, at 37 percent.
- Viruses were the most prevalent type of attack. Denial of service created the most financial loss.
- Only 37 percent of respondents used security standards in 2003, but 65 percent use them now.

# key findings from some surveys

- Organisations have hardened their systems, making them less attractive to security breaches.
- The weakest link is humans, not technology, particularly using phishing and pharming attacks.
- Only 17 percent of respondents overall deem government security-driven regulations as "very effective," and 50 percent "effective" in improving their organisation's security position or in reducing data protection risks.
- There is a trend toward having the chief information security officer report to the highest levels of the organisation.
- Most companies have no formal data backup and storage procedures in place. They rely instead on the initiative of individual employees.
- E-mail viruses are the primary reason to review and change data protection procedures.
- Regular testing of disaster recovery procedures is not yet a common practice.
- Security spending per user and per machine decreases as organisation size increases.
- Allocating money for security does not reduce the probability of being attacked but does help an organisation detect losses.
- Most organisations do not have a security culture or an incident response plan.

# key findings from some surveys

- Only one in five respondents strongly agreed that their organisations perceive information security as a priority at the highest corporate levels.
- Lack of security awareness by users was the top obstacle to effective information security. However, only 28 percent of respondents listed "raising employee information security training or awareness" as a top initiative in 2004.
- The top concern among respondents was viruses, Trojan horses, and Internet worms. A distant second was employee misconduct, regardless of geographic region, industry, or organisational size.
- Fewer than half of the respondents provided employees with ongoing training in security and controls.
- Only one in four respondents thought their information security departments were successful in meeting organisational security needs.
- One in ten respondents consider government security-driven regulations to be effective in improving security or reducing risk.

Cybersecurity economics is a nascent field aimed at building models to answer questions such as:

1. How much should an organisation invest in cybersecurity to protect assets of a given value?
2. What is the likely impact of a security breach?
3. What are the costs and benefits of sharing information?

Cybersecurity economics is a nascent field aimed at building models to answer questions such as:

1. How much should an organisation invest in cybersecurity to protect assets of a given value?
2. What is the likely impact of a security breach?
3. What are the costs and benefits of sharing information?

1. simple model of information protection

three parameters to ask how much to invest on a threat (no more than 36.8%, others say 50%, others 100%):

loss | breach has occurred

prob( threat occurs )

vulnerability = prob( threat succeed | threat occurs )

Cybersecurity economics is a nascent field aimed at building models to answer questions such as:

1. How much should an organisation invest in cybersecurity to protect assets of a given value?
2. What is the likely impact of a security breach?
3. What are the costs and benefits of sharing information?

## 2. economic effect of security breaches

not always have an impact on e.g. stock market value of a company: typically, only if the breaches involve the loss of confidential information.

Cybersecurity economics is a nascent field aimed at building models to answer questions such as:

1. How much should an organisation invest in cybersecurity to protect assets of a given value?
2. What is the likely impact of a security breach?
3. What are the costs and benefits of sharing information?

3. use game theory to analyse how competing companies choose investments levels and info sharing

higher level of spend & sharing triggers higher spend in others
info sharing & spend increase with the company size
there are strong incentives to share info about breaches

These are difficult models to design, as depend heavily on several aspect, including psychological ones

**Framing the issue:**

- when the payoff is small, people focus on the risk
- when the risk is small, people focus on the payoff

in general, the way an issue is presented influences the response: loss avoidance v business opportunities.
This leads to choices that seem irrational.

**Group behaviour:**

team reasoning; normative expectations; dominant members

**Credibility and trust:** trust as an economic issue

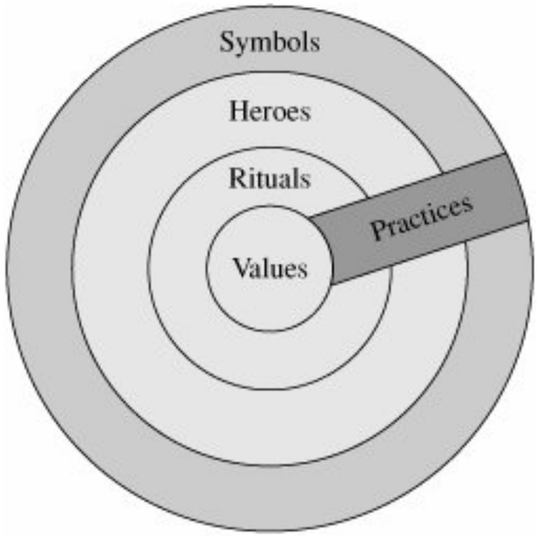
# the role of organisational culture

***Symbols:*** words, gestures, pictures and objects that carry specific meanings for a group.

***Heroes:*** people whose behaviours are highly prized, serving as role models in the group.

***Rituals:*** activities performed by all the group's members that are socially essential but not necessary to the business.

**Figure 9-1. Manifestations of National Culture [Hofstede and Hofstede 2005]**



# dimensions of organisational culture

**Table 9-4. Dimensions of Organizational Culture**

| Pole 1 | Pole 2 | Explanation |
|---|---|---|
| Process oriented | Results oriented | Means versus goals |
| Employee oriented | Job oriented | Concern for people versus concern for completing the job |
| Parochial | Professional | Identity from organization versus from the profession |
| Open system | Closed system | With respect to newcomers |
| Loose control | Tight control | With respect to employee autonomy |
| Normative | Pragmatic | Rule-based versus job-driven |

Organisational culture has a very significant impact on cyber security choices and investments

# dimensions of organisational culture

**Table 9-4. Dimensions of Organizational Culture**

| Pole 1 | Pole 2 | Explanation |
|---|---|---|
| Process oriented | Results oriented | Means versus goals |
| Employee oriented | Job oriented | Concern for people versus concern for completing the job |
| Parochial | Professional | Identity from organization versus from the profession |
| Open system | Closed system | With respect to newcomers |
| Loose control | Tight control | With respect to employee autonomy |
| Normative | Pragmatic | Rule-based versus job-driven |

Organisational culture has a very significant impact on cyber security choices and investments

**Table 9-5. Organizational Culture and Example Security Choices**

| Dimension | Choices |
|---|---|
| Process versus Results | Best practice versus<br>Testing and evaluation |
| Employee versus Job | Employee satisfaction versus<br>Milestones toward completion |
| Parochial versus Professional | Organizational rewards versus<br>Professional rewards and certification |
| Open versus Closed System | Hire from outside versus<br>Promote or retrain from within |
| Loose versus Tight Control | Self-organizing teams with little bureaucratic control versus<br>Managerially imposed teams with much reporting |
| Normative versus Pragmatic | Rule-based, "life cycle methodology" versus<br>Job-driven, "agile methods" |

# modern economics

Modern economics is a mathematical behavioural theory comprising a large body of work and techniques

So far, microeconomics and game theory have found significant applications to cyber security.

microeconomics is focussed on market efficiency:

- self-interest in free market => economic well-being
- specialisation => productivity gains
- *“it is not from the benevolent baker that we expect our dinner, but from their commitment to their self-interest”*

# market failures: monopolies

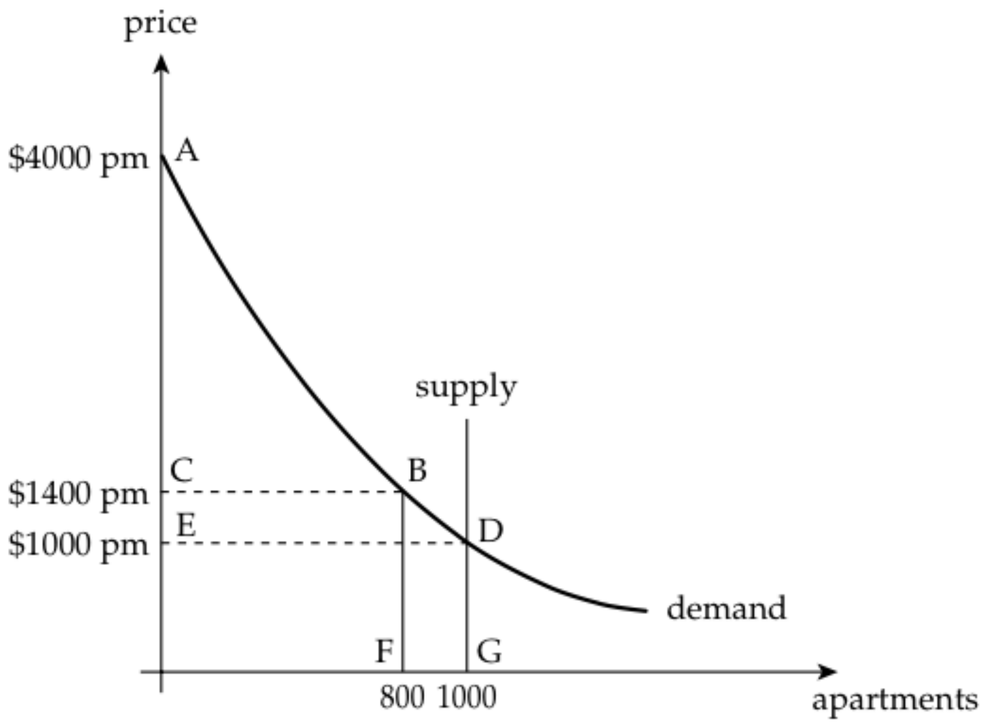



**Figure 7.1:** The market for apartments

supply/demand curve

in monopoly regime

# market failures: monopolies

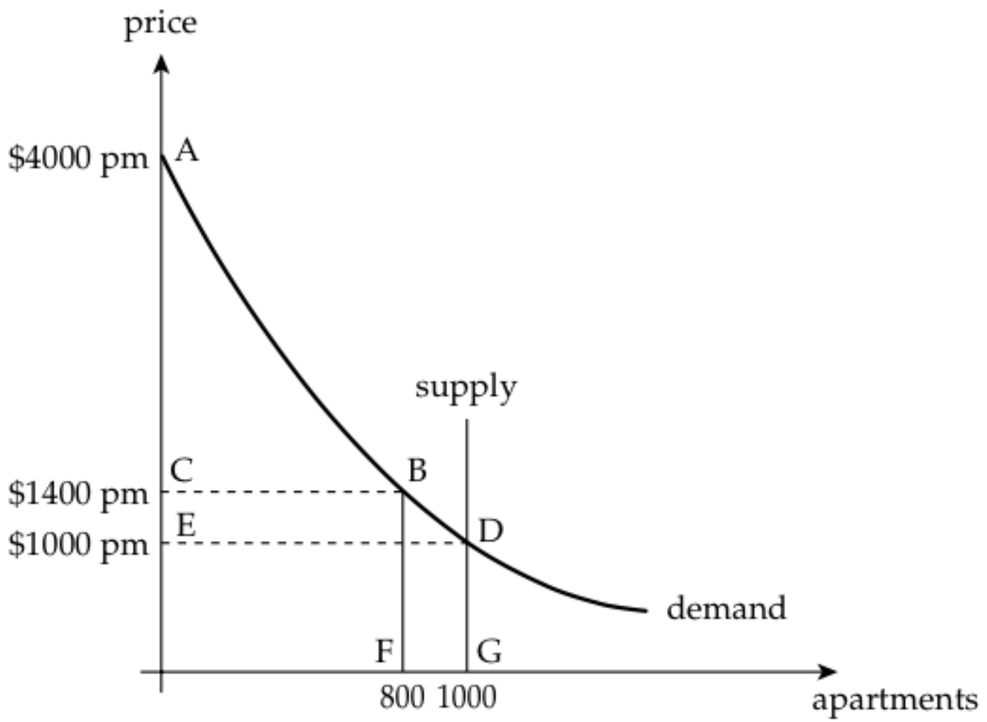



**Figure 7.1:** The market for apartments

**Pareto improvement:** a change that makes some people better off and nobody worse off

supply/demand curve

in monopoly regime

# market failures: monopolies

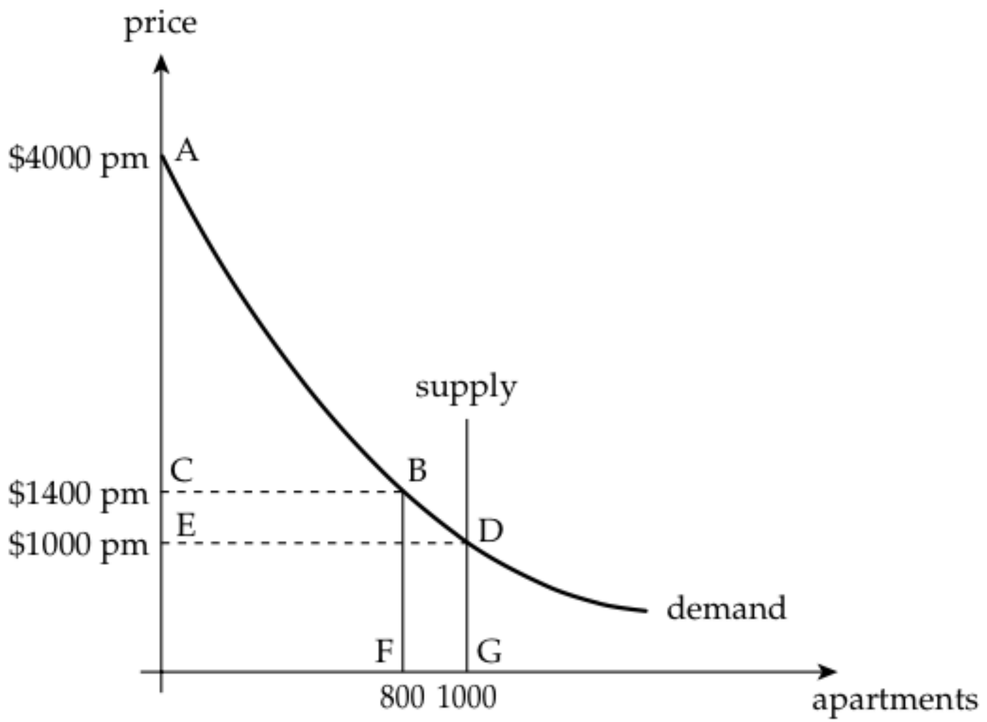



**Figure 7.1:** The market for apartments

**Pareto improvement:** a change that makes some people better off and nobody worse off

**Pareto efficient:** no Pareto improvement possible

supply/demand curve in monopoly regime

# market failures: monopolies

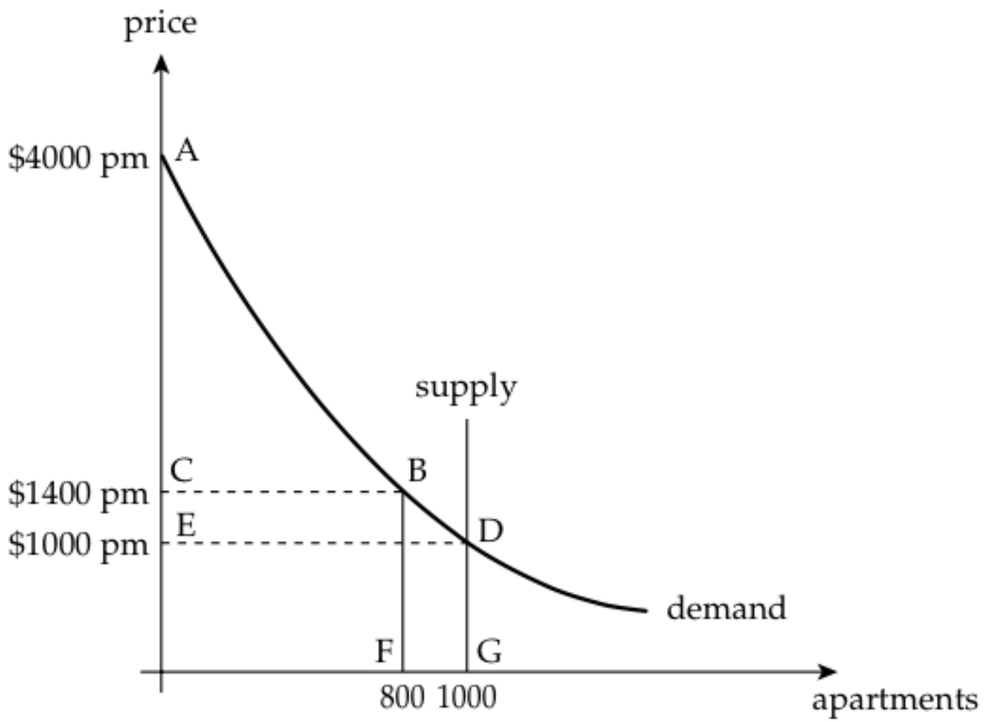



**Figure 7.1:** The market for apartments

supply/demand curve

in monopoly regime

**Pareto improvement:** a change that makes some people better off and nobody worse off

**Pareto efficient:** no Pareto improvement possible

**Price discrimination:** the monopolist charges to each the price they are prepared to pay

# market failure: public goods

These are markets where everybody gets the same quantity of a good, whether they want it or not.

air quality, national defence, scientific research, *cybersecurity*, …

Two approaches:

- authority taxes vulnerabilities, rewards researchers who find them, imposes fines on vulnerable software, etc
- `cap-and-trade' system: vendors who cannot make their software secure, "buy" permits from others to market insecure software.

game theory is the "study of problems of cooperation and conflict among independent decision makers"

- focus is on games of strategy, not games of chance
- main interest on games of imperfect information (unlike chess)

| | | Bob | |
|---|---|---|---|
| | | H | T |
| Alice | H | −1,1 | 1,−1 |
| | T | 1,-1 | −1,1 |

**Figure 7.2:** Matching pennies

- this is an example of a zero-sum game: "*your-loss-is-my-gain*"

| | | Bob | |
|---|---|---|---|
| | | Left | Right |
| Alice | Top | 1,2 | 0,1 |
| | Bottom | 2,1 | 1,0 |

**Figure 7.3:** Dominant strategy equilibrium

| | | Bob: Left | Bob: Right |
|---|---|---|---|
| Alice | Top | 1,2 | 0,1 |
| | Bottom | 2,1 | 1,0 |

**Figure 7.3:** Dominant strategy equilibrium

| | | Bob: Left | Bob: Right |
|---|---|---|---|
| Alice | Top | 2,1 | 0,0 |
| | Bottom | 0,0 | 1,2 |

**Figure 7.4:** Nash equilibrium

# the prisoners' dilemma

One-off games:

| | | Benjy: Confess | Benjy: Deny |
|---|---|---|---|
| Alfie | Confess | −3,−3 | 0,−6 |
| | Deny | −6,0 | −1,−1 |

Nobel Prize Winner

**Figure 7.5:** The prisoners' dilemma

Repeated games: tit-for-tat

| | Hawk | Dove |
|---|---|---|
| Hawk | $\frac{V-C}{2}, \frac{V-C}{2}$ | $V, 0$ |
| Dove | $0, V$ | $\frac{V}{2}, \frac{V}{2}$ |

**Figure 7.6:** The hawk-dove game

| | Hawk | Dove |
|---|---|---|
| Hawk | $\frac{V-C}{2}, \frac{V-C}{2}$ | $V, 0$ |
| Dove | $0, V$ | $\frac{V}{2}, \frac{V}{2}$ |

**Figure 7.6:** The hawk-dove game

if $V > C$, the whole population will become hawk,

if $C > V$ (fighting is too expensive) then there is an equilibrium where the probability $p$ that a bird is a hawk sets the hawk payoff and the dove payoff equal, that is

$$p\frac{V-C}{2} + (1-p)V = (1-p)\frac{V}{2}$$

which is solved by $p = V/C$.

# the price of information

The price of a good at equilibrium is the marginal cost of production, i.e. the cost producer who just manage to survive in business sell at.

# the price of information

The price of a good at equilibrium is the marginal cost of production, i.e. the cost producer who just manage to survive in business sell at.

The price of information is (almost) zero!

Companies give it away for free, and adopt a business model where money comes from some parallel market (typically advertising).

# the price of information

The price of a good at equilibrium is the marginal cost of production, i.e. the cost producer who just manage to survive in business sell at.

The price of information is (almost) zero!

Companies give it away for free, and adopt a business model where money comes from some parallel market (typically advertising).

What characteristics are important here?

1. network externalities: the value grows more than linearly with the number of users; reinforcement: network effect means that one cannot afford to be left out of the technology; e.g., developers develop for Windows because there is more users, and users buy Windows because there is more software.
2. technical lock-in: once a company is committed to using Windows, changing can be expensive

# the value of lock-in

The value of a company is total lock-in of all its customers.

Consider a firm with 100 users of Office, paid £500 per copy. It would save £50,000 moving to OpenOffice. It would do it if the total cost of doing it were less than that. In which case MS would lower the price. On the other hand, if the cost were more than £50,000 MS would raise the price.

This doesn't just apply to mobile phones, PCs, iPods, etc, but every technical system. That is why so much attention is give to antitrust suits. And why standards and commercial wars are waged and systems become more and more locked.

Locked system reduce opportunities and applications, several countries recognise engineers the legal right to reverse engineer.

# asymmetric information: market of lemons

The market for lemons (1970, nobel prize paper)

100 cars on sale, 50 good worth £2,000, 50 `lemons' worth £1,000. Sellers know which is which, buyers don't. What's the market price of car? Turns out is close to £1,000.

# asymmetric information: market of lemons

The market for lemons (1970, nobel prize paper)

100 cars on sale, 50 good worth £2,000, 50 `lemons' worth £1,000. Sellers know which is which, buyers don't. What's the market price of car? Turns out is close to £1,000.

# asymmetric information: market of lemons

The market for lemons (1970, nobel prize paper)

100 cars on sale, 50 good worth £2,000, 50 `lemons' worth £1,000. Sellers know which is which, buyers don't. What's the market price of car? Turns out is close to £1,000.

This is noticeable in cyber security: as users can't distinguish a good product from a bad one, prices are driven down and there is no incentive to make superior products.

# asymmetric information: market of lemons

The market for lemons (1970, nobel prize paper)

100 cars on sale, 50 good worth £2,000, 50 `lemons' worth £1,000. Sellers know which is which, buyers don't. What's the market price of car? Turns out is close to £1,000.

This is noticeable in cyber security: as users can't distinguish a good product from a bad one, prices are driven down and there is no incentive to make superior products.

Asymmetric information explains many market failures in the real world.

Banking was the industry that rekindled interest in security.

Whilst in the USA banks are liable for card fraud, this was not so in the UK. Yet, the UK spent more on security and suffered more frauds. This is a moral-hazard effect: UK staff knew that customers would not be taken seriously, and became careless, leading to an epidemic of fraud.

More in general the picture which emerges is that of security failing because the people guarding the system are not those paying the cost of failure.

Sometimes, security mechanisms are just used to lock-in users, or prevent reverse-engineering, or dump risks on others

# weakest link or sum of efforts?

Like in other contexts, security relies on different kind of efforts.

- program correctness can depend on minimum effort, the weakest link, the most careless programmer who introduces a vulnerability.
- security overall might depend on the “best-effort,” the champion that alone design a strong architecture.
- vulnerability testing depends on a sum-of-all-efforts.

As more staff are added, odds increase for sum-of-all-efforts, and decrease for the weakest link case.

companies should hire fewer but better programmers, and more software testers!

cybersecurity economics provides the ground to answer questions like:

- does opening up a system help more attackers or defenders?
- do public patchers and disclosures help or damage cyber security?
- why is software so full of vulnerabilities?

# why is windows so insecure?

combination of

high fixed costs, low marginal costs, network effect, and technical lock-in

makes platform likely to dominated by a single vendor, who stand to gain a huge fortune if they get there first and appeal to both customers and developers.

"*ship it Tuesday, and get it right by version 3*"

this is perfectly rational. And security gets in the way of applications. Market for lemons, dump security costs on users, etc, do the rest…

People say they value practice, but in practice they don't.

Modern view of privacy: consumers do not want to be bothered by irrelevant advertising, marketers do not want to waste effort: give consumers ownership of data, and allow them to lease it.

Current  privacy erosion is result of desire to charge different prices for the same service to different users: the old idea of price discrimination.

All these ideas are in flux, it will take time for people to assimilate the privacy risks: it was just for geeks only a few  back, it is clearly broadening now…

# summary

we have seen cybersecurity economics both as

- models, techniques, metrics to make and justify business cases for security products/ solutions;
- mechanisms to put the right incentives in security products/solutions.

Many systems fail because incentives are wrong, more than for technical mistakes. Cybersecurity must deal with basic economics as well as with basic crypto, protocols, access controls, psychology, …

This is a growing research area that is trying to explain many of the things so far considered just as `bad weather'