Information Technology in Practice: Risks and Strategic Flexibility

Dr. Marc Brandis

Zurich, 4 March 2024

CONTENTS

RISK CATEGORIES WITH PARTICULAR RELEVANCE FOR APPLIED INFORMATION TECHNOLOGY

IT Project Risks

- Project failure/cancellation
- Project budget and time overrun
- Results not fulfilling project objectives

Business Operational Risks

- Business loss, reputational damage, or financial damage due to outages
- Damage due to system malfunction

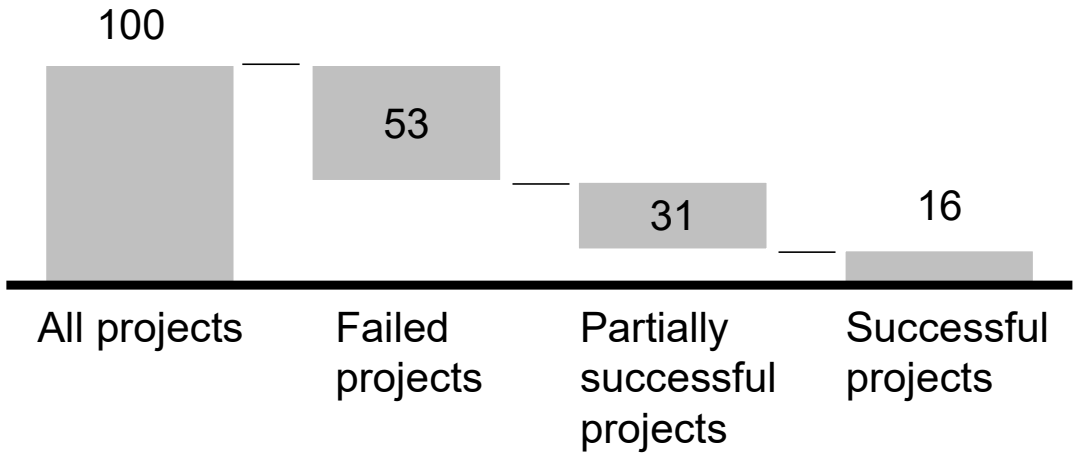
Cyber Risks

- Intrusion to cause damage
- Theft of intellectual property, business or customer data
- Device abuse (e.g. as part of a botnet)
- Ransom
- Collateral damage of unfocused attack

- Corporate risk management is a very broad topic
- This section only addresses these three risk categories with particular relevance for our discussions

IT PROJECT RISKS: SUCCESS RATE OF IT PROJECTS*

Evaluation of 500 projects of different types, in %



- Cost overrun on average 89%
- Time overrun on average 122%

Reasons for project failure

Incomplete requirements	13%
Insufficient user involvement	12%
Inadequate resources	11%
Unrealistic user expectations	10%
Insufficient management support	9%
Requirement changes	9%
Insufficient planning	8%

- Most reasons are at the inter-face business/IT

* See “Software Complexity” for further considerations on IT project risks
Source: Standish Group Survey

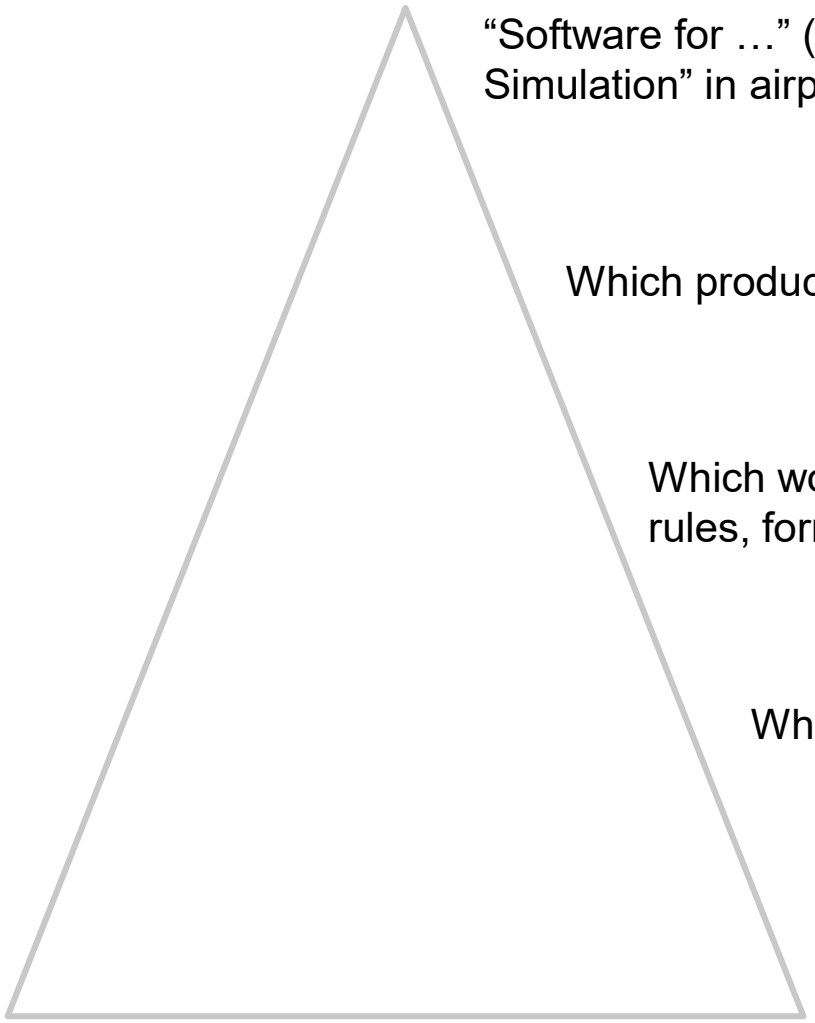
THE DIFFICULTY COLLECTING REQUIREMENTS: EXPERIENCES

BACKUP

- It is very difficult to obtain complete requirements, both for completely new systems as well as for replacement of existing systems
  - People cannot imagine everything they will need in a new system, and express it in a coherent manner
  - The more diverse the user community becomes, the harder it is
  - For systems having existed several years, both business staff as well as IT staff fully understanding their functionality have disappeared or do not remember all details anymore
- The difficulty often leads to excessive “flexibility” requirements, especially if users are pushed to sign-off the requirements
- Projects for multiple stakeholder groups are prone to scope creep
  - Requirements are not challenged
  - New requirements from one group lead to new ones in others as well

LEVELS OF ABSTRACTION FOR BUILDING SOFTWARE*

BACKUP



"Software for …" (e.g. "Claims Handling" in insurance, or "Aerodynamics Simulation" in airplane design)

– *Top Management*

Which products, processes, functionalities, …

– *Business Analysts*

Which workflows, interfaces, user screens visualizations, … and which rules, formulas, …

– *Requirements Engineers*

Which components, modules, … and which base technologies …

– *Software Architects*

Which data structures, algorithms, …

– *Software Engineers*

* The topic will be revisited with more detail in the software development and legacy software sessions of the lecture

BUSINESS OPERATIONAL RISKS

FINANCIALS

UBS to Take $356 Million Loss on Facebook IPO

Maria Bartiromo and Javier E. David
Published 6:01 PM ET Tue, 31 July 2012
CNBC

The fallout from the botched Facebook IPO continues as Swiss banking giant UBS announced it took a $356 million hit on the hotly-anticipated stock sale and that it intends to sue Nasdaq OMX Groupfor what it calls the stock market's "gross mishandling" of the deal.

The reported loss confirms earlier speculation that UBS's loss would top $350 million. Sources within the bank said UBS's trading desk electronically booked orders for Facebook stock, but failed to receive proper confirmation. That prompted traders to re-send the trades, leading to duplicated orders that far exceeded UBS's intended allocation, these people said.

They said UBS is confident that its trading desk was not at fault, which is why it's seeking to recoup its losses from Nasdaq in the courts.

However, UBS's loss from the trade was 10 times worse than other market makers, prompting speculation about how much Nasdaq may really be to blame. By comparison, Nasdaq's plan for compensating customers who lost money on the deal totals just $62 million.

Facebook's IPO was plagued by missteps and trading errors that caused other investors to be shut out of the deal altogether.

- The impact of problems with software can be very large (the mentioned loss accumulated in one day)
- It can lead to losses in multiple companies, and even litigation between them

TOP SOFTWARE FAILURES IN RECENT HISTORY

https://www.computerworld.com/article/3412197/top-software-failures-in-recent-history....

COMPUTERWORLD UNITED STATES IDG TECH(TALK) COMMUNITY WINDOWS MOBILE OFFICE SOFTWARE INSIDER

Home > Vertical Industries > Retail Industry

SLIDESHOW

Top software failures in recent history

The biggest software failures in recent history including ransomware attacks, IT outages and data leakages that have affected some of the biggest companies and millions of customers around the world

By Computerworld UK staff, Computerworld | Feb 17, 2020 6:20 am PST

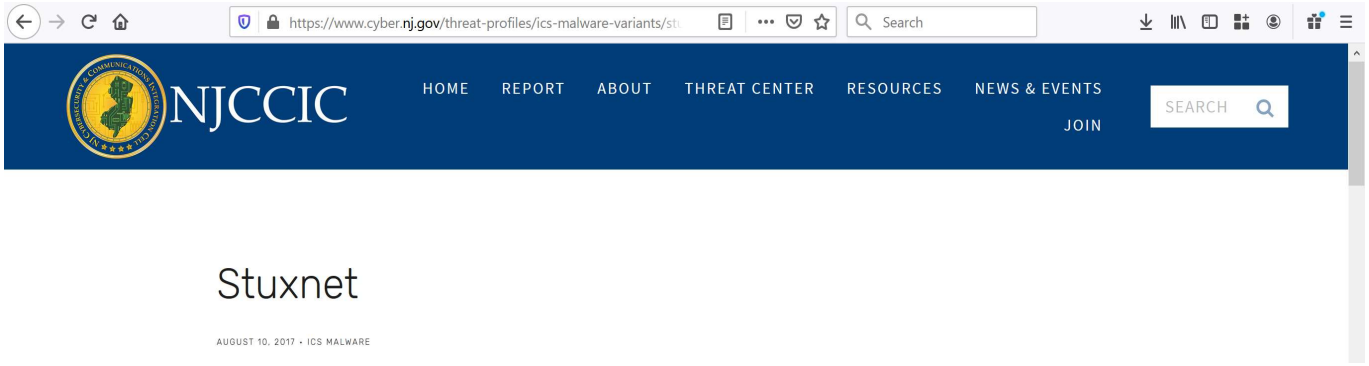
Technology, you can't live with it, you can't live without it. Unfortunately, millions of users around the world have come to realise the latter over recent years due to a series of spectacular, and thoroughly unwelcomed, failures.

Software failures have wreaked havoc at banks, airlines and the NHS, doing billions of pounds of damage and devastating disruption.

1. February 2020: Heathrow disruption
2. British Airways (again)
3. Facebook, Instagram and WhatsApp
4. O2
5. TSB Bank
6. Welsh NHS IT Failure
7. Meltdown & Spectre (Intel, and other chip designers)
8. WannaCry
9. Cloudbleed
10. Bitcoin Unlimited
11. British Airways
12. Nest thermostat leaves users in the cold
13. HSBC suffers major outage
14. …

- The press is full of reports about IT problems and related business problems
- Failures happen in companies large and small, across all (perceived) levels of sophistication, and all industries
- For the complete list with descriptions, see https://www.computerworld.com/article/3412197/top-software-failures-in-recent-history.html#slide1

PLANNED DAMAGE: STUXNET



Stuxnet is a computer worm, reportedly developed and launched by the United States and Israel, that specifically targets programmable logic controllers (PLCs) that control the automation of electromechanical processes, such as those used for centrifuges. It is considered to be the first cyberweapon used in the world due to its ability to cause physical destruction and the first known malware designed to infect industrial control systems (ICS).
[…]
Stuxnet was used specifically to target centrifuges at Iran's uranium enrichment facility outside Natanz, Iran. It manipulated valves on the centrifuges, increasing and decreasing their speed, putting additional pressure on them, and ultimately damaging the machines until they no longer functioned.
[…]
Leading up to the Stuxnet's main attack on Iran's centrifuges, Iran's uranium enrichment program was progressing well, and they were on track to install the 6,000 centrifuges that then-Iran President Ahmadinejad had promised. A version of Stuxnet was launched in late June 2009.
[…]
Between June and August, the number of running centrifuges at the plant decreased to just 4,592. By November, the number further reduced to 3,936. Once inside the system, Stuxnet found the controlling software for the centrifuges, seized control, and manipulated the speed of the centrifuges. The malware forced the centrifuges to spin very fast for 15 minutes and then return them to normal speed. Within five months of the attack, the excessive speed changes caused the machines to break, resulting in the loss of about 1,000 centrifuges.
Unfortunately, Stuxnet was unintentionally unleashed in the wild, reportedly, when one of the engineers at an infected facility connected his work laptop to his home network. It infected many more machines than originally intended.

- Malware can be designed to destroy physical devices, processing plants, and IT systems
- By mistake, even non-targeted institutions can become "collateral damage" of such attacks

GOLDMAN SACHS „OPEN FOR BUSINESS“ DURING HURRICANE SANDY, WHILE FEW OTHERS ARE

- Goldman Sachs invested heavily in “business continuity” measures, and was able to stay open for business during hurricane Sandy in 2012, while most competitors were not operating
- It is rumored that Goldman Sachs made a lot of money during these days, and gained a number of new customers due to its resilience

CYBER-SECURITY

- Attacks and incidents will happen, you can only prepare for them
- Reduce the attack surface, especially challenge “convenience”, e.g. wireless connections, “bring your own device” policies, or single sign-on
- Think like a hacker*
  - Motives
  - How to break in

* See https://www.heise.de/newsticker/meldung/Wie-Geheimdienste-Cyberattacken-durchfuehren-4582214.html for a recent interview with a hacker (in German)

POTENTIAL MOTIVES OF A HACKER

	EXAMPLES
Stealing valuable information	• Copying data files and databases • Copying software • Listening to a company internally (sound/video) • Watching a company internally (photographs/video)
Demanding ransom	• Threatening to disrupt a business • Threatening to disclose confidential information
Benefitting indirectly	• Using confidential information for insider trading • Disrupting a business to benefit from subsequent moves in stock, commodities or other markets • Disrupting a business to sell competitors' products to customers
Mastering an intellectual challenge	• Showing that something considered impossible or very hard can be done

RAMIFICATION POST-BREACH

Post-breach recovery can take years and involve large parts of the organisation

Intangible damages account for over 40% of the total impact

Source: Beneath the surface of a Cyberattack, Deloitte, 2016.
https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

BENEATH THE SURFACE OF A CYBER-ATTACK (DELOITTE)

When a company falls victim of a cyber attack, there are several obvious and visible impacts:

- Deterioration of public relations
- Costs of technical investigation and legal fees (e.g. attorneys)
- Costs caused by the disruption of services
- Post-breach protection / cyber security improvements

But like an iceberg, this is only the tip of the incident and there is more going on behind the scenes:

- Costs of regulatory non-compliance (e.g. GDPR)
- Loss of Intellectual Property
- Loss of potential and/or existing clients
- Increase of insurance premium
- Devaluation of trade name
- Organisational perturbation following the departure of executives

Generally, the immediate and visible costs represent only a small part of the incident – the biggest loss for the company comes in the long-term and is hard to evaluate!

Source: Deloitte 2018

KEY LEARNING: BE SAFE, NOT SORRY

A successful incident response is the work of the enterprise as a whole

Technical and business teams need to be trained to co-ordinate and collaborate when disaster strikes.

Cyber events are subject to external scrutiny

Forensic evidence need to be appropriately documented and preserved to support any investigations that may result.

The foundation for a solid incident response plan is preparation

To mitigate cyber risks, policies need to be defined, playbooks tested and discipline kept around incorporating lessons learned.

Source: Deloitte 2018

QUESTIONS TO THINK THROUGH ON RISKS

- What are the most important things you can do to avoid failure of projects from a top management perspective?
- In which sense can the existence of IT risks become a strategic advantage for you?
- Which risk aspects should you consider when designing an IT-intensive or data-intensive business strategy?
- In which respects will using external IT services (e.g. cloud services) lower risks, or increase risks?

CONTENTS

ACHIEVING STRATEGIC FLEXIBILITY ≈ AVOIDING INHIBITORS FOR CHANGE

Key inhibitors related to technology	Good practices
Vendor dependency	• Understand the strategic relevance of what you buy • Understand the strategic intent of suppliers of key components • Aim for either partnerships or vendor independence in fields of strategic importance in which you cannot build on your own • Make smart make/buy decisions
IT complexity*	• Proactively manage the technology landscape • Avoid business requirements of marginal value – Thoroughly review requirements before sign-off, discarding requirements with little/no business value – Conduct a “Project Value Analysis” to force prioritization (“how to do the project with x% less budget in y% less time”) • Regularly invest into “architecture cleanup” projects (often called “reducing technical debt”)
Lack of skills	• Encourage and support staff to build skills in areas of strategic importance • Hire talent in relevant fields and – let them learn about company and industry through “career starter” programs, stages, conferences – give them room to stay up-to-date on developments in their field – let them explore innovation opportunities, coaching them to make it relevant

* See chapters on „Technology Selection“ and „Software Complexity“ later in the semester

MAKE OR BUY DECISIONS: INFLUENCING FACTORS

FOR DISCUSSION

- Capability is a source of competitive advantage
- System is tightly integrated with other internal systems
  - Integration efforts
  - Influences further make/buy decisions
- There is no strong solution in the market

- Capability is a commodity for the business
- There is one or multiple strong solutions in the market
- The needed integration with other systems is relatively low

MAKE OR BUY (AND BUY FROM WHOM) DECISION: RECENTLY EMERGING FACTORS

(Generic) Strategy of Some Suppliers

Leverage market position to grow into other businesses

- **Forward-integration** into customers'/partners' business
- **Disintermediation** of partners'/customers' businesses

Forward-integration

Vertical integration along an industry supply-chain in the direction towards customers/partners with intents such as

- Optimize processes and reduce slack
- Increase market control and power
- Increase profits

Disintermediation

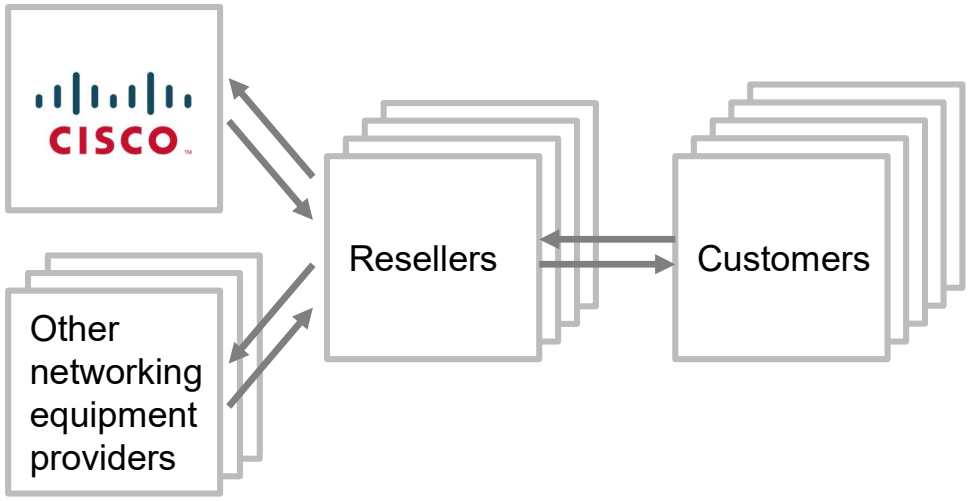
Directly interact with customers'/partners' customers with intents such as

- Eliminating the middleman from the supply chain
- Optimize processes and reduce slack
- Increase market control and power
- Increase profits

CISCO CONNECTION ONLINE (CCO): DEVELOPING A DIRECT CUSTOMER RELATIONSHIP

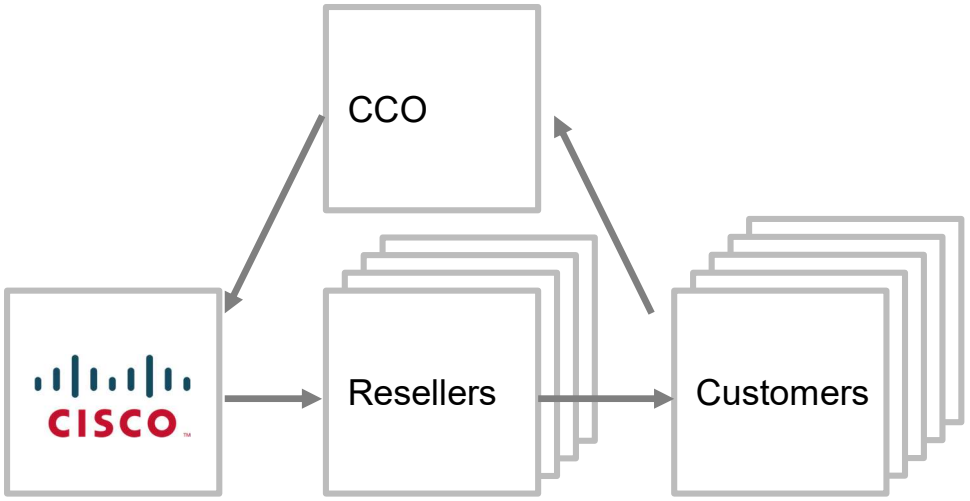
FOR DISCUSSION

Before CCO



- Customers went to resellers to get a networking solution designed (consisting of many devices, potentially from different suppliers)
- The design was a tedious, error-prone, and expensive process
- Total duration from decision to get new networking solution until installation 6-8 weeks

With CCO



- Customers directly design a networking solution on CCO (potentially with help of reseller)
- Order is dispatched directly to reseller and Cisco

Advantages:

- Total duration is reduced to 2-3 weeks
- Much faster, less error-prone and less expensive design process
- Resellers stay in the loop
- Only Cisco products are used (Cisco)
- Direct relationship between customer and Cisco (Cisco)

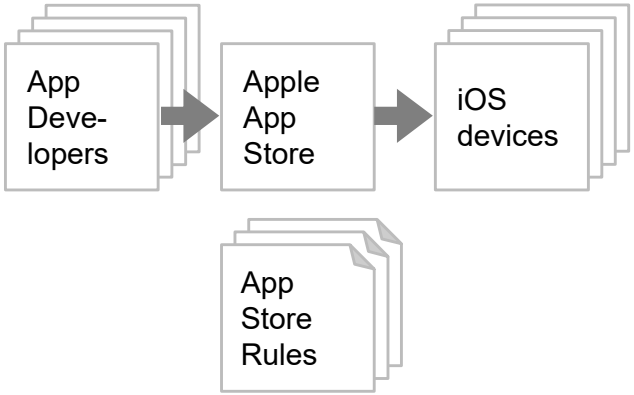
OTHER EXAMPLES FOR BUILDING DIRECT CUSTOMER RELATIONSHIPS

- exivo, a cloud-based access control solution for small and medium-sized enterprises provides dormakaba with a direct relationship to customers, while resellers market, sell, install, and service the solution
- The involvement of the customer with the cloud solution creates switching barriers for the customers

- Intel subsidized PC manufacturers' advertising if it included the "intel inside" logo
- The move created awareness of end users for the intel brand, and created a perception of high quality and high compatibility ("the original PC CPU most manufacturers use")
- In the long-run, it weakened the negotiation position of PC manufacturers vs. intel

APPLE VS. EPIC GAMES (“FORTNITE”)

FOR DISCUSSION



Facts

- The only way to install an App on an iOS device is through the Apple App Store*
- App Developers must submit Apps for review by Apple vs. App Store rules; it rejects Apps at its discretion
- Highly contested rules include:
  - Every purchase transaction (incl. in-app purchases, subscriptions) must use the App-Store payment mechanism; Apple retains 30% of the revenue
  - If the App has a login mechanism (e.g. “login with Google”/”login with Facebook”/”login using id & password”), it must also support “login with AppleId”
  - Apps can only use devices that Apple allows (e.g. Apple did not allow to access the NFC device until regulators intervened)

Apple (key arguments)

- Requiring all App installations go through the App Store and the mandatory review process is necessary to enforce privacy and security safeguards
- Requiring all purchases go through the App store mechanism enables to protect consumers
- Allowing payments bypassing Apple’s mechanisms without Apple getting compensated is similar to allowing taking a product from a store without paying
- The smartphone market is highly competitive, customers and developers can go elsewhere

EPIC Games (key arguments)

- Apple’s conduct is anti-competitive, stifling innovation, blocking competition, and aiming to control markets
- Customers are forced to pay higher prices
- Developers are forced to comply with evolving rules defined by Apple at its discretion
- Apple forbids alternative App stores, which may curate Apps in segment-specific ways
- Users do not really have the option to move to a competing smartphone operating system brand, as there are very high switching barriers

* There are so-called “jailbreak” methods to bypass it, which are very risky, compromise security, and require deep technical knowledge

OTHER ANTITRUST INVESTIGATIONS/LAWSUITS

EXAMPLES

Google vs. EU

Google was found to violate EU antitrust laws by

- **Android:** Requiring smartphone manufacturers to preinstall Google search and Google Chrome as precondition for licensing certain apps, to agree not selling smartphones running competing operating systems based on Android source code, and by giving financial incentives to smartphone manufacturers and network operators to exclusively pre-install Google search
- **AdSense:** Requiring partners to exclusively use Google's AdSense and not engage with competitors, and to predominantly place AdSense ads above any other advertising
- **Shopping:** Favoring Google Shopping results over competitors' results in its search algorithm

Intel vs. EU

Intel was found to violate EU antitrust laws by

- granting rebates to PC and server manufacturers conditional on all or almost all supplies being procured from Intel
- granting rebates to a computer retailer conditional on only selling PCs with Intel CPUs
- granting direct payments to computer manufacturers to halt, delay, or limit launch of products incorporating AMD chips

ANTITRUST LAW: ESSENTIAL FACILITIES DOCTRINE

The **essential facilities doctrine** (sometimes also referred to as the **essential facility doctrine**) is a legal doctrine which describes a particular type of claim of monopolization made under competition laws. In general, it refers to a type of anti-competitive behavior in which a firm with market power uses a "bottleneck" in a market to deny competitors entry into the market. It is closely related to a claim for refusal to deal.

The doctrine has its origins in United States law, but it has been adopted (often with some modification) into the legal systems of the United Kingdom, Australia, South Africa, and the European Union.

Under the essential facilities doctrine, a monopolist found to own "a facility essential to other competitors" is required to provide reasonable use of that facility, unless some aspect of it precludes shared access.[1] The basic elements of a legal claim under this doctrine under United States antitrust law, which a plaintiff is required to show to establish liability, are:

1. control of the essential facility by a monopolist
2. a competitor's inability to practically or reasonably duplicate the essential facility
3. the denial of the use of the facility to a competitor; and
4. the feasibility of providing the facility to competitors

- In layman's terms:
  Your are allowed to build a monopoly and maintain it, but you are not allowed to use it hindering competition in connected markets
- "Almost monopolists" are often happy to have a small competitor and even support it, so they can claim there is no "bottleneck"
  - Microsoft supporting Apple in the 1990's
  - Google supporting Mozilla (Firefox)
  - HP not charging compatible toner and ink manufacturers (e.g. Pelikan, Peach) for patent infringement

Source: https://en.Wikipedia.org/wiki/Essential_facilities_doctrine, downloaded 09.09.20

QUESTIONS TO THINK THROUGH ON VENDOR DEPENDENCY

- As a buyer of Apple iOS products*, how does the way Apple manages the App Store affect you? Consider both positive and negative aspects.
- What are the most important things you can do to limit vendor dependency in a field in which your company wants to buy?
- What are the advantages and disadvantages of selecting a large vs. a small vendor?

* If you are more familiar with Android, you can also look at how the Google Play store affects you. It is managed similarly, and while Google allows competing stores in principle, the licensing conditions for Android (described on page 43) have avoided significant competitors arising. EPIC Games has also sued Google, with similar claims to the Apple case

CONTENTS

BEING THE “GO TO” PLACE IN INTERNET SEARCH

SOME OF THE THINGS (ONLY) GOOGLE CAN DO

EXAMPLES

Google Trends	• Which topic is being researched a lot in which community • Which topic leads to which follow-up search
Google Analytics/ Chrome	• Which sites are which communities visiting, and how much time are they spending on them • Which topics on those sites lead to follow-up searches, or users following links
Google Maps	• Where are there traffic jams (both statistically and right now)
Google Android/ Chrome (location)	• Where are people throughout the day and at night • Where are they working, shopping, dining, …
Who are the largest clients of consulting firm ABC	• Combine data about users' employer ABC with in which business building they are spending time
What may the Xmas business of retailer XYZ be this year	• Frequency data of how many people are in their stores (brick-and-mortar and online) • "Lifestyle" data about the wealth of those persons • Comparison to earlier years and competitors

- While the above things are done by Google, these things could be done by Google, but we do not know whether they are actively doing them

SOME OF THE THINGS (ONLY) FACEBOOK CAN DO

EXAMPLES

Social Interactions	• Who interacts how often with whom? • Which topics (both on FB and on internet sites) trigger people to communicate with others, and with which emotions?
Use of time	• How much time are users spending on which topics? • Where are users using their mobile devices?

SOME FIGURES ABOUT GOOGLE AND FACEBOOK FROM THEIR ANNUAL REPORTS 2019

GOOGLE

- Revenue USD 162bn
- Income from Operations USD 34bn
- R&D Expenses USD 26bn

- Active users on Gsuite 2bn
- About 5bn search users (estimate)
- About 2’000bn searches/year (estimate)
- Revenue/search ~USD 0.08
- Annual revenue/search-user USD 20-30

FACEBOOK

- Revenue USD 71bn
- Income from Operations USD 24bn

- Active users (FB only) 2-3bn
- Revenue/user ~USD 35 (US: 135, EMEA: 43, AsiaPac: 12, Others: 8)

CONTENTS

HOMEWORK EXERCISES: QUESTION 1

- Study the project portfolio in the provided spreadsheet, along with their business cases
- All projects in the portfolio meet the business case requirements the company has for approval (complete benefits and costs information, payback time < 6 years, NPV > 0). However, doing all projects as planned now would require 188* FTE (full-time equivalents, i.e. persons working full-time), and the company only has 140 FTE in Solution Delivery.
  With each of the departments behind the five projects saying their project is important and they absolutely want it, the head of IT suggests to reduce the amount of people working on each project by the same amount, as a fair measure for everybody. The business departments say that they cannot reduce the scope.
  - If the company decides to do that, and the scope of each project cannot be reduced, in which other respect will the project change?
  - What will be the impact on the economic value of each project and the whole portfolio? Calculate it by making the necessary adjustments in the spreadsheet.
  - As an alternative, the company may use 48 additional FTE from an external service provider helping with the projects. Those FTE carry a 34% higher cost than internal staff. What is the impact on the business case?
  - As another alternative, you may cancel or delay one or more projects in the portfolio altogether. What would be the impact?
  - Which is the economically most beneficial alternative? Why (beyond of “it gives the best numbers”)? What general learnings can you derive from your analysis?
  - *Optional question:* Which type of software/which algorithms could you use to always select the “optimal project portfolio” from an economic point of view? Why do companies not do that?

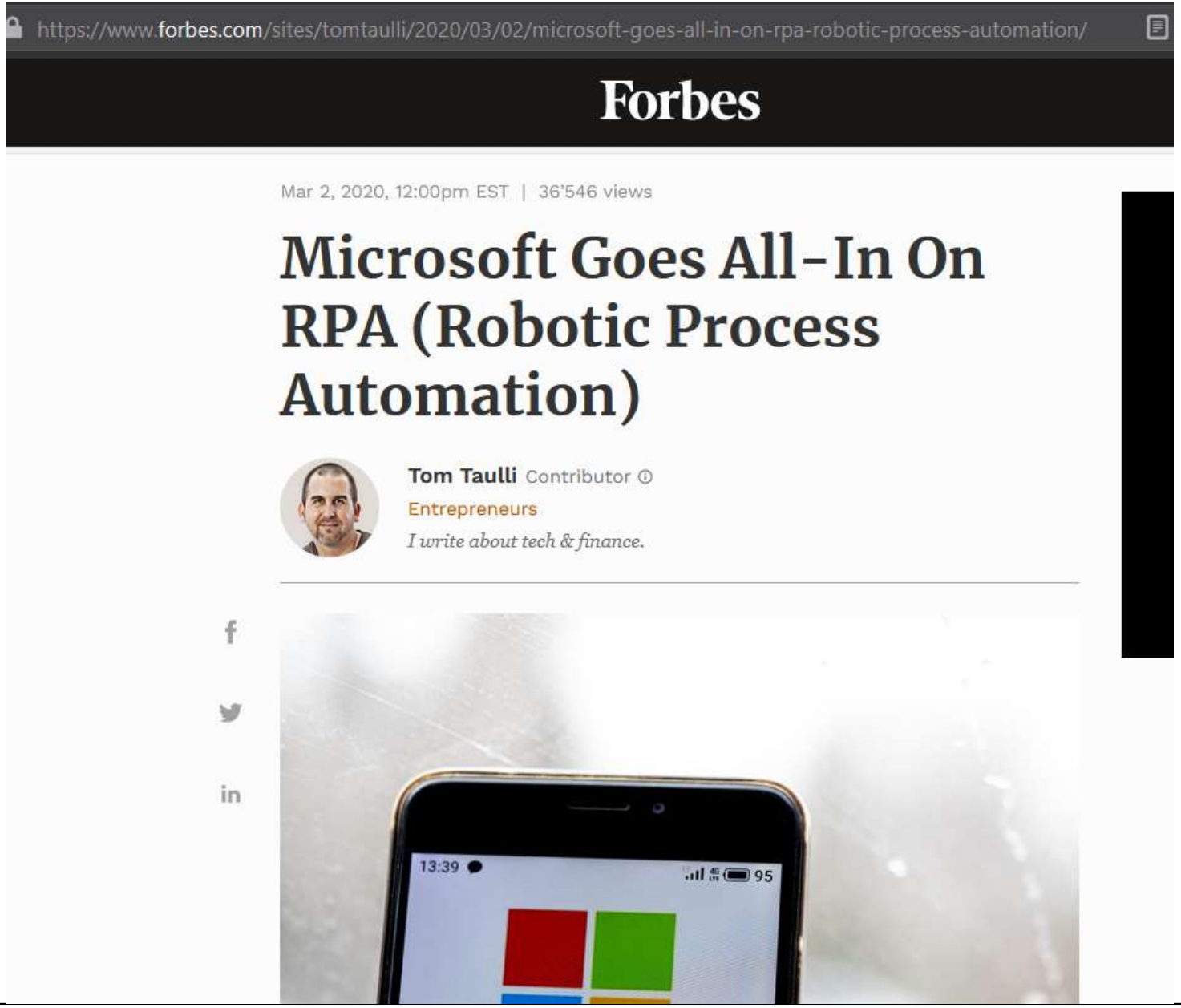
* Calculated as project costs/CHF 200’000. CHF 200k is the average total cost for an employee in Solution Delivery in the company. Note that this amount is much more than the salary of the person, as it includes holidays and sick-leave time, social security and other insurance, employee benefits, workplace (office space, equipment, software licenses), training costs, etc.

HOMEWORK EXERCISES: QUESTION 2

- We are now switching the perspective, from business top management taking decisions on the overall economic value of projects for the business to IT management having to execute the projects and to provide the required personnel.
- Assume projects A-D use Java as programming language, and project E uses COBOL. The Solution Delivery staff of the company has the following profiles: 20 FTE Project Management, 44 FTE Business Analysis and Testing, 18 FTE Software Engineering COBOL, 58 FTE Software Engineering Java.
    - What would the different potential decisions on the project portfolio mean for your availability to staff the projects? Which decisions would lead to major complications for you, and which? What could you do to overcome them?
    - As the head of IT, how would you aim to manage your workforce to avoid such complications?

HOMEWORK EXERCISES: QUESTION 3 (1/2)

- Read the following article, and other articles you find about Microsoft's move into Robotic Process Automation (RPA) with Power Automate.



HOMEWORK EXERCISES: QUESTION 3 (2/2)

- Find out about other providers of RPA: What kind of companies are they, how big, is RPA their only product, or is it part of a broad portfolio of products?
- Which advantages does Microsoft have vs. these other providers? Think about it from a user's perspective (which would use Microsoft's products, which others).
- How is the strong push of Microsoft into that market affecting the other providers? Consider especially the recent move of Microsoft to make many functions of Power Automate available for free for Windows 10.
- From a competition authorities point of view, how do you assess the moves by Microsoft?