Software Security: Lessons learned from Risk and Security Economics

Christophe Huygens
Christophe.Huygens@cs.kuleuven.be

Objectives for today

Session is *context* for secure application development

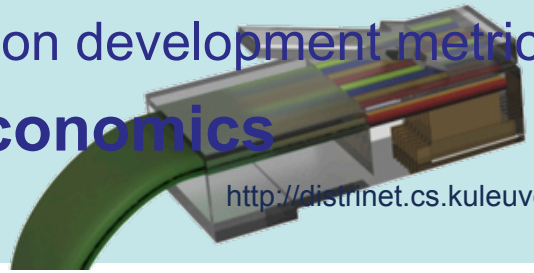
1. Understand risk and policy from an techno-economic perspective

- What is risk?
- Risk taxonomies
  - Industrial versus operational
  - Exploring risk dimensions
  - ICT risks
- Risk and policy

2. Handling risk

- Approaches
- Managing implies quantification of *???*
- Risk indicators
- Security metrics
- Secure application development metrics

3. Real world economics



Can we learn something for sec app dev?

What is risk ?

- *"Risk is the probability that a hazard will turn into a disaster"*
- *Oxford "hazard, danger; exposure to mischance or peril"*
- *Holton "there has to be uncertainty, and the outcome has to matter"*
  - *the plane jump*
  - *throwing dice versus gambling*

*Risk = Probability * Outcome*

- Engineer versus the stock trader
  - Engineer (and sw developer) focuses on negative outcomes
  - Engineer typically needs to deal will with events with very low, hard-to-quantify probabilities

Is risk positive?

- life is not risk-free
- we take risks because there are rewards
- … or at least minimize risk to achieve objective
- good assessment of risk/reward value pair is key to success
- threshold defines acceptable behavior
- R/R T is continuously changing!
- examples

Risk posture

Table 1. Result of multiple regression: β (standardized regression coefficient) for anxiety of each risk

	Earthquake	Cancer	Decrease in income	Global warming	Leaks of personal information on the internet
Japan					
probability	.314 ***	.286 ***	.239 ***	.203 ***	.206 ***
severity	.243 ***	.202 ***	.374 ***	.371 ***	.327 ***
Clarification by specialists	.021 ns	−.020 ns	−.015 ns	−.041 ns	−.056 *
Knowledge of a person		.108 ***	.066 *	.192 ***	.138 ***
controllability	.009 ns	−.047 ns	−.053 ns	.032 ns	−.099 **
	(R2= .212)	(R2= .171)	(R2= .299)	(R2= .327)	(R2= .280)
USA					
probability	.442 ***	.410 ***	.288 ***	.326 ***	.265 ***
severity	.091 *	.208 ***	.315 ***	.325 ***	.341 ***
Clarification by specialists	−.012 ns	.006 ns	.053 ns	.156 ***	.087 *
Knowledge of a person	.076 ns	.016 ns	.118 **	.052 ns	−.056 ns
controllability	.004 ns	.085 *	−.077 ns	.025 ns	.026 ns
	(R2= .247)	(R2= .258)	(R2= .311)	(R2= .451)	(R2=.256)
China					
probability	.079 *	.054 ns	.128 ***	−.008 ns	.197 ***
severity	.138***	.149 ***	.155 ***	.229***	.286 ***
Clarification by specialists	.030 ns	.253 ***	.181 ***	.039 ns	.078 **
Knowledge of a person	.171***	.158 ***	.166 ***	.183 ***	.183 ***
controllability	.055 ns	−.097 *	.018 ns	.012 ns	.004 ns
	(R2=.072)	(R2= .153)	(R2= .152)	(R2= .107)	(R2= .324)

* p< .05 ** p< .01 *** p< .001

Y. Nara, A Cross-Cultural Study on Attitudes toward Risk, Safety and Security. LNCS Volume 5178, Knowledge-Based Intelligent Information and Engineering Systems, 2010, pp. 734-741.

L1: Risk attitude and SAD

- Single attitude towards risk does not exist
- E.g. provision of controls for personal information leakage (monitoring, enforcement)
  - No significant effect on anxiety in China and USA
  - Clear negative effect on anxiety in Japan

Qualify
demographics of target audience (geography, age, customer…)
and associated security requirements

<> Security requirements introduce variability

Counter using methodology that can address this structurally
(SPL, FOP, …)

Our risk posture (2)

- = our attitude to risks
- a most fundamental characteristic of an organization

- policy = a description of this attitude
- (so reflects the values of an organization)
- (provides guidelines for behavior -- more later)

- innovation = better risk handling (use or protection)
- Risk Management is the science (or art) of handling

Risk management

- theoretical equation is very simple

hardest harder hard

*Risk (€) = Σ Likelihood * Impact (can be > 1) * Value (€)*

All business lines, all processes, all applications, all infrastructure elements and code

- Many unknowns, hard-to-measure, hard-to-quantify
- Use estimators and metrics – more later
- Powerful when captured - enables comparison, CBA

Decomposing risk (1)

- risk landscape has many dimensions
- within dimensions live many sub-risks
- = the risk ecosystem
- increase detail until we reach s/w risk

Total Risk = Industrial risk + Operational risk

- Industrial risk: risk directly associated with our business objective
  - GM selling Hummers when the customer wants to go green
  - Toyota gas pedal problem, government GTIs
- Operational risk: risk of supporting activities and external factors
  - e-shop security of on-line bookseller
- For a bank FX is IR, for a car maker it is OR
- For Microsoft secure applications should be IR, for users OR

IR and quality

- applications are developed in the software factory … just like cars are assembled in the car factory
- “traditional” quality management is highly similar to management of industrial risk
  - achieve predictable output
  - *Product value = Σ (1-Likelihood of defect) * Impact [can be >1] * Subsystem Value*
- qeneral frameworks apply
  - ISO 9000, six-sigma, CMMI-DEV
- IT or more specific quality frameworks apply…
  - COBIT IT governance and audit, ITIL service delivery
  - BSIMM for secure software (development and some deployment)
  - maturity model is important – need to be in-line with peers
- secure software IR must be driven by the development team
- (note: development activities are subject to OR)

Operational risk drivers

- a solid operational risk practice is often a requirement
- legal or regulatory
  - Basel II: In (Europe's) financial industry regulators want business to demonstrate solid ORM and provides capital allocation guidelines
  - SOX: (US) Mandates controls regarding several aspects of financial reporting, oversight and ethics
  - HIPAA-security: (US) Mandates control on health information with regard to confidentiality, integrity and availability
- corporate governance and service disruption
  - protect shareholder value
  - provide service with necessary degree of confidence

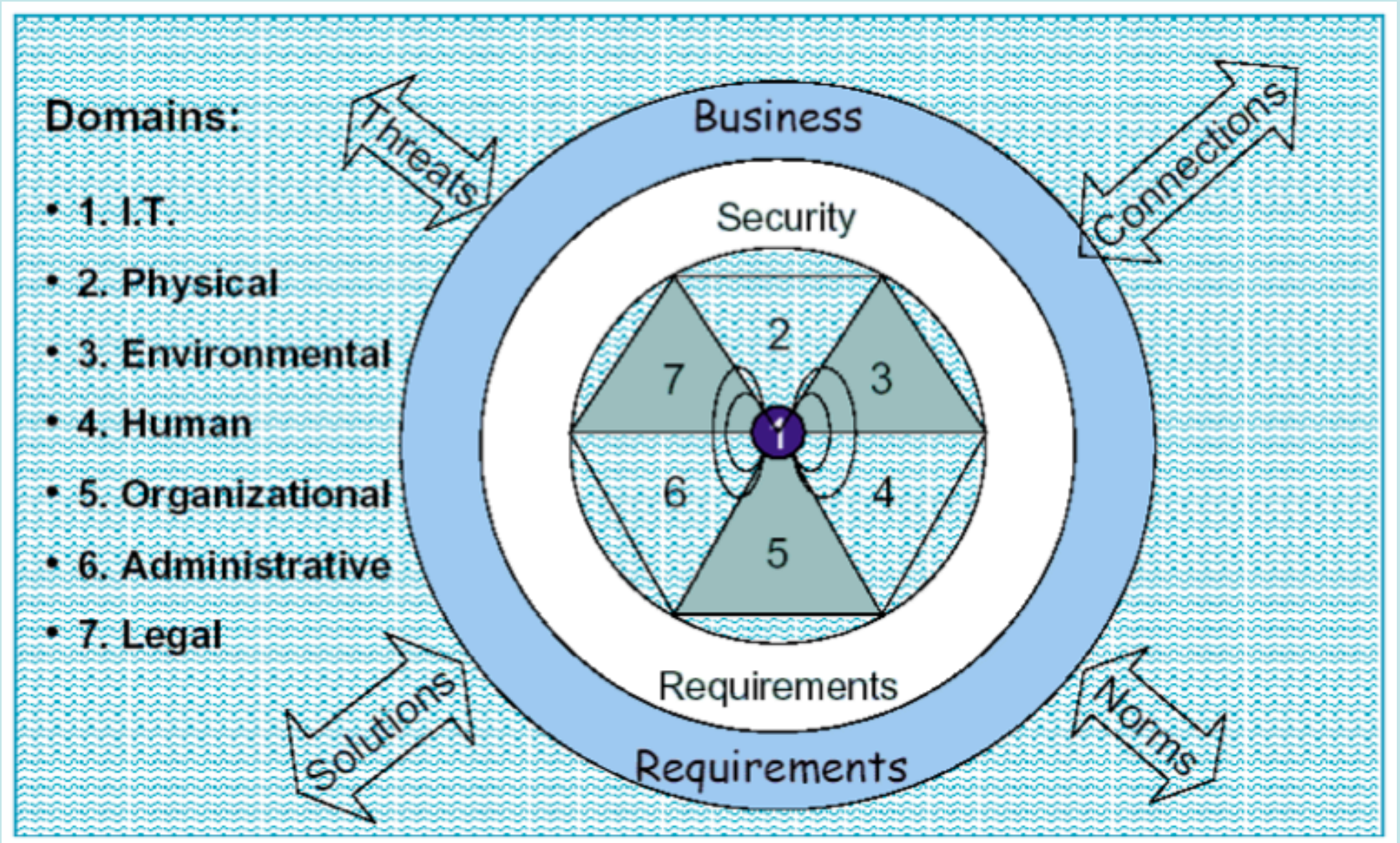
Operational risk

- Operational risk = loss by inadequate or failed
  - people, processes, ***systems*** (performance/security)
  - external events (natural disasters)
- using software implies OR tackled by th(e) system(s folks)
- … so the s/w product companies developers' IR becomes the client sysadmin's OR

- for now, the software industry seems to get away with this
- related to risk:
  - the risk/reward norm of the s/w community is wrong
  - the customers are not really empowered
  - the market mechanisms that drive IR down do not seem to apply
  - there seem to be little, if any penalties for production of unsecure s/w
  - some self-policing going on, little regulation or legal challenges

Opinion

Decomposing Risk (2)

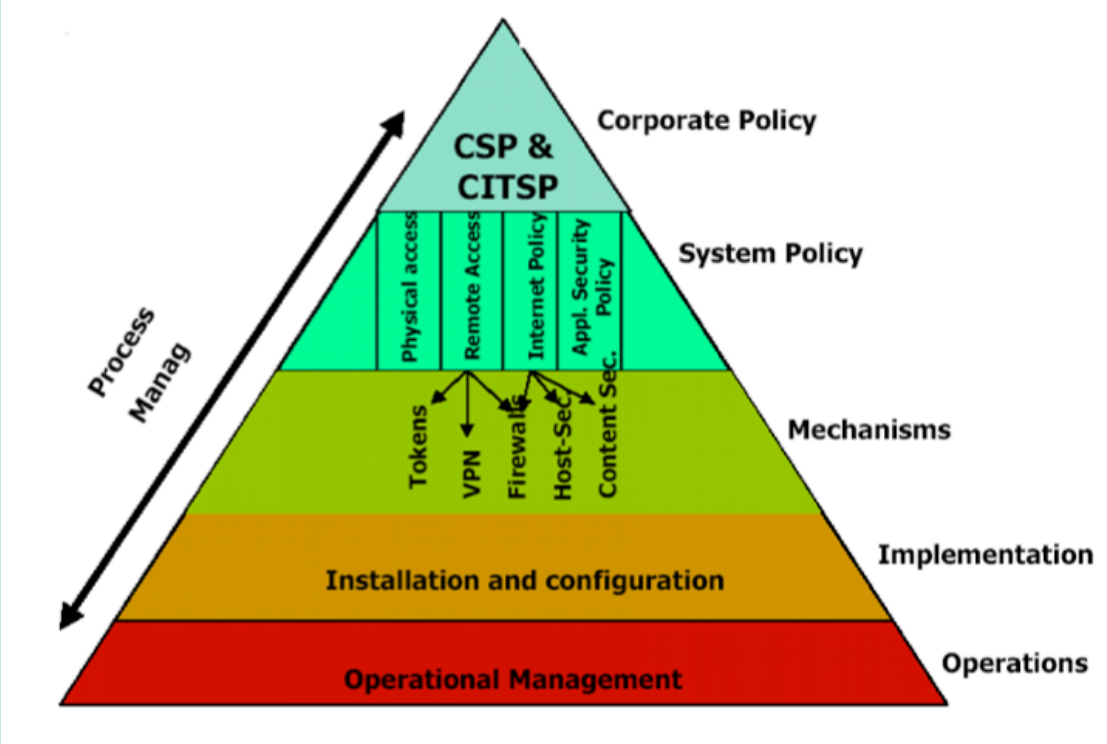


Risk domains

- to achieve objectives (max. profit) actions must be taken
- each action implies positioning R/R in each domain
- examples of risky behaviour in some domains
  - human: shoe producer decides to produce using child labor
  - environmental: agro-industrial complex makes heavy use of pesticides
  - legal: bank decides to keep less reserves than Basel requires
  - IT: to get on-line quickly we are using un-patched servers
  - organizational: use strong hierarchical mgmt style with little input from lower ranked co-workers
- clearly some guidance is required

Policy revisited

- the organizations policy describes its R/R positioning
  - reflects top-level values of the organization
  - guides our actions by refinement



… a typical s/w factory

Microsoft Standards of Business Conduct

Published: May 15, 2003 | Updated: June 29, 2009 | Current as of 2009

Great People with Great Values

This online version of the Microsoft Standards of Business Conduct has been modified from the original version distributed to our employees. The references to some internal resources and electronic links have been changed to facilitate communications from the public at large.

On This Page

- Letter from Steven A. Ballmer, Chief Executive Officer
- Microsoft Values
- Compliance with the Standards of Business Conduct
- Microsoft Standards of Business Conduct
- Microsoft Business Conduct and Compliance Program
- Our Responsibilities

Letter from Steven A. Ballmer, Chief Executive Officer

Dear Fellow Employee:

Microsoft aspires to be a great company, and our success depends on you. It and are committed to growing our business responsibly. People who dedicate customers, helping partners, and improving the communities in which we do accountable for achieving big, bold goals with unwavering integrity. People w that to be truly great, we must continually strive to do better ourselves and h

We must expect the best from ourselves because who we are as a company

Opinion

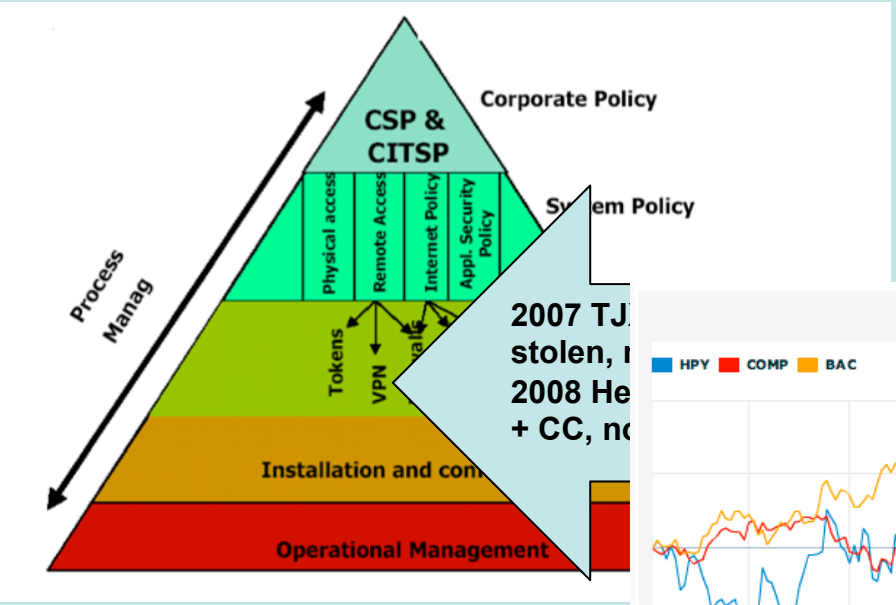
L2: Where do I work?

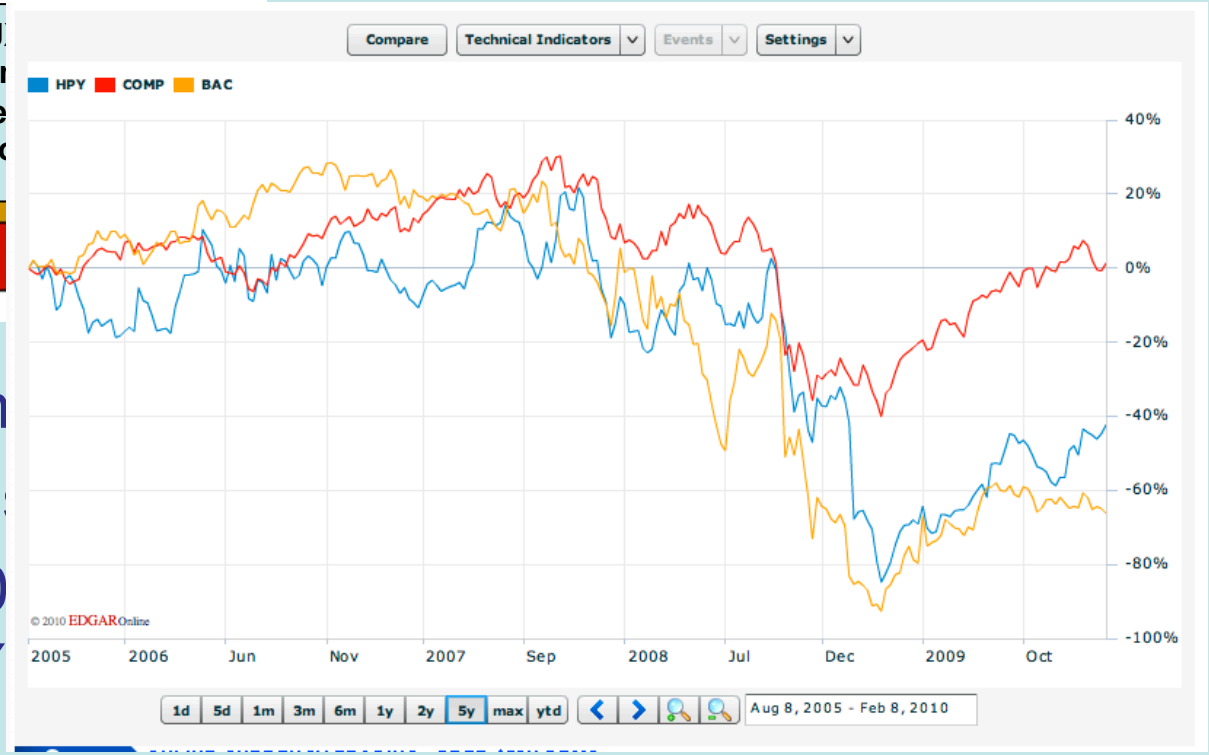
- As a s/w developer, I work for a company that …
  - Has no attitude towards risk at all
  - Or has an explicit short-term vision
- …versus…
  - Has explicit risk company guidelines
  - Has a long-term customer-centric vision
  - …maybe even translated to commitments at the secure s/w factory level

"Every developer should ask whether the organization he is working for is committed to secure software. You would not want to work for polluter - would you?"

- Be aware of cultural differences when trying to get commitments (=money)

Cost of not having security (OR)

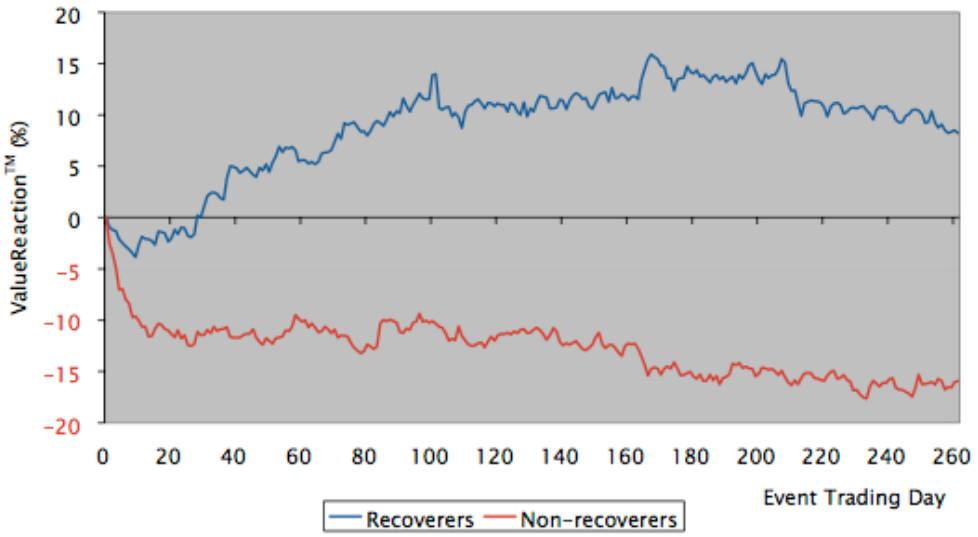




- TJX: Analyst estin
- TJX: *no effect* on
- Heartland: 2/2010
  class action (HPY

Cost of not having security (2)

Figure 1: Value Reaction to Reputation Crises in general



5.1. The Effect of Security Breach Announcements on Announcing Firms

On the announcement day (t=0) we observed an average abnormal return of -0.8638 %. The stocks realized, on the average, an abnormal return of -1.2282 % in the day following the announcement (t=1). This gave rise to a -2.092 % cumulative abnormal return over the event window. This translated

Protecting Value in the Face of Mass Fatality Events, Oxford. Metrica.
Reputation and Value: the case of corporate catastrophes, (2001), by Rory F Knight & Deborah J Pretty, Oxford. Metrica.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *Int. J. Electron. Commerce* 9, 1 (Oct. 2004), 70-104.

L3: How not to convince my CEO

- The impact on stock price can be both – and +
- Some security problems + excellent communications strategy = a decent share price pump
- Emphasis both sides: predictability + recovery plan
  - Manage the risk
  - = Make sure software development is involved in both
  - = Take credit for both proactive and reactive actions

“Don’t leave incident handling to the marcom magicians”

Risk handling (OR/IR)

- identify
- then
  - transfer to others by default (identification not needed)
  - transfer through insurance
  - provision
  - accept and communicate
- or
  - reduce (be yr own insurer)
  - “quantification” is a must

Security quantification

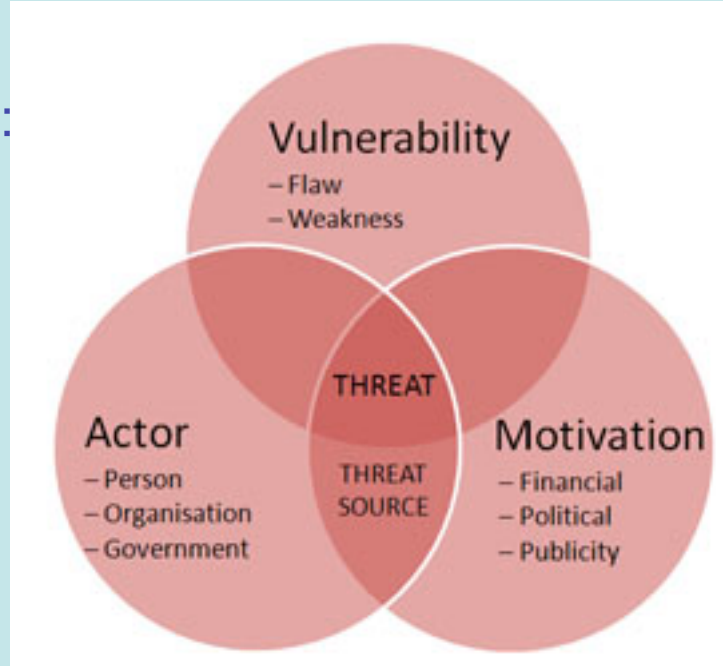
- Recap

  *Risk (€) = Σ Likelihood * Impact (can be > 1) * Value (€)*

- Security

  *Risk (€) = Σ Threat Source * Vulnerability * Business Impact(€)*

- Controlled environment (dev, testing, Q/A):
  - White box quantification = Vulnerabilities
  - Black box quantification = Vulnerabilities
- Wild:
  - Black box quantification = Threat Source*Vuln.
  - OR Incidents (banks have more interesting loss databases then universities)



L4: Managing S/W risk

- *Risk (€) = Σ Threat Source * Vulnerability * Business Impact(€)*
- Challenge is in quantifying these factors
- As a developer I should track:

The end customers loss databases: measure some T*V*B

My testing and QA activities: measure some V

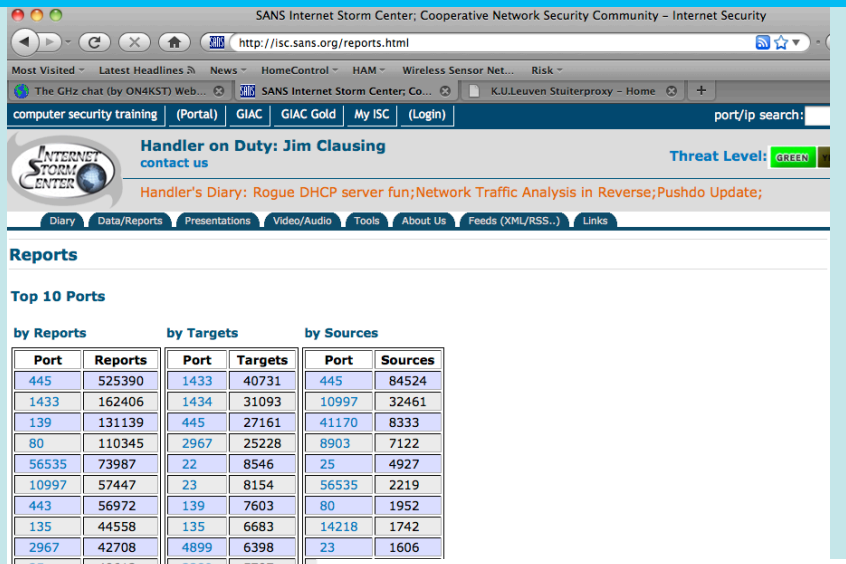
Honey pot approach: measure some T*V

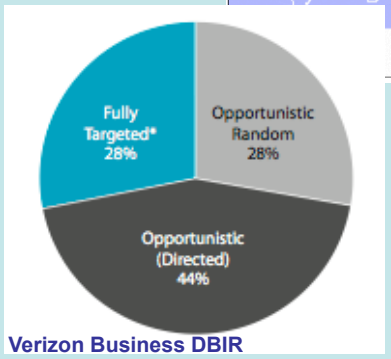
My development OR: estimate V

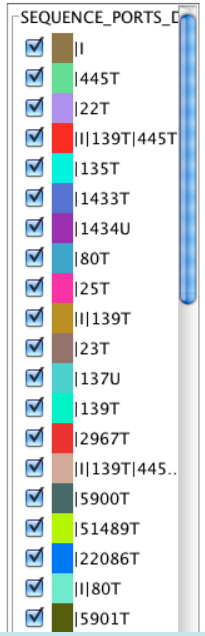
Model approaches: calculate some (proxy of) V
Formal model: proof absence of V

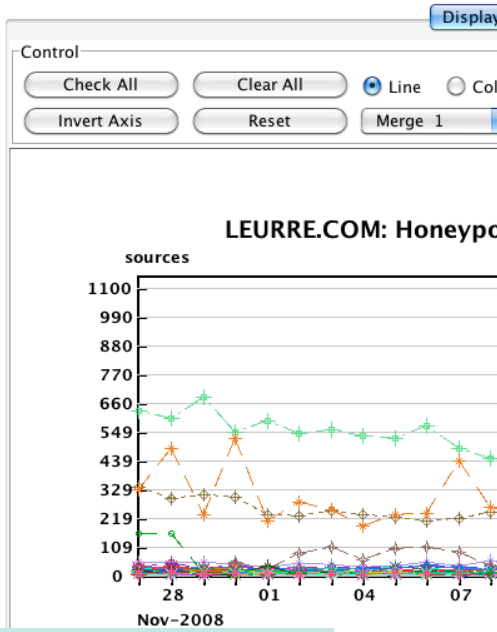
Threat source quantification

- Hard
  - interplay between threat and vulnerability
  - profile (motivation)
  - sophistication (resources)
  - not stationary
  - not rational
- Generic efforts (weather reports)
  - SANS
  - Verizon DBIR
  - Honey* (getting closer to application with tools such as glastopf)
- Targeted efforts
  - counter(intelligence), 90%
- Emerging efforts
  - Root cause analysis based on OR incidents or logs









Quantified security zoo

A Guide to Security Metrics - SANS Security Essentials GSEC Practical Assignment Version 1.2e - Shirley C. Payne June 19, 2006

Quantified security zoo

NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security

IR/OR and **secure software** quantification

- I develop
- IR perspective
- “white box”
- mostly developer, q/a, tester
- direct measurements on code, architecture
- weak incentive
- scale
- ➔➔ ss/w metrics

- I use
- OR perspective
- “black box” - only for s/w
- indirect observation of s/w behavior
- q/a and testers
- user incidents
- strong incentive (legal)
- OR “metrics” are ss/w…
- ➔➔indicators

OR indicators (generic)

- Operational risk = loss by inadequate or failed
  - people, processes, ***systems*** (performance/security)
  - external events (natural disasters)
- OR indicators as used in financial industry
- People
  - availability: effective FTE %, consultant %
  - compliance: compliance violation %, awareness trained %
  - exceution/adequacy: skill set coverage, training ratio, seniority, productivity
  - management: sick days, leavers, transfers
  - organizational: hierarchical ratio, job descriptions
- Process
  - availability: SLA breaches
  - compliance: transactions without evidence or non-standard ratio
  - execution: planned/actual transactions, exceptions (non STP, late), incidents
  - management: exception delta
  - organizational: process changes, undocumented processes ratio

OR indicators (generic ctd.)

- Systems
  - availability: SLA breaches
  - compliance: non-(security) policy compliant systems ratio
  - execution: incidents/support requests
  - management: support time evolution, incident delta
  - organizational: change requests, undocumented-unsupported systems ratio
- (External)
  - BCP
  - stability of regulatory frame
  - business dependencies

"Unless we can get cloud computing as reliable and secure as utilities it is going to be a security assessment nightmare as (cloud users) we are black-boxing even more" ***Opinion***

OR IT security indicators

- People
- Process
  - partners not having subscribe to internal standards (such as s/w providers)
- System
  - compliance: non-compliant systems and apps ratio (backup, a/v, SDLC, …)
  - management: incident resolution time delta, incident rate evolution
  - execution: incidents / systems, resolution time
  - organizational: non-tracked assets: systems, data

- ISO 17799, 27001/2 provides for inspiration
  - Control objectives: risk assessment; security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management, access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; compliance.

How to use OR indicators

- For software factories
  - have people, processes, systems subject to OR
  - can use OR indicators to gauge their performance
  - the correlation between OR indicators and product (= s/w) quality is high
  - strength of correlation can even be improved by pooling over many s/w factories
  - part of philosophy of BSIMM, “practices are qualitative metrics”
- For software users
  - have people, processes, systems subject to OR
  - can use OR indicators to gauge their performance
  - the correlation between OR indicators and quality of used s/w is partial at best
  - some OR indicators are better than others (systems)
  - pooling incident data over many users could improve strength of correlation
  - bad: a lot of resistance (reputation) – regulation required?
  - bad: need to factor out all other influences
  - good: losses related to incidents are already pooled to provide OR loss distribution

Earlier quantification work

- *Quantified Security is a Weak Hypothesis*, Vilhelm Verendel. Proceedings of NSPW'09, September 8–11, 2009, Oxford, United Kingdom,
- 90 paper survey (1980-2008)
- white and black box, assumptions (rationality, stationary, independence)

"The result shows how the validity of most methods is still strikingly unclear"

"Despite applying a number of techniques from fields such as computer science, economics and reliability theory to the problem it is unclear what valid results exist with respect to operational security"

"Quantified security is thus a weak hypothesis because a lack of validation and comparison between such methods against empirical data"

- we need (your) long-term and structured data!
- … not saying it is impossible
  - 1 of the approaches may be right, or better ones constructed
  - we just cannot validate metrics and/or models well at this time

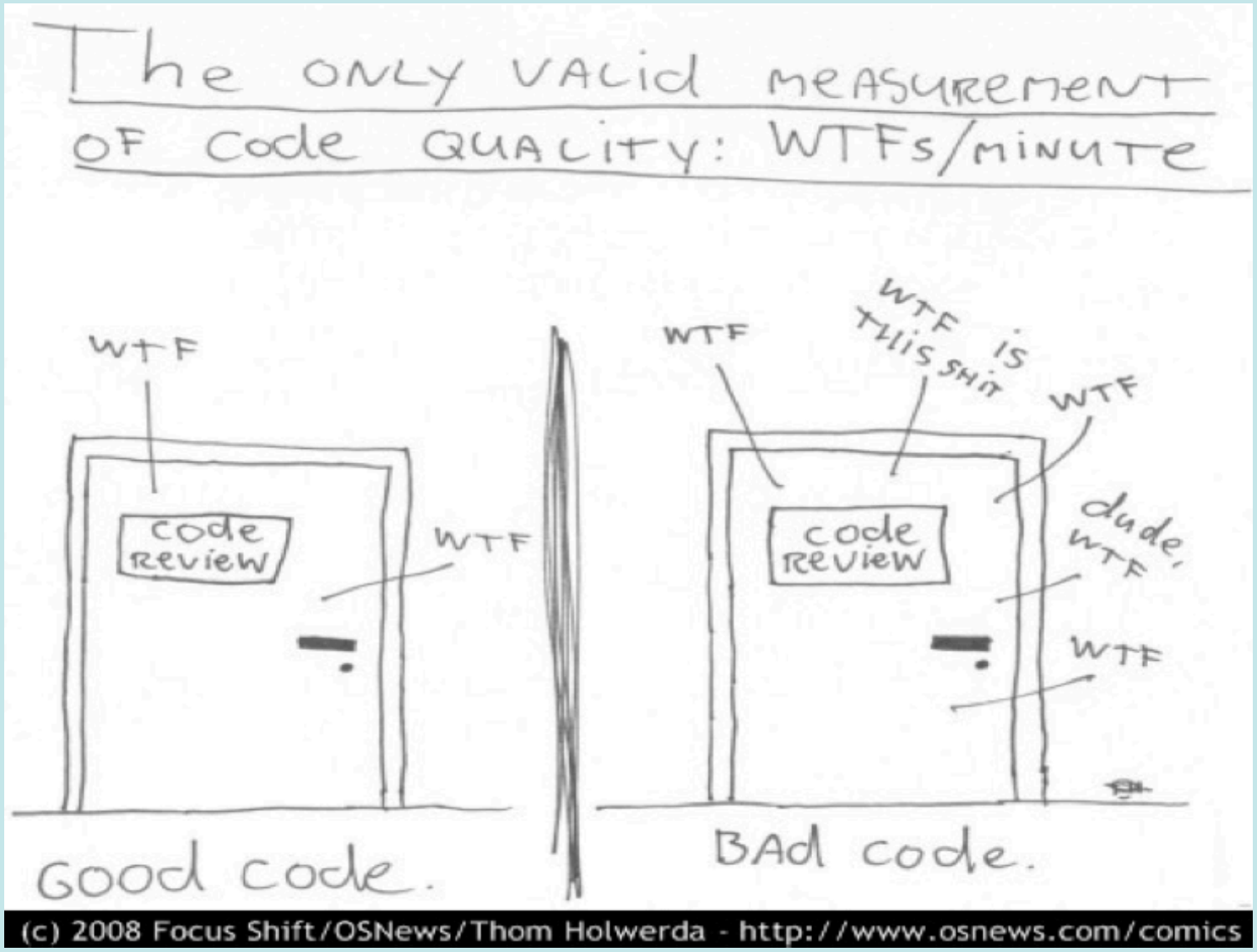
Skepticism in quantification (2)

- S. M. Bellovin. *On the brittleness of software and the infeasibility of security metrics*. IEEE Security and Privacy, 04(4):96, 2006.
  - philosophical view
  - software brittleness, linearity of layered defense, danger of composition
  - brittleness: intrinsic defensive capability of s/w is low > all metrics are essentially 0
    - Self-healing s/w - very early stage
    - New composition mechanism where defense layers reinforce each other, instead of onion approach

Real-time monitoring

- Reijo Savola. *On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems.* IJCSNS, Vol. 10 1-2010
  - it is just immature
  - good metrics have many attributes
  - much more attention needed for validation
  - Multi-dimensional validation methodology

Quantified security – only way

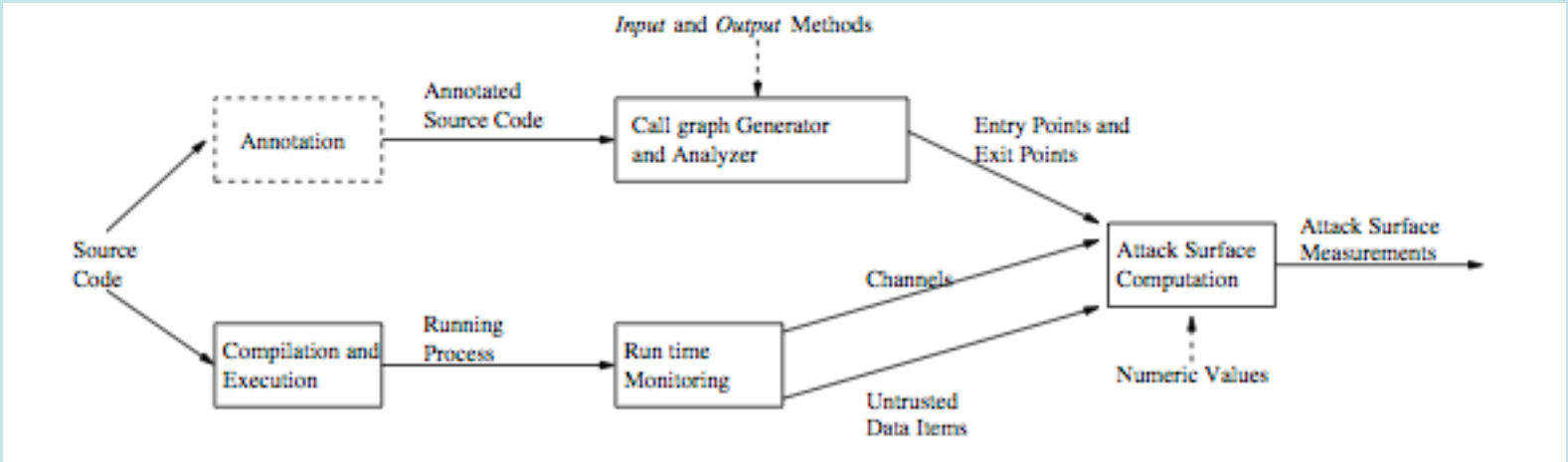


White box quantification

- Good metrics (A. Jacquith, Security Metrics):
  - easy to measure
  - consistent
  - expressed as a number
  - have a unit
  - specific
- Some principles or practices immediately elicit metrics at design or code time (Scandariato et al., 2006)
  - KISS: cyclomatic complexity, size KLOC, attack surface
  - separation of concern: degree of ➔AOD concern diffusion
  - layered security: lines of defense ➔checks/scenario, input val.
  - minimize critical sections: number of critical modules ➔UML/dd
  - accountability: degree of accountibility ➔ audit ratio

Attack surface metrics of code

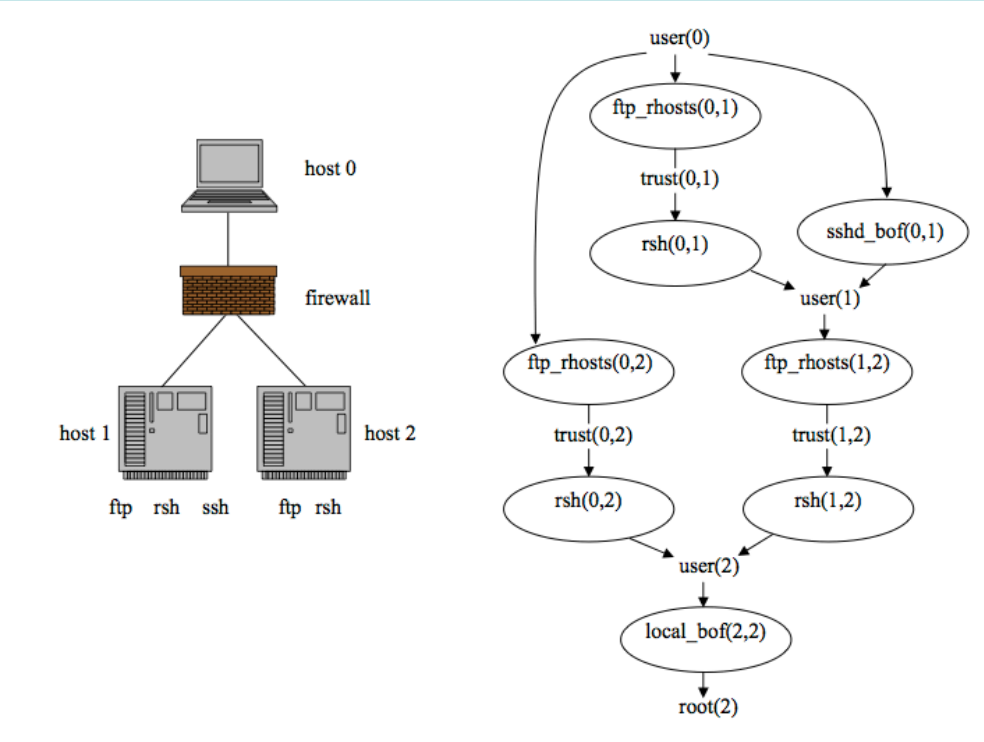
- Entry and exit points, untrusted data and channels
- Not all are created equal
- Analyze for points, monitor for untrusted data/channels



A Formal Model for A System's Attack Surface, Pratyusa K. Manadhata, Dilsun K. Kaynar, and Jeannette M. Wing, CMU Technical Report CMU-CS-07-144, July 2007.

Aggregation using attack graphs

- focus on **composition**, not individual s/w system (pre/post of exploits known)
- based on analysis total effort of "path of attack"
- interesting finds:
  - less vulnerabilities does not mean more security (all must be exploited)
  - security is not equal to path of least effort
  - diversity and security are not related
- can be extended with probabilistic, dynamic view
- automated/real world: attack trees - TVA, vulnerabilities from – CVSS



Lingyu Wang, Anoop Singhal, Sushil Jajodia, "*Toward Measuring Network Security Using Attack Graphs*" Proc. 3rd International Workshop on Quality of Protection (QoP 2007), Oct 29, 2007, pages 49-54.

L5: Managing S/W risk: do's…

- *Risk (€) = Σ Threat Source * Vulnerability * Business Impact(€)*
- Challenge is in quantifying these factors
- As a developer I should track:

The end customers loss databases: measure some T*V*B

My testing and QA activities: measure some V

Honey pot approach: measure some T*V

My development OR: estimate V

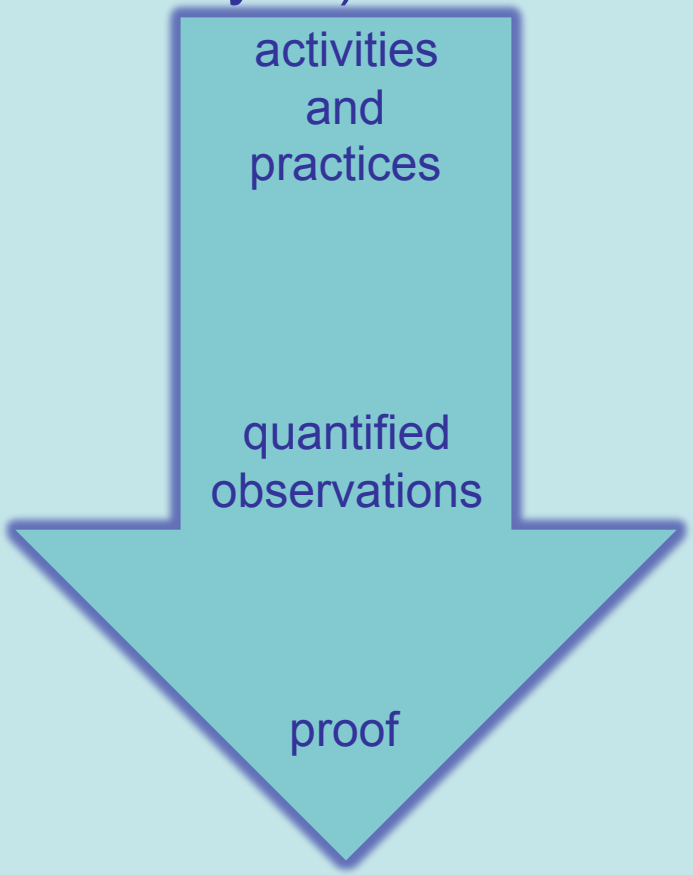
Model approaches: calculate some (proxy of) V
Formal model: proof absence of V

2011 SecAppDev perspective

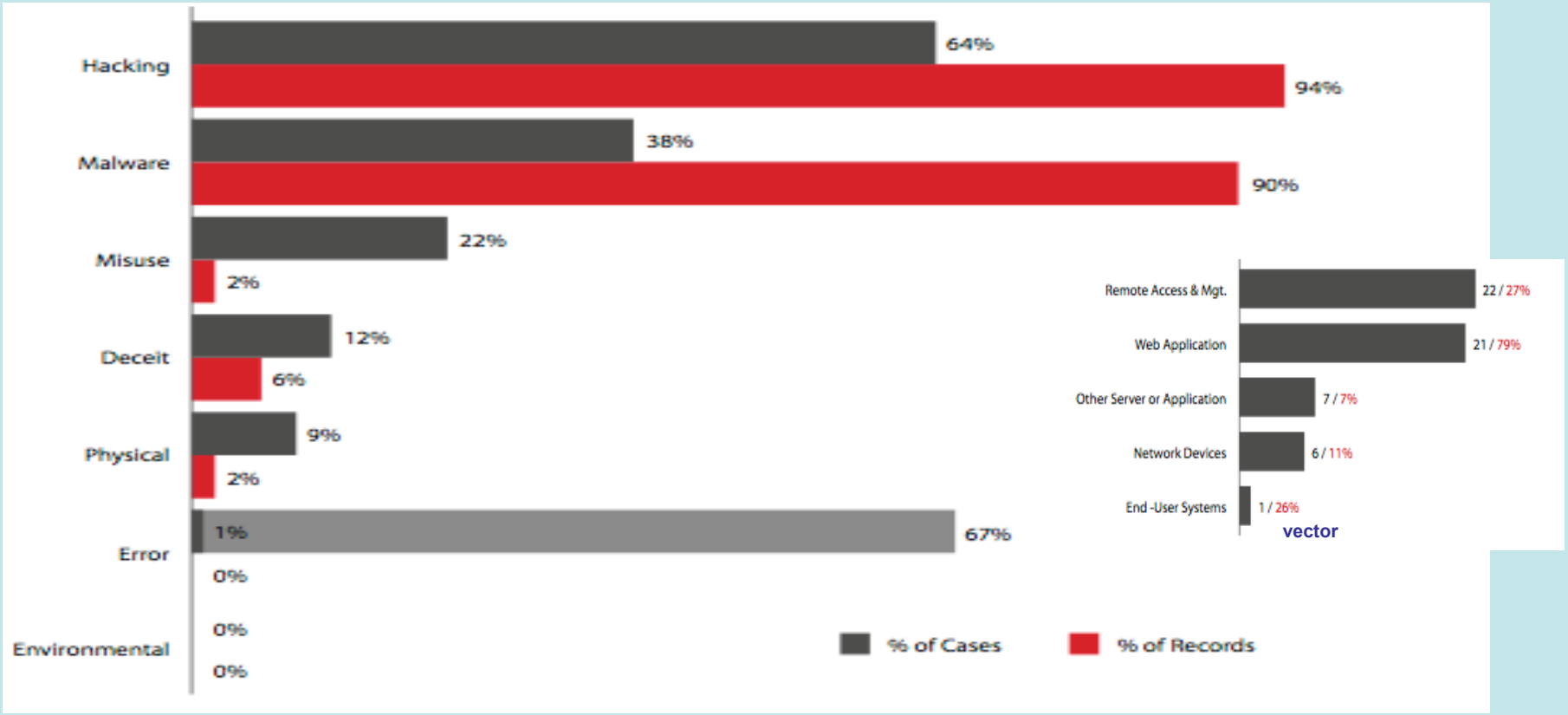
- Finding security vulnerabilities (static analysis) 28/2
- Security testing 24/2
- Architectural risk analysis 28/2
- Hands-on security tools 4/3
- (BSIMM)

- (Indicators)
- (Metrics)

- Models 2/3



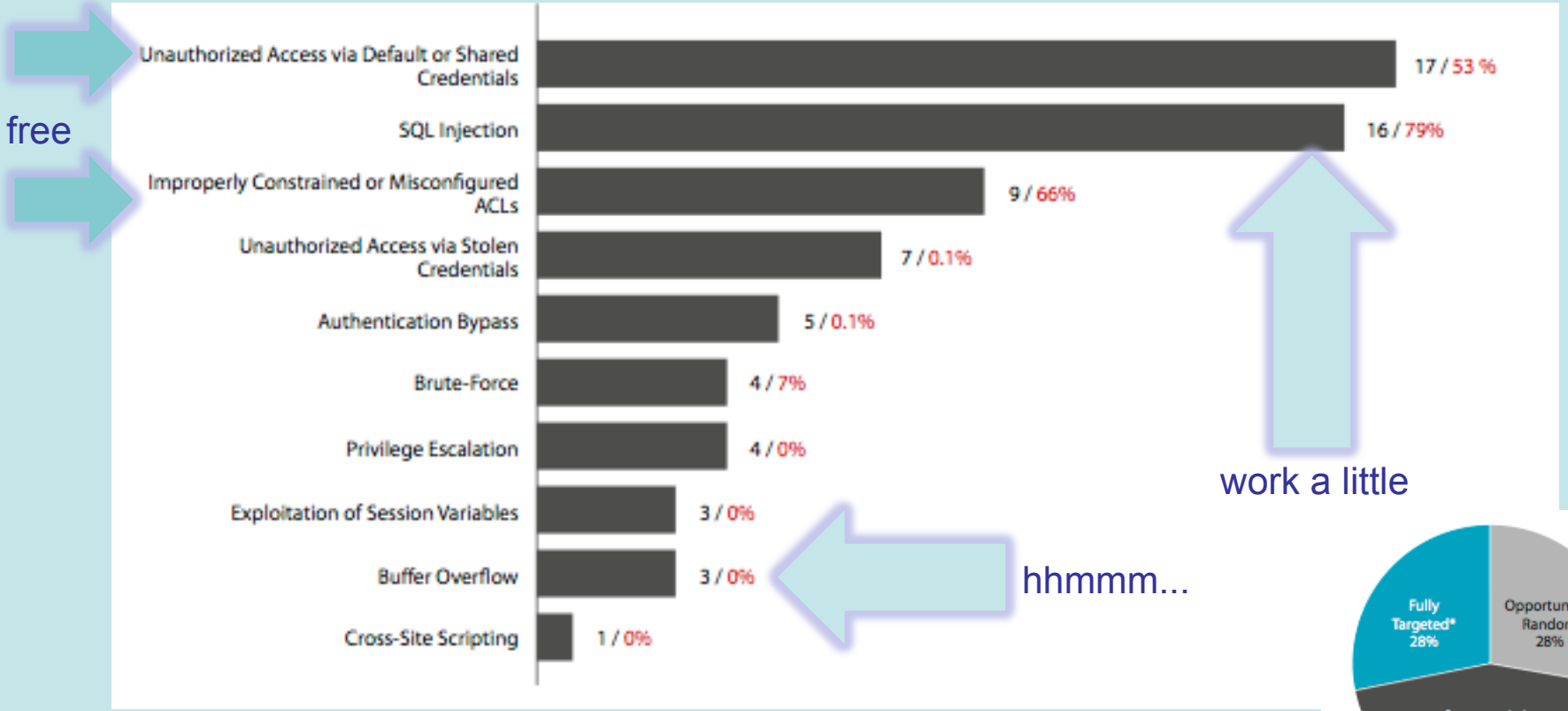
Breach: entry path



Verizon Business DBIR, 2009

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

Breach: nature of the hack



90% of records result from FT

Verizon Business DBIR, 2009

Underground economy

2008 Rank	2007 Rank	Item	2008 Percentage	2007 Percentage	Range of Prices
1	1	Credit card information	32%	21%	$0.06–$30
2	2	Bank account credentials	19%	17%	$10–$1000
3	9	Email accounts	5%	4%	$0.10–$100
4	3	Email addresses	5%	6%	$0.33/MB–$100/MB
5	12	Proxies	4%	3%	$0.16–$20
6	4	Full identities	4%	6%	$0.70–$60
7	6	Mailers	3%	5%	$2–$40
8	5	Cash out services	3%	5%	8%–50% or flat rate of $200–$2000 per item
9	17	Shell scripts	3%	2%	$2–$20
10	8	Scams	3%	5%	$3–$40/week for hosting, $2–$20 design

Symantec, Internet Security Threat Report Volume XIV: April, 2009

A serious hack (TJX, HPY) is worth about 10Mio USD. The average income in say China or Georgia is about 5000 USD yearly. Gonzalez had >1.5Mio in cash when arrested.

Opinion

Underground economy (2)

- Observed value of offered goods (6/2007-7/2008): 275 Mio USD (unique offers)
- Market value: app. 10B USD (about the GDP of Georgia)
- Cookie cutters are cheap, but customization costs

Attack Kit Type	Average Price	Price Range
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150
Shopadmin exploiter	$33	$20–$45
RFI scanner	$26	
LFI scanner	$23	
XSS scanner	$20	

Symantec, various publications

Exploit Type	Average Price	Price Range
Site-specific vulnerability (financial site)	$740	$100–$2,999
Remote file include exploit (500 links)	$200	$150–$250
Shopadmin (50 exploitable shops)	$150	$100–$200
Browser exploit	$37	$5–$60
Remote file include exploit (100 links)	$34	$20–$50
Remote file include exploit (200 links)	$70	$50–$80
Remote operating system exploit	$9	$8–$10

Underground economy (3)

- *Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy*. Herley and Florencio. Microsoft Research, 2009
- lemon market principle
  - asymmetry of information
  - low seller quality (rippers)
- offer goods values and market value are exaggerated.
- 2 tiers: gangs (bypass markets) and technicians (use markets)
- 350M spams bring in 3000 USD but the cost for the regular economy is high
- only the gangs are making money and are fairly invisible

A serious hack (TJX, HPY) is worth about 10Mio USD. TJX cash-out was also about 10Mio USD. Black market economics tend to have market value equal to value of offered goods. Profitability is not huge but still enough and the myth is strong. Analog to drug dealing pyramids.

Opinion

How are we doing?

- Email account
  - 4/2009 100USD, 9/2009 25 USD, 12/2009 12 USD
- the 0wned Price index suggest some deflation
- but not too much…
- our efforts to break the market are not really successful
  - rippers are already present
  - our systems are not secure enough
- deflation:
  - are we losing?
  - or is the black market getting more educated?
  - more entering?

the 0wned Price index, Dan Geer, IEEE Security & Privacy, 1/2009

L6: Security economics lessons

- Except for corner cases, monetary gains are small
- Black market is not very important
- Don’t let security marketers scare you
- … collateral damage is high

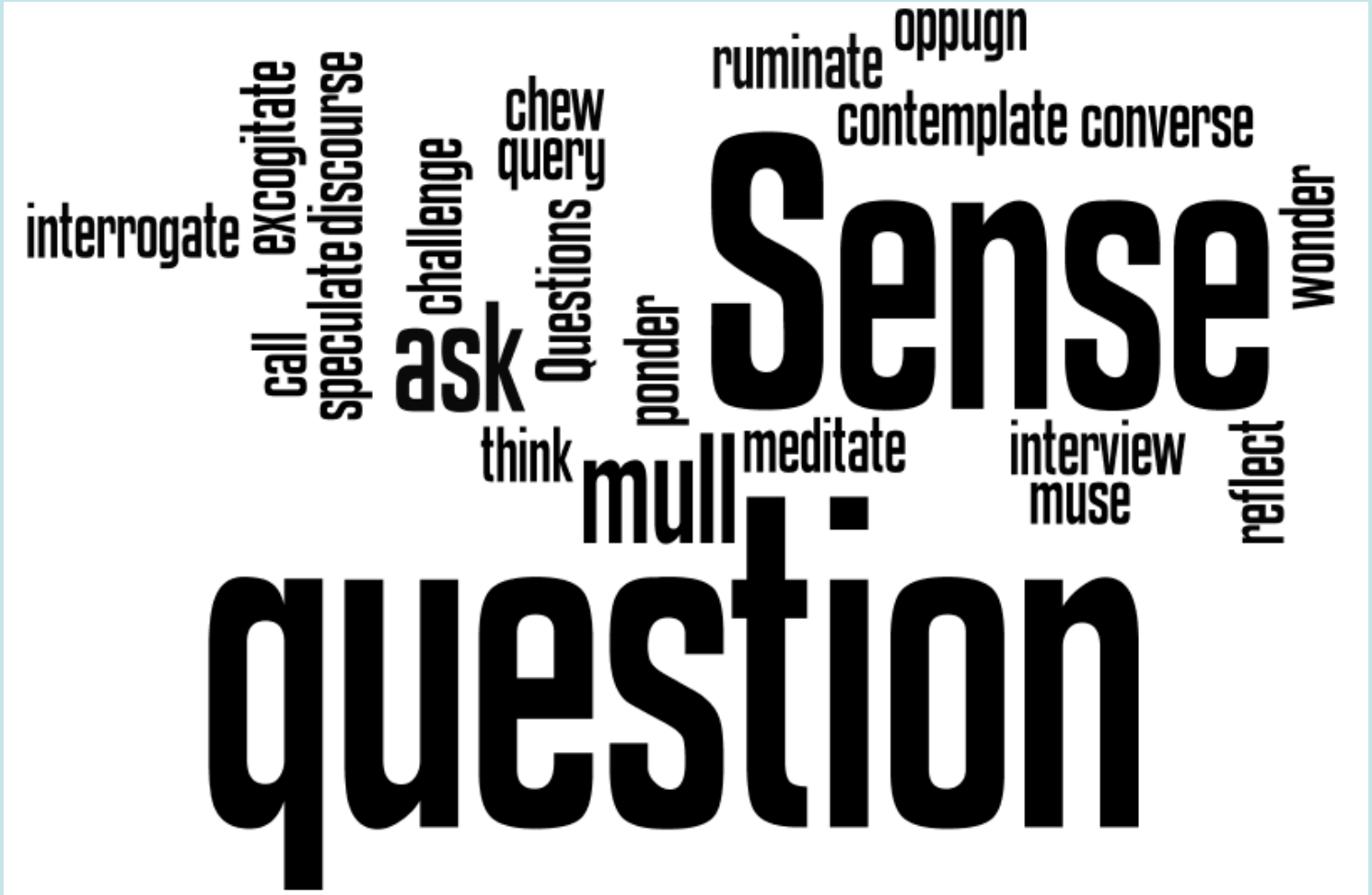
- Traditional market mechanisms do not apply
- … also not for the regular market: eg Metcalfe, 0 production cost
- Expect regulation!

(Regulatory) Mechanisms WILL be introduced to
1. transfer risk from customers to developers 2. Keep markets from becoming monolithic.

Risk becomes more costly for s/w companies

Those that manage well will do better!

Thanks – Q&A!


oppugn
ruminate
contemplate converse
chew
query
excogitate
discourse
challenge
interrogate
Sense
wonder
Questions
ponder
call
speculate
ask
think
mull
meditate
interview
muse
reflect
question