Risk in Analysis and Design

Dan Conway, CISSP, AAGG
University of Notre Dame
dconway@nd.edu

Number of U.S. jobs moving offshore

Job category	2000	2005	2010	2015
Management	0	37,477	117,835	288,281
Business	10,787	61,252	161,722	348,028
Computer	27,171	108,991	276,954	472,632
Architecture	3,498	32,302	83,237	184,347
Life sciences	0	3,677	14,478	36,770
Legal	1,793	14,22	034,673	74,642
Art,design	818	5,576	13,846	29,639
Sales	4,619	29,064	97,321	226,564
Office	53,987	295,034	791,03	1,659,310
Total	102,674	587,592	1,591,101	3,320,213

Source: U.S. Department of Labor and Forrester Research, Inc.
All numbers have been rounded.

What are the components of Risk?

- Asset at risk
  - Value of asset
- Stakeholder / Risk owner / Liability
  - Incentives, Counter-interests
  - Appetite, utility, frame, expectation, value-at-risk
- Potential event
- Probability of event
  - Residual risk, quality of data, assumptions
- Time period / Interest rates / Opportunity costs
- Management Options
  - Accept, Transfer, Insure, Hedge, Exit

Three dimensions of IS design

- Software Engineering
  - Performance, memory usage, on budget, technical issues, compatibility, architecture
- User Acceptance
  - Ease of use, productivity
- Incentive Alignment
  - Alignment with organizational goals, economics, game theory, psychology
  - risk management

Risicare

- Pascal 1623
  - Vacuums, barometric pressure & mercury
  - Pascal's triangle
  - Gravity (outcome) & probability (likelihood) play a role.
  - "God is, or he is not. Reason cannot answer."
- Chevalier de Mere
  - Small margins, multiple samples
- Fermat 1654
  - Analytic geometry, optics, contributions to calculus
  - Number theory

1600's

- John Graunt – 1663
  - Merchant
  - Founder of modern economics
  - Sampling
  - Mortality statistics (facts about the state)
  - Statistical inference
- Edmund Halley 1680
  - Astronomer
  - Detailed population analysis & risk management
  - Created 1st actuarial table (not used for 100 years)
  - Still basis of today's insurance

1600s

- 1666 – Great fire of London burns 80% of town
- 1675 Lloyd's of London coffee house
  - Wealth created for first time
  - Lloyd's list – selling of information as product
  - 1771 Lloyd's becomes self-regulated company

1700s

- Jacob Bernoulli's Law of Large #s
  - Calculating probabilities a posteriori
  - Measured & true means will vary by smaller amt as the samples increase
  - Average or expected value may be very unnatural!
  - Moral certainty was 1000/1001 (now called confidence)
- Daniel Bernoulli – utility theory
  - Appetite for risk involves player preference in risk
  - Human capital introduced
  - Disutility caused by a loss will always exceed the positive utility provided by a gain of equal size – risk aversion
  - Rational person required

1700s

- Abraham DeMoivre
  - Distribution around the mean, std dev
  - Normal curve introduced
  - Confidence Intervals
- Thomas Bayes
  - Combines statistical information about the past with gut feelings about the future

Francis Galton (1822-1911)

- Measurement fetish
- Saw Normal distribution in everything, reversed the concept to identify fraud.
- Sought the "average man"
- Tried to show that superior people were "genetically" gifted – wanted to preserve the best of humanity
- Credited for the concept of "Regression to the Mean"

Regression to the Mean

- Now part of language – "What goes up, must come down"
- Assumption: fundamentals are constant, variation will *eventually* cancel out.
- Produced concepts of
  - Conventional Wisdom
  - Supply/Demand
  - Fundamental change (New Economy)
  - Contrarian investors

The Essence of Risk Management

Lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us.

John Maynard Keynes (1883 - ?)

- Dislikes classical version of rational man
- Writes
  - *A Treatise on Probability,*
  - *The General Theory*
- We simply don't know.
- Little patience w/ decisions based on frequencies of past events
- Proposed active government to reduce uncertainties in economy

John Von Neumann (1903-1957)

- Operations Research, Linear Programming, Digital Computer
- Game Theory
  - Penny game, prisoner's delimma
- Risk Aversion: How far we are willing to go in making decisions that may provoke others to make decisions that will have adverse consequences for us.

Harry Markowitz

- Portfolio Selection – Nobel Prize
  - Studies portfolio vs. individual holding
- Ties expected return with variance
  - Works if you minimize your correlations (covariances)
- Diversification, efficient portfolios & financial engineering
- Game theory – you vs. the market
- Is variance a proper proxy for risk?

People are different

- Kahneman & Tversky
  - Prospect theory
  - the death of the rational person via the failure of invariance
  - Framing questions & risk response.
- David Bell
  - Decision regret
- Thaler & DeBondt
  - Endowment effect

Financial Composite of Risk

- Event/Impact are the same – easy to map one to the other.
- Probability of events – assume log-normal equity price movements.
- Volatility – implied volatility can be computed from historical data.
- Substitute market – interest rates
- Time frame – over what period are we pricing?
- Ownership – who are the players?

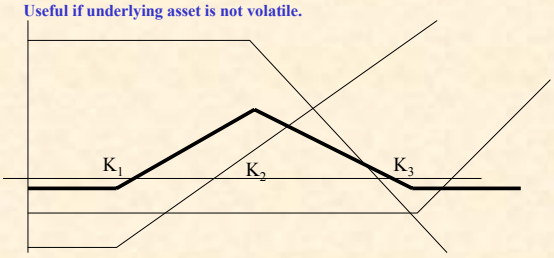
Derivatives & Side Bets

- Derivatives are often options & futures
- These instruments allow a contract to quantify & transfer risk in very complex manners.
- Measures include time, prices, interest rates, and volatility
- See Butterfly Spread…

Build Your Own Distribution

Let $K_1 < K_2 < K_3$.
Buy 2 calls, one with strike price K_1 and one with strike price K_3.
Sell 2 calls with strike price K_2

Useful if underlying asset is not volatile.



What tech risks should we address?

Traditional Information Assurance Risks
- Unauthorized disclosure (confidentiality)
- Unauthorized modification (integrity)
- Loss of use (availability)

Other Risks
- Non-repudiation / accountability
- Legal / regulatory
- Process Risks
- Change management
- Completeness of data

These are technical risks – we'll need to relate them to relevant business risks:
- What if we make decisions from incorrect or incomplete data?
- What if the Notre Dame donor list is disclosed publicly?
- What if an incident occurs which is damages to our reputation?

What controls should we provide?

- Preventive
- Detective
- Corrective

Risk-based Security

- Identify assets
  - Hardware
  - System software
  - Proprietary application software
  - Company data
  - Company secrets
- Identify threats
  - Corruption of data
  - Loss of network
  - Physical disaster
  - Software bugs
  - Crackers or employee terrorism
  - Viruses

What is Risk Analysis?

- Risk Analysis is any method – qualitative and/or quantitative – for assessing the impacts of risk on decision situations.
- The goal is to give the decision maker a better understanding of the possible outcomes that could occur
- Steps
  - Develop a Model
  - Identifying Uncertainty
  - Analyzing the model w/ simulation
  - Making a decision

Best Practices

- Risk mitigation technique is transfer
- Negligence can be avoided
- No solid data is available

Scenario Analysis

- Rank scenarios in order of impact – can be qualitative
- Useful for sales as people tend to overestimate the probability of unlikely events

ALE / VAR

- Annual Loss Expectation or Value at Risk
- Requires
  - scenarios and probabilities
  - Pricing of mitigation methods
- Example (next page)

Threat Severity Analysis

Step	Threat	A	B	C	D
1	Cost if scenario plays out	$500,000	$10,000	$100,000	$10,000
2	Probability of occurrence	80%	20%	5%	70%
3	Threat severity	$400,000	$2,000	$5,000	$7,000
4	Countermeasure cost	$100,000	$3,000	$2,000	$20,000
5	Value of protection	$300,000	($1,000)	$3,000	($13,000)
6	Apply countermeasure?	Yes	No	Yes	No
7	Priority	1	NA	2	NA

Decision Analysis

- Requires
  - Scenarios and probability distributions
  - Pricing of mitigation methods
  - Techniques
    - Simulation environment such as @Risk
    - Closed form equations – stochastic equations

The CSI / FBI Report

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 48-month period

In 2003, 75% of our survey respondents acknowledged financial losses, but only 47% could quantify the losses.

How Money Was Lost

	Lowest Reported				Highest Reported				Average Losses				Total Annual Losses			
	00	01	02	03	00	01	02	03	00	01	02	03	00	01	02	03
Theft of proprietary info.	$1K	$100	$1K	$2K	$25M	$50M	$50M	$55M	$3,032,288	$4,447,900	$6,571,000	$2,699,842	$66,708,200	$151,230,100	$170,827,200	70,195,500
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	919,350	541,000	214,521	27,148,010	5,383,100	15,234,010	5,148,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,0010	76,000
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,114,010	11,066,600	13,055,000	2,754,400
Insider abuse of Net access	240	100	1K	100	15M	10M	10M	6M	317,524	357,160	536,000	135,255	27,686,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	2M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,096,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,371,500	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,374,700	45,288,350	49,079,000	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	310,00	31,254	22,554,500	6,064,000	4,503,010	406,300
Telecom fraud	1K	500	1K	100	3M	8M	100K	250K	212,000	502,278	22,000	50,117	4,028,000	9,041,010	6,015,00	703,510
Active wiretapping	5M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,010	0	0	705,010
Laptop theft	500	1K	1K	2400	1.2M	2M	5M	2M	58,794	61,881	89,000	47,117	10,404,310	8,849,000	11,766,510	6,830,500
												Total Annual Losses	265337,490	377,828,700	455,848,000	202,797,340

CSI/FBI 2003 Computer Crime and Security Survey
Source: Computer Security Institute

IT Security: A Report Card

A look at selected key elements of computer and network security

The Blotter

Percentage of businesses and other organizations saying they detected the following types of attack or misuse in the previous 12 months*

Virus	82%
Insider abuse of Internet access	80
Laptop theft	59
Unauthorized access by insiders	45
Denial of service	42
System penetration	38
Theft of propietary information	21
Sabotage	21
Financial fraud	15
Telecom fraud	10
Telecom eavesdropping	6
Active wiretap	1

*2003 survey of computer-security officials at businesses, government agencies, financial institutions, medical institutions and universities; 490 respondents
Source: Computer Security Institute

The Financial Impact

Total dollar amount of losses by type of attack or misuse among 251 survey respondents

Theft of proprietary information	$70,195,900
Denial of service	65,643,300
Virus	27,382,340
Insider abuse of Internet access	11,767,200
Financial fraud	10,186,400
Laptop theft	6,830,500
Sabotage	5,148,500
System penetration	2,754,400
Active wiretap	705,000
Telecom fraud	701,500
Unauthorized access by insides	406,300
Telecom eavesdropping	76,000

Source: Computer Security Institute

The Offenders

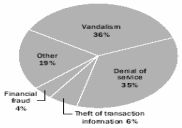
Insiders top the list of likely sources of attack*

Disgruntled employees	86%
Independent hackers	74
U.S. competitors	53
Foreign companies	30
Foreign governments	21

*2003 survey, 488 respondents
Source: Computer Security Institute

Internet Attacks

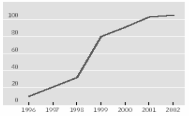
Web-site incidents, by type



Source: Computer Security Institute

The Spread of Viruses...

The monthly rate of infection per 1,000 PCs*



*Based on data for November and December of each year
Source: ICSA Labs

...And Where They Come From

The means of infection for respondents' latest virus incident, 2002 survey

E-mail attachment	86%
Internet downloads	11
Web browsing	4
Don't know	1
Other	3

Note: Figures total more than 100% due to multiple responses
Source: ICSA Labs

Playing Defense

Spending on computer security software (in millions)

Category	2002	2007	Growth[1]
Secure content management[2]	$2,694.5	$6,379.5	18.8%
User authentication, authorization, administration software	$2,487.3	$5,063.9	15.3%
Firewall/VPN software	$891.7	$1,179.4	5.8%
Intrusion detection	$723	$1,548.5	16.4%
Encryption	$249.2	$518.2	15.8%

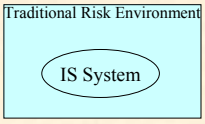
[1]Cumulative annual growth rate, 2002-07
[2]Includes antivirus, content filtering and antispam software
Source: IDC

Data & Metrics

- We can cure people of rolling 6's!
- Data has already been through some degree of risk management
- Difficulty of mapping event to costs
- Forecasting – Who doesn't make changes based on the past? Why assume others won't?
- If information has time-value and is a competitive asset, who has incentive to share it honestly?

Application Development w/ Risk

How information systems are designed today



All systems operate within a risk context

Environmental:

Interest rates, competitive landscape, model assumptions, options for management (hedge, outsource, exit, accept, transfer)

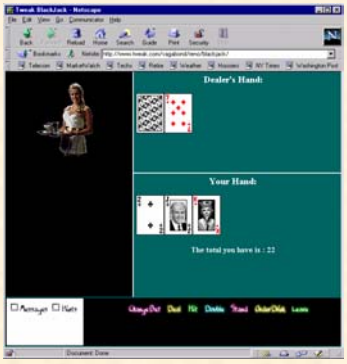
Management:

incentives, punishments, physical controls, policies, procedures, norms, legal backdrop, job rotation, separation of duties, common sense

Technology:

Access controls, VPNs, packet-based layered filtering

Anything different on the net?

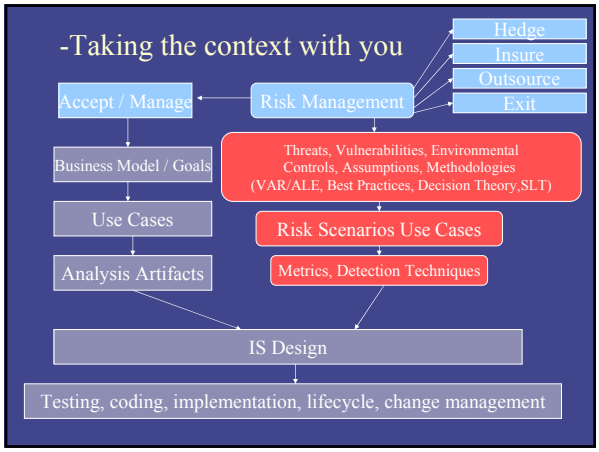


Interface Agents and Gaming

- What environmental controls exist in the physical world that don't yet have an equivalent in the virtual world?
  - Common sense
  - Cameras
  - Identity management
  - Distractions
  - Gaming commission
  - Intimidation

Removing a system from its controlling context

- Previous controls and monitoring are ineffective
- Systems are currently designed to operate only in one context.



Regulatory Risks

- GLB Privacy
- HIPPA Healthcare Privacy
- Sarbanes-Oxley Internal Control
  - (404 is IS security controls section)

How does a system know if it is being misused?

- Requires metrics to determine "Normal" or expected behavior (DeMoivre, Gauss)
- Monitors statistical anomalies like an IDS
- Must be post transaction, but not too post.
- Must have documentation for liability protection.

Your future…

- Computer programs are like hash functions. They must generate not only an output (4), but also process metadata stating how that output was arrived at, as well as a digital signature from a risk management authority module.

Example of Risk Output

```
<Output>
    <value>4</value>
    <routine description = "Multiply by 2" priorRoutine = "Lookup Month">
        <input>2</input>
    </routine>
    <routine description = "Lookup Month" priorRoutine = "Class CalcRent
    constructor">
        <input>1</input>
    </routine>
    <RiskSignature entity=RM1 encoding=Base64 hashAlgorithm=SHA-1
    pkAlgorithm=RSA>
        a4Ey9Kqp3XrIc48
    </RiskSignature>
</Output>
```

Measurement is the first step

- Property records enabled property taxes
- Unemployment records enabled unemployment insurance.
- Mortality figures enabled life insurance.

- NIST 800-30 gives guidelines for Risk Management and Information Technology Systems