

The Psychology of Security

Bruce Schneier

InfoSec

London

25 April 2007



Security

- A feeling and a reality
- Different
 - You can feel secure even though you aren't secure
 - You can be secure even though you don't feel secure
- Really, two different words

Security as a Trade-Off

- Security is always a trade-off
- You are a security consumer
- Is it worth it?
 - Bullet-proof vests
 - Home burglar alarms
 - Invading Iraq
- People have natural intuitions about trade-offs
 - We do it every day
 - Rabbits do it
- Why do we get it wrong so often?

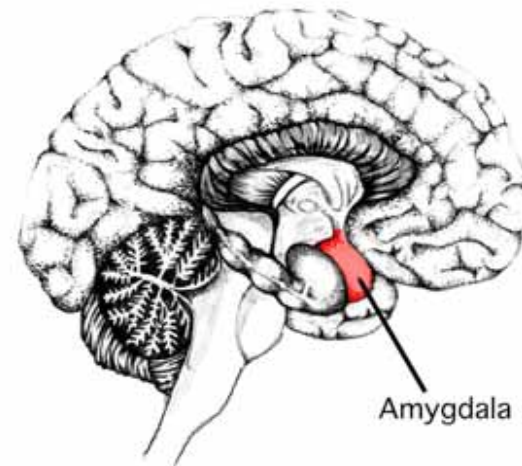
Aspects of the Trade-Off

1. The severity of the risk
2. The probability of the risk
3. The magnitude of the costs
4. How effective the countermeasure is at mitigating the risk
5. The trade-off itself

Amygdala

- Ancient part of the brain
- Controls “flight or fight” reflex
 - Adrenaline
 - Increased heart rate
 - Increased muscle tension
 - Sweaty palms
- Very fast, faster than consciousness
- Can be overridden by higher parts of the brain
 - But it takes effort

Amygdala The amygdala is a small structure lying in the medial temporal lobe which is important for the emotional content of new memories.



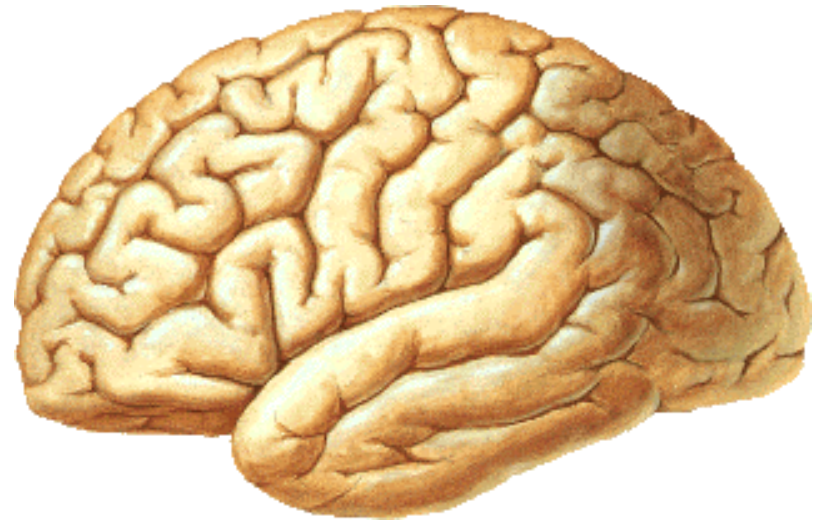
by Catherine E. Myers. Copyright © 2006 *Memory Loss and the Brain*
Artwork copyright © 2000 Ann L. Myers

Neocortex

n
e
w

m
e
m
o
r
i
e
s
.

- The part of the mammalian brain associated with consciousness
 - Thinking
 - Reasoning
- Newest part of the brain
- Slower
- Uses heuristics
 - Rules of thumb
 - Biases
 - Generally beneficial, but can fail



“Common Sense” About Risks

People exaggerate risks that are:	People downplay risks that are:
Spectacular	Pedestrian
Rare	Common
Personified	Anonymous
Beyond their control, or externally imposed	More under their control, or taken willingly
Talked about	Not discussed
Intentional or man-made	Natural
Immediate	Long-term
Sudden	Evolving slowly over time
Affecting them personally	Affecting others
New and unfamiliar	Familiar
Uncertain	Well-understood
Directed against their children	Directed against themselves
Morally offensive	Morally desirable
Entirely without redeeming features	Associated with some ancillary benefit
Not like their current situation	Like their current situation

Risk Heuristics: Prospect Theory: Experiment 1

- Group 1, given the choice between:
 - A sure gain of \$500
 - A 50% gain of \$1,000
- Group 2, given the choice between:
 - A sure loss of \$500
 - A 50% loss of \$1,000

Risk Heuristics: Prospect Theory: Experiment 1

- Group 1, given the choice between:
 - A sure gain of \$500 **84%**
 - A 50% gain of \$1,000
- Group 2, given the choice between:
 - A sure loss of \$500
 - A 50% loss of \$1,000 **70%**

Risk Heuristics: Prospect Theory: Experiment 2

- Imagine preparing for the outbreak of a disease expected to kill 600 people.
- Group 1:
 - Program A: “200 people will be saved.”
 - Program B: “There is a one-third probability that 600 people will be saved, and a two-thirds probability that no people will be saved.”
- Group 2:
 - Program C: “400 people will die.”
 - Program D: “There is a one-third probability that nobody will die, and a two-third probability that 600 people will die.”

Risk Heuristics: Prospect Theory: Experiment 2

- Imagine preparing for the outbreak of a disease expected to kill 600 people.
- Group 1:
 - Program A: “200 people will be saved.” **72%**
 - Program B: “There is a one-third probability that 600 people will be saved, and a two-thirds probability that no people will be saved.”
- Group 2:
 - Program C: “400 people will die.”
 - Program D: “There is a one-third probability that nobody will die, and a two-third probability that 600 people will die.” **78%**

Risk Heuristics: Prospect Theory: Endowment Effect

■ Mug experiment

- Half of subjects given a mug
- Those who have one are asked the price they're willing to sell
- Those who don't have one are asked the price they're willing to buy

■ Pen/mug experiment

- Half of subjects given a mug, half given a pen
- Subjects asked whether or not they would like to change

Risk Heuristics: Prospect Theory: Endowment Effect

■ Mug experiment

- Half of subjects given a mug
- Those who have one are asked the price they're willing to sell
- Those who don't have one are asked the price they're willing to buy **Sell price twice asking price**

■ Pen/mug experiment

- Half of subjects given a mug, half given a pen
- Subjects asked whether or not they would like to change

Risk Heuristics: Prospect Theory: Endowment Effect

■ Mug experiment

- Half of subjects given a mug
- Those who have one are asked the price they're willing to sell
- Those who don't have one are asked the price they're willing to buy **Sell price twice asking price**

■ Pen/mug experiment

- Half of subjects given a mug, half given a pen
- Subjects asked whether or not they would like to change

Only 22% change

Risk Heuristics: Other Heuristics

- Optimism bias
- Control bias
- Risks involving people
- Risks involving children

Probability Heuristics: Availability Heuristic

- In a typical sample of text in the English language, is it more likely that a word starts with the letter K or that K is its third letter (not counting words with fewer than three letters)?
- Football experiment
- Presidential election experiment

Probability Heuristics: Availability Heuristic

- In a typical sample of text in the English language, is it more likely that a word starts with the letter K or that K is its third letter (not counting words with fewer than three letters)? **70% said 1st letter**
- Football experiment **Twice as many 3rd letter**
- Presidential election experiment

Probability Heuristics: Availability Heuristic: Vividness

■ Pallid vs. vivid:

- On his way out the door, Sanders [the defendant] staggers against a serving table, knocking a bowl to the floor.
- One his way out the door, Sanders staggers against a serving table, knocking a bowl of guacamole dip to the floor and splattering guacamole on the white shag carpet.

■ Pallid vs. vivid:

- The owner of the garbage truck admitted under cross-examination that his garbage truck is difficult to see at night because it is grey in color.
- The owner of the garbage truck admitted under cross-examination that his garbage truck is difficult to see at night because it is grey in color. The owner said his trucks are grey “because it hides the dirt,” and he said, “What do you want, I should paint them pink?”

Probability Heuristics: Availability Heuristic: Other

- Worst memory is most available
- Hindsight bias

Probability Heuristics: Representativeness

- Linda is 31 years old, single, outspoken, and very bright. She majored in philosophy. As a student, she was deeply concerned with issues of discrimination and social justice, and also participated in antinuclear demonstrations. Please check off the most likely alternative:
 - Linda is a bank teller.
 - Linda is a bank teller and is active in the feminist movement.

Probability Heuristics: Representativeness

- Linda is 31 years old, single, outspoken, and very bright. She majored in philosophy. As a student, she was deeply concerned with issues of discrimination and social justice, and also participated in antinuclear demonstrations. Please check off the most likely alternative:
 - Linda is a bank teller.
 - Linda is a bank teller and is active in the feminist movement.

90%

Cost Heuristics: Mental Accounting: Experiment 1

- Trade-off 1: Imagine that you have decided to see a play where the admission is \$10 per ticket. As you enter the theater, you discover that you have lost a \$10 bill. Would you still pay \$10 for a ticket to the play?
- Trade-off 2: Imagine that you have decided to see a play where the admission is \$10 per ticket. As you enter the theater, you discover that you have lost the ticket. The seat is not marked and the ticket cannot be recovered. Would you pay \$10 for another ticket?

Cost Heuristics: Mental Accounting: Experiment 1

- Trade-off 1: Imagine that you have decided to see a play where the admission is \$10 per ticket. As you enter the theater, you discover that you have lost a \$10 bill. Would you still pay \$10 for a ticket to the play?
88% yes
- Trade-off 2: Imagine that you have decided to see a play where the admission is \$10 per ticket. As you enter the theater, you discover that you have lost the ticket. The seat is not marked and the ticket cannot be recovered. Would you pay \$10 for another ticket?
46% yes

Cost Heuristics: Mental Accounting: Experiment 2

- Imagine that you are about to purchase a jacket for \$125, and a calculator for \$15. The calculator salesman informs you that the calculator you wish to buy is on sale for \$10 at the other branch of the store, located 20 minutes' drive away. Would you make the trip to the other store?
- Imagine that you are about to purchase a jacket for \$15, and a calculator for \$125. The calculator salesman informs you that the calculator you wish to buy is on sale for \$120 at the other branch of the store, located 20 minutes' drive away. Would you make the trip to the other store?

Cost Heuristics: Mental Accounting: Experiment 2

- Imagine that you are about to purchase a jacket for \$125, and a calculator for \$15. The calculator salesman informs you that the calculator you wish to buy is on sale for \$10 at the other branch of the store, located 20 minutes' drive away. Would you make the trip to the other store? **68% yes**
- Imagine that you are about to purchase a jacket for \$15, and a calculator for \$125. The calculator salesman informs you that the calculator you wish to buy is on sale for \$120 at the other branch of the store, located 20 minutes' drive away. Would you make the trip to the other store? **29% yes**

Cost Heuristics: Time Discounting

- People are indifferent to:

- \$15 today and \$60 In twelve months (139%)
- \$250 today and \$350 in twelve months (34%)
- \$3,000 today and \$4,000 in twelve months (29%)

- Framing effects

- Acceleration vs. delay

Other Decision-Making Heuristics

- Context effect
- Choice bracketing
- Anchoring effect

Other Decision-Making Heuristics: Anchoring Effect

- Question 1: Should divorce in this country be easier to obtain, more difficult to obtain, or stay the same?
- Question 2: Should divorce in this country be easier to obtain, stay the same, or be more difficult to obtain?

Other Decision-Making Heuristics: Anchoring Effect

- Question 1: Should divorce in this country be easier to obtain, more difficult to obtain, or stay the same?
- Question 2: Should divorce in this country be easier to obtain, stay the same, or be more difficult to obtain?

23% easier, 36% harder, 41% same

26% easier, 46% harder, 29% same

What does this all mean?

“The Psychology of Security”

<http://www.schneier.com/essay-155.html>

Useful Resources from Bruce Schneier

Crypto-Gram: Free Monthly Security Newsletter

by Bruce Schneier

www.schneier.com/crypto-gram.html

Bruce Schneier

October 15, 2003

by Bruce Schneier
Founder and CTO
Counterpane Internet Security, Inc.
schneier@counterpane.com
<<http://www.schneier.com>>
<<http://www.counterpane.com>>

A free monthly newsletter providing summaries, analyses, insights, and commentaries on security: computer and otherwise.

Back issues are available at <<http://www.schneier.com/crypto-gram.html>>. To subscribe, visit <<http://www.schneier.com/crypto-gram.html>> or send a blank message to crypto-gram-subscribe@chapparraltree.com.

In this issue:

- [The Future of Surveillance](#)
- [Crypto-Gram Reprints](#)
- [SmartShield](#)
- [The Patriot Act and Mission Creep](#)
- [News](#)
- [Counterpane News](#)
- [More Beyond Fear Reviews](#)
- [Security Notes from All Over: Reaction to a Bomb Threat](#)
- [Pirating Movies](#)
- [Security Notes from All Over: Precision Stripping](#)
- [Issuing Identity Cards](#)
- [Security Risks of Monoculture](#)
- [Comments from Readers](#)

The Future of Surveillance

At a gas station in Coquitlam, British Columbia, two employees installed a camera in the ceiling in front of an ATM machine. They recorded thousands of people as they typed in their PIN numbers. Combined with a false front on the ATM that recorded account numbers from the cards, the pair was able to steal millions before they were caught.

In at least 14 Kinko's copy shops in New York City, Juju Jang installed keystroke loggers on the rentable computers. For over a year he eavesdropped on people, capturing more than 450 user names and passwords, and using them to access and open bank accounts online.

A lot has been written about the dangers of increased government surveillance, but we also need to be aware of the potential for more pedestrian forms of surveillance. A combination of forces -- the miniaturization of surveillance technologies, the falling price of digital

Useful Resources from Bruce Schneier

Schneier on Security: Free Security Blog by Bruce Schneier

www.schneier.com/blog



The screenshot shows the homepage of the 'Schneier on Security' blog. The header features the author's name 'Bruce Schneier' and the blog title 'Schneier on Security' with a subtitle 'A weblog covering security and security technology.' The main content area displays a recent post titled 'Random Observation from the RSA Conference' by Dave Barry, dated February 06, 2007. The post text discusses the industry's lack of good names for security companies and lists security measures for the Super Bowl game, such as arrival times, prohibited items, and tailgating. A sidebar on the right includes a 'Weblog Menu' with a search box and radio buttons for 'blog only' and 'whole site', a 'Recent Entries' list with links to various articles, and a 'Bloggers on Blogging' section.

Bruce Schneier

Schneier on Security
A weblog covering security and security technology.

Random Observation from the RSA Conference
[Protegrity?](#) [Counterstorm?](#) [Authenticate?](#)

I officially declare that the industry has run out of good names for security companies.

Posted on February 06, 2007 at 10:03 AM • 18 Comments
[Dig this](#) • [Add to del.icio.us](#)

Dave Barry on Super Bowl Security
Funny:

Also, if you are planning to go to the Super Bowl game on Sunday, be aware that additional security measures will be in effect, as follows:

- **WHEN TO ARRIVE:** All persons attending the game **MUST** arrive at the stadium no later than 7:45 a.m. yesterday. There will be **NO** EXCEPTIONS. I am talking to you, Prince.
- **PERSONAL BELONGINGS:** Fans will not be allowed to take anything into the stadium except medically required organs. If you need, for example, both kidneys, you will be required to produce a note from your doctor, as well as your actual doctor.
- **TAILGATING:** There will be no tailgating. This is to thwart the terrorists, who are believed to have been planning a tailgate-based attack (code name "Death

Weblog Menu

Search

blog only
 whole site

Recent Entries

[Random Observation from the RSA Conference](#)

[Dave Barry on Super Bowl Security](#)

[Business Models for Discovering Security Vulnerabilities](#)

[Social Science and the "War on Terror"](#)

[Friday Squid Blogging: Squid Art](#)

[Bloggers on Blogging](#)

[Excessive Secrecy and Security Helps Terrorists](#)

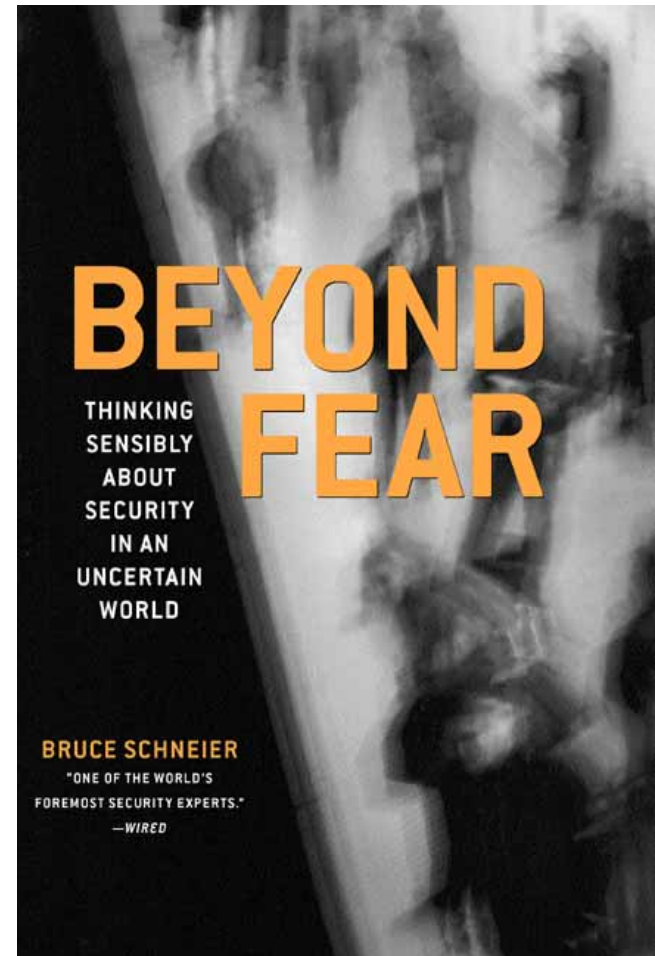
Non-Terrorist

Useful Resources from Bruce Schneier

Beyond Fear: Thinking Sensibly about Security in an Uncertain World

by Bruce Schneier

www.schneier.com/bf.html



BT Counterpane

1090 La Avenida Street | Mountain View, CA 94043 | USA

1.888.710.8175

sales@counterpane.com

