



Donau-Universität Krems

Zentrum für praxisorientierte Informatik
Dr. Karl-Dorrek Straße 30
A-3500 Krems/Donau

Understanding a hacker's mind – A psychological insight into the hijacking of identities

a White Paper by the Danube-University Krems, Austria
Christian S. Föttinger
Wolfgang Ziegler

Commissioned by RSA Security

Table of Contents

1. Introduction	page 2
2. Identity Theft – A menace to society	page 2
3. Hackers – The anonymous threat?	page 4
3.1. Typology – Who are Hackers and what makes them tick?	page 5
3.2. The good and the evil - Ideology and ethics of hackers	page 6
3.3. Self-assessment by Hackers	page 11
3.4. Psychological and sociological drivers	page 19
3.5. Methodology	page 23
3.6. A study by the German BKA (Bundeskriminalamt)	page 26
3.7. Conclusion	page 35
4. Best practice	page 35
4.1. Individuals	page 42
4.2. Companies	page 43
4.3. Industry	page 45
5. Conclusion	page 46
6. References	page 48



1. Introduction

With the explosion of Internet usage ushering in the Information Age, around 300 million computer users are now connected to each other through a maze of networks. However security considerations have generally lagged behind the rush to get networked and go online, with the result that each connection to a network also represents a potential opening for hackers. DSL and cable modems, the equivalent of always-on, high-speed connections for personal computer users, pose particular security problems because they provide more resources and bandwidth to hide misuse. In short, if your computer is connected to the Internet, you can be verified by hackers for potential attacks.

This paper explores both the scope and the intentions of hackers – and furthermore, how enterprises are victimised, especially in terms of identity theft. It was important to us to understand the minds of hackers; therefore we spent time analysing their psychological and sociological drivers as well as their intentions and methodologies. We examined recent abstracts and research projects conducted by prominent academics and experts, including an empiric study by the German Bundeskriminalamt (BKA) that aims to sensitise society in terms of identity theft, underlining theory with examples from the real world. The discussion then turns to issues of accountability and outcomes, and describes best security practices for thwarting identity-related crime with a solution-orientated approach.

2. Identity theft – A menace to society

Not a week goes by without a newsworthy identity theft incident taking place somewhere around the world. As an example, a news report in April 2003 stated that, “Names, addresses and credit card data of sponsors of the Georgia Institute of Technology in Atlanta have been hacked. Online intruders have stolen 57,000 identities over the last two months. There is no information yet on the attackers.”

While estimates vary widely, there is no doubt that identity theft is widespread, fast-growing and costly to society. The Federal Trade Commission (FTC) reported in September 2003 that identity theft had affected nearly 10 million Americans and cost almost \$53 billion in the previous year. Reported incidents increased 73% from 2001 to 2002 and accounted for 43% of the complaints fielded by the FTC. Worldwide, identity theft and related crimes were projected to cost an estimated \$221 billion in 2003, and experts believe the problem will get worse before it gets better. If the current 300% compound annual growth rate continues, annual losses worldwide could top \$2 trillion by 2005. (1)

Identity theft is a prevalent crime today. It is easy for someone to steal your identity in many ways, and this information is then used to apply for credit cards in your name, charge goods to your credit cards, get loans under your name, and even take money from your own checking accounts. The theft of one's identity can be done by stealing your mail, getting receipts from stores, or even by gaining access to information you have on your computer or on Web sites you access to buy goods. And, what is worse, if your identity is stolen it can be a long, tedious, and sometimes painstaking process to correct the wrongs that are committed.

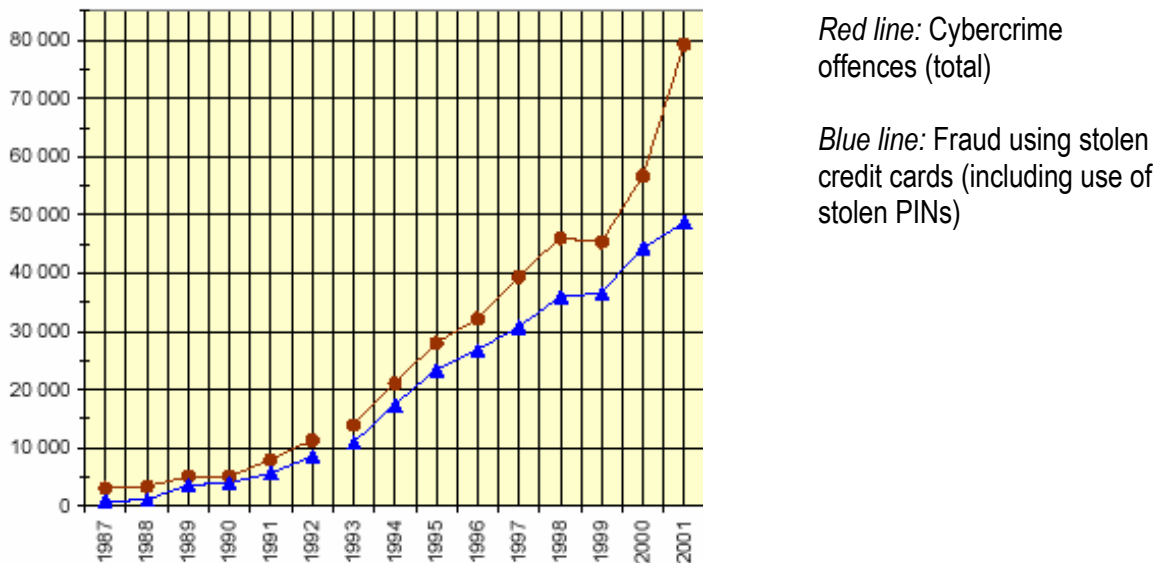


Figure1 - Identity theft in Germany (2)

The Internet is becoming an ever-more popular resource for thieves who wish to gain information to conduct identity theft.

Identity theft is a quick and easy way to gain money with a low probability of prosecution. All that is needed is your social security number, your date of birth and other basic identification information such as your address and phone number. With this information the crime can begin. The intruder applies in person for instant credit, or through the mail by posing as you. They will often provide their own address, claiming to have moved. Other ways involve lifting people's credit cards numbers and trying to use them for personal gain. Sometimes if a person or group steals a quantity of credit cards they will buy small items here or there to test it out. If successful they will wait to make a large purchase and sell that product back for cash. Negligent credit organisations, in their haste to issue credit, do not always verify the supplied information or even the address. Once the impostor opens the first account, they use this new account along with the other ID information to add to their credibility. This facilitates the proliferation of the fraud. Now the thief is well on his/her way to getting rich – and ruining both your credit record and your reputation. (3)

Systematic in nature, identity theft is a consequence of the information-driven society we live in. Over the course of a lifetime, the typical citizen willingly surrenders personal information to dozens or even hundreds of different entities. This data ends up being stored electronically – often with weak or negligible protection. Identity information is often sent through the traditional mail system where it can be easily diverted.

To obtain someone's identity, a hacker can take advantage of weak passwords or security vulnerabilities, either by watching transactions via the Web or by attacking servers directly. Once the hacker has obtained personal information they often go to a hacker chat room. This is a place on the Web using an Internet Relay Chat, which provides these culprits with some anonymity and allows them to mention that they have this 'special information' and are willing to trade it. In this context, hackers are motivated to steal identities by two things: one is obviously profit, the opportunity to make a buck, and the other is just to show that they can do it.

Unfortunately identity theft is very easy to do. On one hand we have security vulnerabilities on servers, and sometimes sensitive data is stored on Web servers; on the other hand many users don't sufficiently protect their PCs. Passwords can be cracked within minutes, so it is necessary to protect private PCs with a personal firewall and for companies to ensure that sensitive data is encrypted.

There are varying objectives for those who commit identity theft: *felonies, terrorism, financial crimes and online attacks.*

After focusing on the intentions and psychological drivers for hackers, we will be able to categorise those different objectives according to the personality-profile of the intruder.

3. Hackers – The anonymous threat?

To understand a person's intention and motivation to hack into a system we have first to analyse their background, psychology and social environment. We have to be very clear how intruders tick. The image of the typical computer criminal that is often conveyed by the media can be misleading – and can hamper our efforts to implement an appropriate defence...

Research to date indicates that criminal computer behaviour is on the rise and will continue to be so for the next few years. Therefore it is important that we develop a reasonable understanding of those people who become involved; elements of this understanding must include personality characteristics, motivations, and what attracts these criminals in the first place.

Bruce Schneier, the well-known information security guru, states: "In this same vein, computer networks have been plagued for years by hackers breaking into them. But these people aren't breaking into systems for profit; they don't commit fraud or theft. They're breaking into systems to satisfy their intellectual curiosity, for the thrill, and just to see if they can... Hackers' traditional and common defence is that they're breaking into systems to test their security. They say the only way to learn about computer and network security is to attack systems. Never mind that these hackers don't own the systems they're breaking into; that's just the excuse." He points out that there is an ongoing controversial discussion about whether hackers are genuinely committing criminal acts

while intruding into a network: “*I was only testing security*” is not a valid defence. For years, we in the computer security field have heard that excuse. Because the hacker didn’t intend harm, because he just broke into the system and merely looked around, it wasn’t a real crime. Here’s a thought for you: imagine you return home and find the following note attached to your refrigerator: “I was testing the security of back doors in the neighborhood and found yours unlocked. I just looked around. I didn’t take anything. You should fix your lock.” Would you feel violated? Of course you would.” (4)

3.1. Typology – Who are Hackers and what makes them tick?

Two experts in the field of cyber-forensics and psychology have some answers to this question. One is Marc Rogers, a behavioural sciences researcher at the University of Manitoba in Winnipeg, Canada, and a former cyber-detective. The other is Jerrold M. Post, a psychiatrist at George Washington University in Washington, D.C.

Rogers and Post have identified some basic behavioural trends in hackers who commit crimes. Rogers says one characteristic is that they tend to minimise or misconstrue the consequences of their activities, rationalising that their behaviour is really performing a service to society. (Some researchers call this the *Robin Hood Syndrome*). They may also tend to dehumanise the problem and blame the ‘victim sites’ that they attack. Post says the same hackers share a sense of “ethical flexibility”, which means that since human contact is minimised over the computer, hacking becomes like a game where the serious consequences can be easily ignored.

But Rogers is careful to point out that not all hackers are criminals. He’s identified four categories as follows:

- I. **Old School Hackers:** These are your 1960s style computer programmers from Stanford or MIT for whom the term ‘hacking’ is a badge of honour. They’re interested in lines of code and analysing systems, but what they do is not related to criminal activity. They don’t have a malicious intent, though they may have a lack of concern for privacy and proprietary information because they believe the Internet was designed to be an open system.
- II. **Script Kiddies or Cyber-Punks:** most commonly what the media call “hackers”. These are the kids, like Mafia Boy, who most frequently get caught by authorities because they brag online about their exploits. As an age group, they can be between 12 and 30 years old; they’re predominantly white and male; and on average have a grade 12 education. Bored in school, very adept with computers and technology, they download scripts or hack into systems with intent to vandalise or disrupt. There is also the “wannabee” hacker phenomenon: the would-be hackers. Historical note: The wannabee phenomenon has a slightly different flavour now (1993) than it did ten or fifteen years ago. When the people who are now hackerdom’s tribal elders were in larval stage, the process of becoming a hacker was largely unconscious and unaffected by models renowned in popular culture -- communities formed spontaneously around people who, as *individuals*, felt irresistibly drawn to do hackerly

things, and what wannabees experienced was a fairly pure, skill-focused desire to become similarly wizardly. Those days of innocence are gone forever; society's adaptation to the advent of the microcomputer after 1980 included the elevation of the hacker into a new kind of folk hero, and the result is that some people now semi-consciously set out to *be hackers* and borrow hackish prestige by fitting the popular image of hackers. Fortunately, to do this really well, one has to actually become a wizard. Nevertheless, old-time hackers tend to share a poorly articulated disquiet about the change; among other things, it gives them mixed feelings about the effects of public compendia of lore like this one.

- III. **Professional Criminals, or Crackers:** These guys make a living breaking into systems and selling the information. They might get hired for corporate or government espionage. They may also have ties to organised criminal groups.
- IV. **Coders and Virus Writers:** Not a lot of research has been done on these guys. They like to see themselves as an *elite*. They have a lot of programming background and write code but won't use it themselves. They have their own networks to experiment with, which they call "Zoos." They leave it to others to introduce their codes into "The Wild," or the Internet.

Underlying the psychology of the criminal hacker may be a deep sense of inferiority. Consequently, the mastery of computer technology, or the shut down of a major site, might bestow on them a sense of power. "It's a population that takes refuge in computers because of their problems sustaining real world relationships," says Post. "Causing millions of dollars of damage is a real power trip." (5)

3.2. The good and the evil - Ideology and ethics of hackers

There is a consistent perception amongst the population about the typical hacker. These images are usually driven by the media. When incidents involving hackers take place it is very common for the press to project all manner of evil on this interest group. But who can blame them? Marc Rogers' classification above is not widely known or understood, with the result that most people do not distinguish between a hacker and a criminal.

No matter how deeply we discuss this topic in theory, one fact remains: hackers are something of a myth for society, because we cannot deal rationally with them. Once again, a person who enters your house and leaves a message on your fridge saying, "I was testing the security of back doors in the neighborhood and found yours unlocked. I didn't take anything, but you should fix your system!" is violating your privacy. And this is criminal - even though the intention of the incident was ostensibly good. This simple example will help us both to understand hackers' behaviour in the discussion below, and also to gain a better understanding of the difference between malicious hackers and those who claim to be honourable.



The distributed denial of service attacks on Microsoft's and Sun's websites in the 1st quarter of 2004 focused more attention on hackers' activities than any other incidents recently. Hackers spread programmes to a large number of PCs over the Internet and used them to overload the systems of those companies. (In this case a worm was used to spread itself via email to PCs connected to the Internet; on 1st February more than 50.000 unprotected PCs attacked the sites.)

Not as spectacular but with lots of criminal potential is the following example. An Italian couple hacked into the security system of two American banks and stole credit card data of nearly 1,500 clients of the bank. They used the credit cards for various purchases, and once they felt bored with living in luxury, they decided to play the 'lotto'. In one month, they purchased \$750,000-worth of tickets. The winnings of \$400,000 were directly transferred into their bank account.

Through incidents like these, hackers gain extraordinary publicity – whether or not it is desired or intended. And the public is not able to distinguish – for them, a hacker is a threat – pure and simple. Our governments are forever promising stricter laws and regulations to defend against such attacks – but they all forget that hackers' activities and efforts have brought a lot of advantages to the informational community as well.

And indeed, there does seem to be a difference between good and evil hackers. We conducted some interviews with hackers that prove this assumption. Having already categorised hackers in the typology earlier, the most important distinction is between 'hackers' and so-called 'crackers'.

Hackers have defined ethics which are respected within their community. They want to use their knowledge for good purposes. They inform about security gaps in networks and electronic communication, about vulnerabilities in e-commerce or about desiderative accuracy in the programming processes of software. The builders of the Open Source society are hackers. People including the developer of the Linux operating system - Linus Torvalds - or Richard Stallmann, founder of the Free Software Foundation, can all be considered hackers.

There is an encyclopedia of the hacker scene which is called "Jargon File". Initiated in 1975, this file is updated on a regular basis by freelance authors. The main focus is a definition of hackers - by themselves - and how they differentiate themselves from Crackers.

Eric S. Raymond is one of the most recognised experts in the context of the hacker topic, and one of the authors of the "Jargon File". He points out:

"The Jargon File contains a bunch of definitions of the term 'hacker', most having to do with technical adeptness and a delight in solving problems and overcoming limits. There is a community, a shared culture, of expert programmers and networking wizards that traces its history back through decades to the first time-sharing minicomputers and the earliest ARPAnet experiments. The members of this culture originated the term 'hacker'. Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other

people in it know who you are and call you a hacker, you're a hacker. The hacker mind-set is not confined to this software-hacker culture. There are people who apply the hacker attitude to other things, like electronics or music -- actually, you can find it at the highest levels of any science or art. Software hackers recognise these kindred spirits elsewhere and may call them "hackers" too -- and some claim that the hacker nature is really independent of the particular medium the hacker works in. There is another group of people who loudly call themselves hackers, but aren't. These are people (mainly adolescent males) who get a kick out of breaking into computers and phreaking the phone system. Real hackers call these people 'crackers' and want nothing to do with them. Real hackers mostly think crackers are lazy, irresponsible, and not very bright, and object that being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer. Unfortunately, many journalists and writers have been fooled into using the word 'hacker' to describe crackers; this irritates real hackers no end. ***The basic difference is this: hackers build things, crackers break them.*** (6)

The most important manifesto of hackerdom was drawn up by the journalist Steven Levy in his book "Hacker", published in 1984. It was the very first time that the public received deep and detailed information about these outlandish 'computer freaks', despite the fact that the hacker scene was already some 30 years old by that stage. One chapter also had a big influence on the scene itself. In this chapter he describes something new: a new way of life with a philosophy, ethics, and a dream.

Levy distilled an ideology from long discussions with old school hackers, and he terms this "hacker ethics":

1. Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-on imperative!
2. All information must be free.
3. Mistrust authority – Promote decentralisation.
4. Hackers should be judged by their hacking, not by bogus criteria such as degrees, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

(7)

So if the community *per se* is not following evil intentions, who are the people who hack into systems to damage them or for commercial purposes?

As we learned, experts and the hacker community itself distance themselves from those people who seek to cause damage and disruption. They call them crackers. Crackers are the evil hackers of the scene. The "Jargon Files" describe them as follows:

Cracker

One who breaks security on a system. Coined c.1985 by hackers in defense against journalistic misuse of 'hacker' (q.v., sense 8). An earlier attempt to establish 'worm' in this sense around 1981-82 on Usenet was largely a failure.

Use of both these neologisms reflects a strong revulsion against the theft and vandalism perpetrated by cracking rings. While it is expected that any real hacker will have done some playful cracking and knows many of the basic techniques, anyone past larval stage is expected to have outgrown the desire to do so except for immediate, benign, practical reasons (for example, if it's necessary to get around some security in order to get some work done).

Thus, there is far less overlap between hackerdom and crackerdom than the mundane reader misled by sensationalistic journalism might expect. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open poly-culture this lexicon describes; though crackers often like to describe *themselves* as hackers, most true hackers consider them a separate and lower form of life.

Ethical considerations aside, hackers figure that anyone who can't imagine a more interesting way to play with their computers than breaking into someone else's has to be pretty losing. Some other reasons crackers are looked down on are discussed in the entries on cracking and phreaking. See also samurai, dark-side hacker, and hacker ethic.

(8)

When we interviewed hackers that can truly be seen as "criminals", we often concluded that they seemed to be very destructive. Most of them couldn't answer the questions clearly – something which might correlate to their age and their lack of experience in life. It was obvious that most of their hacking takes place either simply because they are bored, or to get media attention, or to gain respect amongst their peers. The concept of 'truth' also plays a role: "I am a hacker because I want the truth. I want to know what the government knows. I want to know what they are hiding. I want to know the reason for it all." But this attitude is not the norm within the community.

Now that we know the typology of hackers and we have learned that a hacker is not necessarily a criminal, we should shift our focus to the ideology and intentions: why those 'computer freaks' behave as they do. We will talk about psychological and sociological issues, and drivers, later. A good approach to this topic is a study undertaken by Bernhardt Lieberman, a professor of sociology in Pittsburgh.

Hackers' ideology and ethics

Hackers are often portrayed as being pasty white from a lack of outside contact. They have weird hairstyles and no girlfriends, and they will bring about the end of the world, with malicious intent, through computers. Bernhardt Lieberman, professor emeritus of sociology at the University of Pittsburgh, has studied hackers for more than 10 years and finished an empiric study in August



2003. Lieberman interviewed 14 hackers in western Pennsylvania and gave them five questionnaires, ranging from one rating their attitudes toward the law, to another about their social interactions. He also attended a professional meeting of hackers, where he interviewed and questioned 28 hackers. "We have very little reliable information about the tens of thousands, perhaps hundreds of thousands, of hackers who live and work in the United States and all over the world," Lieberman said.

His findings indicate that hackers are not markedly different from anyone else - with the obvious exception that many commit crimes on a daily basis by hacking into computers. Lieberman says there are two definitions of hackers. A hacker is either someone who does "elegant programming" on computers and is considered positive in the public's eyes, or a hacker is someone who intrudes upon another's computer and is viewed as someone who does harm. From the information he gathered, Lieberman learned that they are neither as "weird" as the hackers depicted in the movie "Hackers," nor as destructive as the hacker in "War Games."

According to the responses to his "Motivation of Hackers" questionnaire, hackers' highest-rated motivations are "intellectual challenge" and to "learn about computers and computing."

Their lowest-rated motivations are "to break the law" and "to get to be known," according to the results.

The findings are contrary to the image projected by popular books and films about hackers, Lieberman said, adding that their actions are often associated, in popular thought, with the idea of having "an informal social system that is omnipotent." He comments that others stereotype hackers as possessing the ability to instigate World War III.

But if hackers' intentions are not malevolent, Lieberman said, he does believe they can cause great harm. Lieberman's study allowed hackers to speak for themselves.

"A hacker is someone who understands technology, so they can make it do anything they want it to do," one hacker is quoted as saying in Lieberman's memorandum.

Though the quote might make the hacker sound as if he is both destructive and seeking omnipotence, the questionnaire's results indicate that hackers don't generally seek power for negative results.

In the "Belief in the Hacker Ethic" questionnaire, the responses "you can create art and beauty on a computer" and "computers can change life for the better" rated as some of the most frequently chosen among the hackers.

Some discrepancy exists, however, between hackers' beliefs and what they actually do. In the ethics questionnaire, only 7 percent agreed with the statement "privacy is not important to me." Lieberman pointed out that hackers do not extend that belief to those whose computers they hack. Also, on the "attitude toward the law" scale, hackers had moderately high respect toward the law, even though they "repeatedly break the law," according to Lieberman.

Perhaps the statements that most defied the hacker stereotype were the highly-agreed-upon "I find it easy to relax with other people" and "I don't mind talking to people at parties or social gatherings."

Hackers responded to these on the "Social Anxiety and Social Avoidance" questionnaire, and these answers defy what Lieberman described as the mass media image of hackers as people "incapable of normal social interactions."



Another misconception, that hackers have "undeveloped sex lives," is not true either, Lieberman said. Many of the hackers he interviewed said they have girlfriends, and have sexual relations with them.

The idea that hackers are almost always male *does* seem to be true. Even though the hackers Lieberman interviewed varied in race and age, none were female. (9)

3.3. Self-assessment by hackers

Of course there is a discrepancy between the way hackers describe themselves and how they are perceived by the public and media. It is both interesting and worthwhile taking a closer look at their psychological, sociological and ethical environment. The "Jargon File" provides us with a closer look how "hacker XY" lives, behaves and fulfills himself:

General Appearance

Intelligent. Scruffy. Intense. Abstracted. Surprisingly for a sedentary profession, most hackers tend to be skinny rather than fat; both extremes are more common than elsewhere. Tans are rare.

Reading Habits

Omnivorous, but usually includes lots of science and science fiction. The typical hacker household might subscribe to "Analog", "Scientific American", "Whole-Earth Review", and "Smithsonian" (most hackers ignore "Wired" and other self-consciously 'cyberpunk' magazines, considering them wannabee fodder). Hackers often have a reading range that astonishes liberal arts people but tend not to talk about it as much. Many hackers spend as much of their spare time reading as the average American burns up watching TV, and often keep shelves and shelves of well-thumbed books in their homes.

Other Interests

Some hobbies are widely shared and recognised as going with the culture: science fiction, music, medievalism (in the active form practiced by the Society for Creative Anachronism and similar organisations), chess, go, backgammon, wargames, and intellectual games of all kinds. (Role-playing games such as Dungeons and Dragons used to be extremely popular among hackers but they lost a bit of their lustre as they moved into the mainstream and became heavily commercialised. More recently, "Magic: The Gathering" has been widely popular among hackers.) Logic puzzles. Ham radio. Other interests that seem to correlate less strongly but positively with hackerdom include linguistics and theatre teaching.

Education

Nearly all hackers past their teens are either college-degreed or self-educated to an equivalent level. The self-taught hacker is often considered (at least by other hackers) to be better-motivated, and may be more respected, than his school-shaped counterpart. Academic areas from which people often gravitate into hackerdom include (besides the obvious computer science and electrical engineering) physics, mathematics, linguistics, and philosophy.

Things Hackers Detest and Avoid

IBM mainframes. All the works of Microsoft. Smurfs, Ewoks, and other forms of offensive cuteness. Bureaucracies. Stupid people. Easy-listening music. Television (with occasional exceptions for cartoons, movies, and good science-fiction like the original "Star Trek" or Babylon 5). Business suits. Dishonesty. Incompetence. Boredom. COBOL. BASIC. Character-based menu interfaces.

Politics

Vaguely liberal-moderate, except for the strong libertarian contingent which rejects conventional left-right politics entirely. The only safe generalisation is that hackers tend to be rather anti-authoritarian; thus, both conventional conservatism and 'hard' leftism are rare. Hackers are far more likely than most non-hackers to either (a) be aggressively apolitical or (b) entertain peculiar or idiosyncratic political ideas and actually try to live by them day-to-day.

Gender and Ethnicity

Hackerdom is still predominantly male. However, the percentage of women is clearly higher than the low-single-digit range typical for technical professions, and female hackers are generally respected and dealt with as equals.

In the U.S., hackerdom is predominantly Caucasian with strong minorities of Jews (East Coast) and Orientals (West Coast). The Jewish contingent has exerted a particularly pervasive cultural influence.

The ethnic distribution of hackers is understood by them to be a function of which ethnic groups tend to seek and value education. Racial and ethnic prejudice is notably uncommon and tends to be met with freezing contempt.

When asked, hackers often ascribe their culture's gender- and colour-blindness to a positive effect of text-only network channels, and this is doubtless a powerful influence. Also, the ties many hackers have to AI research and SF literature may have helped them to develop an idea of personhood that is inclusive rather than exclusive -- after all, if one's imagination readily grants full human rights to future AI programmes, robots, dolphins, and extraterrestrial aliens, mere colour and gender can't seem very important any more.

Religion

Agnostic. Atheist. Non-observant Jewish. Neo-pagan. Very commonly, three or more of these are combined in the same person. Conventional faith-holding Christianity is rare though not unknown.

Even hackers who identify with a religious affiliation tend to be relaxed about it, hostile to organised religion in general and all forms of religious bigotry in particular. Many enjoy `parody' religions such as Discordianism and the Church of the Sub Genius.

Also, many hackers are influenced to varying degrees by Zen Buddhism or (less commonly) Taoism, and blend them easily with their `native' religions.

There is a definite strain of mystical, almost Gnostic sensibility that shows up even among those hackers not actively involved with neo-paganism, Discordianism, or Zen. Hacker folklore that pays homage to `wizards' and speaks of incantations and demons has too much psychological truthfulness about it to be entirely a joke.

Communication Style

Though hackers often have poor person-to-person communication skills, they are as a rule quite sensitive to nuances of language and very precise in their use of it. They are often better at writing than at speaking.

Personality Characteristics

The most obvious common `personality' characteristics of hackers are high intelligence, consuming curiosity, and facility with intellectual abstractions. Also, most hackers are `neophiles', stimulated by and appreciative of novelty (especially intellectual novelty). Most are also relatively individualistic and anti-conformist.

Although high general intelligence is common among hackers, it is not the *sine qua non* one might expect. Another trait is probably even more important: the ability to mentally absorb, retain, and reference large amounts of `meaningless' detail, trusting to later experience to give it context and meaning. A person of merely average analytical intelligence who has this trait can become an effective hacker, but a creative genius who lacks it will swiftly find himself outdistanced by people who routinely upload the contents of thick reference manuals into their brains. [During the production of the first book version of this document, for example, I learned most of the rather complex typesetting language TeX over about four working days, mainly by inhaling Knuth's 477-page manual. My editor's flabbergasted reaction to this genuinely surprised me, because years of associating with hackers have conditioned me to consider such performances routine and to be expected. -- ESR]

Contrary to stereotype, hackers are *not* usually intellectually narrow; they tend to be interested in any subject that can provide mental stimulation, and can often

discourse knowledgeably and even interestingly on any number of obscure subjects -- if you can get them to talk at all, as opposed to, say, going back to their hacking.

It is noticeable (and contrary to many outsiders' expectations) that the better a hacker is at hacking, the more likely he or she is to have outside interests at which he or she is more than merely competent.

Hackers are 'control freaks' in a way that has nothing to do with the usual coercive or authoritarian connotations of the term. In the same way that children delight in making model trains go forward and back by moving a switch, hackers love making complicated things like computers do nifty stuff for them. But it has to be *their* nifty stuff. They don't like tedium, non-determinism, or most of the fussy, boring, ill-defined little tasks that go with maintaining a normal existence. Accordingly, they tend to be careful and orderly in their intellectual lives and chaotic elsewhere. Their code will be beautiful, even if their desks are buried in 3 feet of crap.

Hackers are generally only very weakly motivated by conventional rewards such as social approval or money. They tend to be attracted by challenges and excited by interesting toys, and to judge the interest of work or other activities in terms of the challenges offered and the toys they get to play with.

In terms of Myers-Briggs and equivalent psychometric systems, hackerdom appears to concentrate the relatively rare INTJ and INTP types; that is, introverted, intuitive, and thinker types (as opposed to the extroverted-sensate personalities that predominate in the mainstream culture). ENT[JP] types are also concentrated among hackers but are in a minority.

Weaknesses of the Hacker Personality

Hackers have relatively little ability to identify emotionally with other people. This may be because hackers generally aren't much like 'other people'. Unsurprisingly, hackers also tend towards self-absorption, intellectual arrogance, and impatience with people and tasks perceived to be wasting their time.

As cynically as hackers sometimes wax about the amount of idiocy in the world, they tend by reflex to assume that everyone is as rational, 'cool', and imaginative as they consider themselves. This bias often contributes to weakness in communication skills. Hackers tend to be especially poor at confrontation and negotiation.

Because of their passionate embrace of (what they consider to be) the Right Thing, hackers can be unfortunately intolerant and bigoted on technical issues, in marked contrast to their general spirit of camaraderie and tolerance of alternative viewpoints otherwise. Old-time ITS partisans look down on the ever-growing hordes of Unix hackers; Unix aficionados despise VMS and MS-DOS; and hackers who are used to conventional command-line user interfaces loudly loathe mouse-and-menu based systems such as the Macintosh. Hackers who don't indulge in Usenet consider it a huge waste of time and bandwidth; fans of old adventure games such as ADVENT and Zork consider MUDs to be glorified chat systems devoid of atmosphere or interesting puzzles; hackers who are willing to devote endless hours to Usenet or MUDs consider IRC to be a *real* waste of time; IRCies think MUDs might be okay if

there weren't all those silly puzzles in the way. And, of course, there are the perennial holy wars -- EMACS vs. vi, big-endian vs. little-endian, RISC vs. CISC, etc., etc., etc. As in society at large, the intensity and duration of these debates is usually inversely proportional to the number of objective, factual arguments available to buttress any position.

As a result of all the above traits, many hackers have difficulty maintaining stable relationships. At worst, they can produce the classic computer geek: withdrawn, relationally-incompetent, sexually frustrated, and desperately unhappy when not submerged in his or her craft. Fortunately, this extreme is far less common than mainstream folklore paints it -- but almost all hackers will recognise something of themselves in the unflattering paragraphs above.

Hackers are often monumentally disorganised and sloppy about dealing with the physical world. Bills don't get paid on time, clutter piles up to incredible heights in homes and offices, and minor maintenance tasks get deferred indefinitely.

1994-95's fad behavioural disease was a syndrome called Attention Deficit Disorder (ADD), supposedly characterised by (among other things) a combination of short attention span with an ability to 'hyper-focus' imaginatively on interesting tasks. In 1998-1999 another syndrome that is said to overlap with many hacker traits entered popular awareness: Asperger's syndrome (AS). This disorder is also sometimes called 'high-function autism', though researchers are divided on whether AS is in fact a mild form of autism or a distinct syndrome with a different etiology. AS patients exhibit mild to severe deficits in interpreting facial and body-language cues and in modeling or empathising with others' emotions. Though some AS patients exhibit mild retardation, others compensate for their deficits with high intelligence and analytical ability, and frequently seek out technical fields where problem-solving abilities are at a premium and people skills are relatively unimportant. Both syndromes are thought to relate to abnormalities in neurotransmitter chemistry, especially the brain's processing of serotonin.

Many hackers have noticed that mainstream culture has shown a tendency to pathologise and medicalise normal variations in personality, especially those variations that make life more complicated for authority figures and conformists. Thus, hackers aware of the issue tend to be among those questioning whether ADD and AS actually exist; and if so whether they are really 'diseases' rather than extremes of a normal genetic variation like having freckles or being able to taste DPT. In either case, they have a sneaking tendency to wonder if these syndromes are over-diagnosed and over-treated. After all, people in authority will always be inconvenienced by schoolchildren or workers or citizens who are prickly, intelligent individualists - thus, any social system that depends on authority relationships will tend to helpfully ostracise and therapise and drug such 'abnormal' people until they are properly docile and stupid and 'well-socialised'.

So hackers tend to believe they have good reason for skepticism about clinical explanations of the hacker personality. That being said, most would also concede that some hacker traits coincide with indicators for ADD and AS. It is probably true that boosters of both would find a rather higher rate of clinical ADD among hackers

than the supposedly mainstream-normal 10% (AS is rarer and there are not yet good estimates of incidence as of 2000).

Miscellaneous

Hackers are more likely to have cats than dogs (in fact, it is widely suggested that cats have the hacker nature). Many drive incredibly decrepit heaps and forget to wash them; richer ones drive spiffy Porsches and RX-7s and then forget to have them washed. Almost all hackers have terribly bad handwriting, and often fall into the habit of block-printing everything like junior draftsmen. (8)

Hacking is about respect and reputation

Having looked behind the curtain, we might be tempted to believe that hackers are very altruistic, do serve the environment and are socially engaged. However this is as likely to be the case as the opposing theory that all hackers are criminals. The truth, of course, lies somewhere in-between. We will get a better understanding in the next chapter. But before discussing the psychological and sociological drivers, we might ask once more: What do hackers do it all for?

The answer is: for reputation, respect and acknowledgement.

Like most cultures without a money-based economy, hackerdom runs on reputation. Hackers try to solve interesting problems, but how interesting they are - and whether their solutions are really good - is something that only technical peers or superiors are normally equipped to judge. Accordingly, when hackers play the hacker game, they learn to keep score primarily by what other hackers think of their skill (this is why they aren't really a hacker until other hackers consistently call them one). This fact is obscured by the image of hacking as solitary work; and further by a cultural taboo amongst hackers that forbids admitting that ego or external validation are involved in one's motivation in any way.

Specifically, hackerdom is what anthropologists call a *gift culture*. Hackers gain status and reputation in it not by dominating other people, nor by being beautiful, nor by having things that other people want, but rather by giving things away. Specifically, by giving away time, creativity, and the results of their particular skill.

Eric S. Raymond describes five types of things hackers can do to gain respect from other hackers:

1. Write open-source software

The first (the most central and most traditional) is to write programmes that other hackers think are fun or useful, and give the programme sources to the hacker community as a whole to use.



(We used to call this “free software”, but this confused too many people who weren’t sure exactly what “free” was supposed to mean. Many of us now prefer the term “open-source” software.)

Hackerdom’s most revered demigods are people who have written large, capable programmes that met a widespread need, and given them away - so that now everyone uses them.

2. Help test and debug open-source software

They also serve who stand and debug open-source software. In this imperfect world, we inevitably spend most of our software development time in the debugging phase. That’s why any open-source author who’s thinking will tell you that good beta-testers (who know how to describe symptoms clearly; localise problems well; can tolerate bugs in a quickie release; and are willing to apply a few simple diagnostic routines) are worth their weight in rubies. Even one such person can make the difference between a debugging phase that is a protracted, exhausting nightmare and one that’s merely a salutary nuisance.

If you’re a newbie (new into the hacker-scene), try to find a programme under development that you’re interested in and be a good beta-tester. There’s a natural progression from helping with test programmes to helping debug them to helping modify them. You’ll learn a lot this way, and generate good karma with people who will help you later on.

3. Publish useful information

Another good thing is to collect and filter useful and interesting information into Web pages or documents like FAQs (Frequently Asked Questions lists), and make those generally available.

Maintainers of major technical FAQs get almost as much respect as open-source authors.

4. Help keep the infrastructure working

The hacker culture (and the engineering development of the Internet, for that matter) is run by volunteers. There’s a lot of necessary but unglamorous work that needs to be done to keep it going -- administering mailing lists, moderating newsgroups, maintaining large software archive sites, developing RFCs and other technical standards.

People who do this sort of thing well get a lot of respect, because everybody knows these jobs are huge time sinks and not as much fun as playing with code. Doing them shows dedication.

5. Serve the hacker culture itself

Finally, you can serve and propagate the culture itself. This is not something you'll be positioned to do until you've been around for while and become well-known for one of the first four things.

The hacker culture doesn't have leaders, exactly, but it does have cultural heroes and tribal elders and historians and spokespeople. When you've been in the trenches long enough, you may grow into one of these. Beware: hackers distrust blatant ego in their tribal elders, so visibly reaching for this kind of fame is dangerous. Rather than striving for it, you have to sort of position yourself so it drops in your lap, and then be modest and gracious about your status.

(10)

In his highly recognised essay "Homesteading the Noosphere", Raymond adds the following thoughts about reputation and respect in the hacker community:

One's reputation can suffer unfairly if someone else misappropriates or mangles one's work ... taboos (and related customs) attempt to prevent this from happening. (Or, to put it more pragmatically, hackers generally refrain from forking or rogue-patching others' projects in order to be able to deny legitimacy to the same behaviour if practiced against themselves.)

- Forking projects is bad because it exposes pre-fork contributors to a reputation risk they can only control by being active in both child projects simultaneously after the fork. (This would generally be too confusing or difficult to be practical.)

- Distributing rogue patches (or, much worse, rogue binaries) exposes the owners to an unfair reputation risk. Even if the official code is perfect, the owners will catch flak from bugs in the patches .

- Surreptitiously filing someone's name off a project is, in cultural context, one of the ultimate crimes. Doing this steals the victim's gift to be presented as the thief's own.

(11)

3.4. Psychological and sociological drivers

Reputation incentives continue to operate whether or not a craftsman is aware of them; thus, ultimately, whether or not a hacker understands his own behaviour as part of the reputation game, his behaviour will be shaped by that game.

The rewards of peer-esteem and the pure joy of hacking were – for some respondents – at levels above subsistence needs in Abraham Maslow’s well-known ‘hierarchy of values’ model of human motivation.

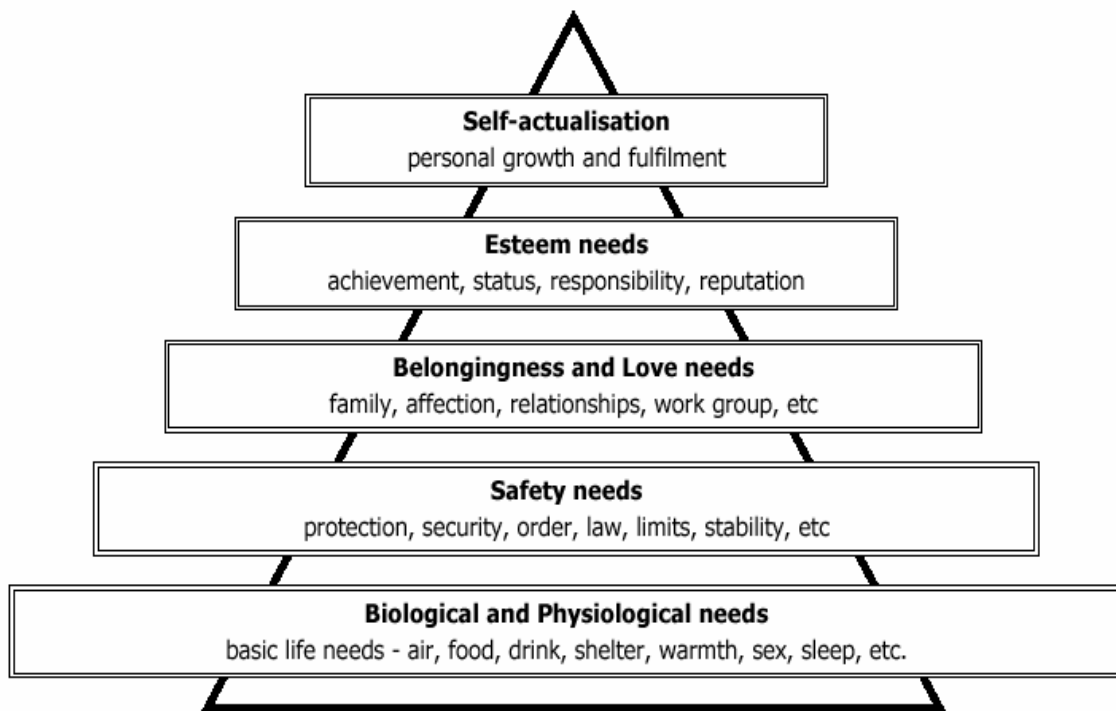


Figure 2 Maslow’s Hierarchy of Needs

Abraham Maslow developed the Hierarchy of Needs model in 1940-50’s USA. The model remains valid today for understanding human motivation. Each of us is motivated by needs. Our most basic needs are with us from birth, having evolved over tens of thousands of years. Maslow’s Hierarchy of Needs helps to explain how these needs motivate us all. It states that we must satisfy each need in turn, starting with the first, which deals with the most obvious needs for survival itself.

Only when the lower-order needs of physical and emotional well-being are satisfied are we concerned with the higher-order needs of influence and personal development.

Conversely, if the things that satisfy our lower-order needs are swept away, we are no longer concerned about the maintenance of our higher-order needs.

In this context, the joy of hacking fulfills a self-actualisation or transcendence need, which will not be consistently expressed until lower-level needs (including those for physical security and for 'belonging' or peer-esteem) have been at least minimally satisfied. Thus, the reputation game may be critical in providing a social context within which the joy of hacking can in fact *become* the individual's primary motive.

There are reasons common to every gift culture as to why repute amongst peers (prestige) is worth playing for:

Firstly, and most obvious, good reputation among one's peers is a primary reward. We're wired to experience it that way for evolutionary reasons touched on earlier. (Many people learn to redirect their drive for prestige into various sublimations that have no obvious connection to a visible peer group, such as "honour", "ethical integrity", "piety" etc.; this does not change the underlying mechanism.)

Secondly, prestige is a good way (and in a pure gift economy, the *only* way) to attract attention and cooperation from others. If one is well-known for generosity, intelligence, fair dealing, leadership ability, or other good qualities, it becomes much easier to persuade other people that they will gain from association with you.

Another interesting example of this phenomenon was observed when discussing the reputation-game analysis with hackers. Many hackers resisted the analysis and showed a strong reluctance to admit that their behaviour was motivated by a desire for peer repute or, as Raymond labeled it at the time, 'ego satisfaction'.

This illustrates an interesting point about the hacker culture. It consciously distrusts and despises egotism and ego-based motivations; self-promotion tends to be mercilessly criticised, even when the community might appear to have something to gain from it. So much so, in fact, that the culture's 'big men' and tribal elders are required to talk softly and with humorous self-deprecation at every turn in order to maintain their status.

Only sublimated and disguised forms such as "peer repute", "self-esteem", "professionalism" or "pride of accomplishment" are generally acceptable.

Finally, the reputation-game analysis explains the oft-cited dictum that you do not become a hacker by calling yourself a hacker - you become a hacker when *other hackers* call you a hacker. A 'hacker', considered in this light, is somebody who has shown (by contributing gifts) that he or she both has technical ability and understands how the reputation game works. This judgment is mostly one of awareness and acculturation, and can be delivered only by those already well inside the culture. **(11)**

In order to understand the criminal behaviour of hackers, it is necessary to examine the traditional psychological theories of criminal behaviour and how they may be applied to develop an understanding of hacking.

Major Psychological Theories of Crime

The following remarks are based on the study “Psychological Theories of Crime and Hacking” by Marc Rogers from the University of Manitoba. His thoughts have generated much controversy and discussion. Nevertheless he has attempted to assess psychological theories in crime and see how these may be applied to hackers.

The major psychological theories of crime can be categorised into the following areas: psychoanalytic theory, learning theory, and control theory. Dominant theories within each of these categories will be briefly reviewed. The major psychological theories of crime have been influenced to some extent by other fields (i.e. criminology, sociology, & biology). Criminology may have had the largest effect on the development of behavioural theories of crime. As such it is important to briefly review the two predominant schools of thought in criminology, classical, and positivist theory. The classical theorists hold central the concept that man is capable of free will. Crime can be explained in terms of choices between criminal behaviour (if the opportunity arose) or non-criminal behaviour. If the rewards for a criminal act are greater than the retribution, the probability of criminal behaviour increases.

The positivist theorists believe that the causes of criminal behaviour are outside the realm of free will and are influenced by other factors. The factors range from the *biological (genetics)*, to the *sociological (environment)* and to the *psychological (personality, learning, etc.)*. It has been argued that psychological theories are positivist in nature as they all seek to account for criminal behaviour by way of factors outside of the individual's control.

If the consequences of a person engaging in criminal activity were rewarding (i.e. increase in prestige, money, or feelings of adequacy) the person is likely to engage in further criminal activity. If the consequences were negative (i.e. being arrested, shunned, etc.) the frequency of future criminal behaviour should be reduced.

Criminal behaviour is acquired through observational learning. The learning takes place in three contexts, the family, prevalent subculture, and the social environment. The reinforcement for criminal behaviour comes from both the internal and external sources. The reinforcement can be in the form of tangible rewards of the criminal activity itself (i.e. money), or from social rewards (i.e. increase in peer status). Criminal behaviour is maintained through a complex schedule of reinforcement and punishment throughout the life of the individual.

The term hacker doesn't refer to a single homogeneous group. The limited empirical research into this behaviour indicates that there are various sub-groups (communities). These subgroups can be ordered from novices up to professional criminals. The subgroup the hacker would be classified as depends on the motives and causes behind the behaviour. At best some of the traditional theories reviewed

can only be applied to a limited portion of the theorised hacker subgroups. The psychoanalytic theories concentrate mainly on unconscious factors and the child-parent interactions. Although several of the more infamous hackers have come from dysfunctional families, this is not sufficient to explain their choice of the criminal activity to engage in. Psychoanalytic theories are not adequate at explaining criminal behaviour that is planned out. Hacking is such an activity, as it requires a specific skill set, familiarity with computers, networks and a relatively advanced technological understanding. To be successful at hacking the individual also has to plan the attack in some detail. The attacks are deliberate and the victim system or networks are usually pre-chosen and not random.

The success of control theory in explaining hacking is mixed. The majority of the arrested hackers and those which have responded to surveys, indicate they are withdrawn, uncomfortable with other people and are introverts.

Moral development theory may be more useful in understanding a subset of hackers. One of the pre-morality stages is hedonism. There have been many documented anecdotal accounts of the lack of concern by hackers over the systems they have attacked. Many of the written interviews with convicted hackers portray them as being more concerned with fulfilling their own material needs regardless of the consequences.

Hackers tend to associate with other individuals who also engage in hacking behaviour. These associations can take the form of purely electronic, as in online chat sessions, or more intimately by joining a hacking club (e.g., Cult of the Dead Cow CDC, Legion of Doom). The hackers even hold conventions such as the recent Defcon in Las Vegas, where they share ideas, techniques, and intelligence information.

It is also evident that the hackers are learning their respective criminal behaviour, and are doing so amongst individuals who hold positive attitudes toward such behaviour. The continuation of hacking may be due to several reinforcing factors. The reinforcement derived from hacking may come from the increase in knowledge, prestige within the hacking community, or the successful completion of the puzzle (some hackers indicate that to them attacking a system is a type of game). In some rare cases prestigious companies have hired hackers who have penetrated their systems. This has led to the large-scale myth that hackers can “land” good jobs in the computer security industry. Such a myth can definitely be seen as reinforcing.

Other reinforcing aspects of hacking include the fact that the media is enamoured with the romantic notion of hackers, and is turning some into celebrities.

(12)

Sociological Motivation

Being a hacker can be associated with having a flexible world-view about stress, time management, work, and play. A hacker tries to harmonise the rhythm of their creative work with the rhythm of the rest of their life, so that play and work become one and the same. It's a

fundamentally new work ethic. True hackers are willing to work at something in order to improve it and are not always motivated to do so by the almighty dollar. They will come into work at 10 or 11 am and stay until almost midnight every day in order to tinker with and ultimately complete a project.

Hackers, like IT professionals in general, are task-oriented rather than time-oriented. Leisure, hobby and professional accomplishment are all merged together in their mindset. They sleep during the day, and hack at night, not only because they are naturally nocturnal, but because there are less distractions at night. They survive on Twinkies and Jolt Cola with "Food, Sleep, Code" as their mantra. The sociological conception of a hacker resembles the occupation of a mathematician, or a mechanic who likes to tinker with automobiles. The difference, however, is that at the centre of the hacker ethic is a belief in information-sharing and that everything ought to be free. It is held as a duty to share interesting information with like-minded people. The hacker ethic is a counterforce to the market culture. Hackers are not motivated by money, but by enthusiasm, joy and passion. Their working times are individualised and optimised, and they don't respect hierarchies and rules from above. Sociologists have a lot more to say about our changing cultural attitudes toward time and work, as the website called 'The Sociology of Cyberspace' illustrates.

3.5. Methodology

According to Marc Rogers, hacking consists of three fundamental approaches:

1. social engineering
2. brute force
3. technical intrusions

Social engineering is the process of posing as a network administrator over the phone and getting good-natured employees to give out passwords or sensitive information. Brute force is the use of common point-and-click tools to identify targets and attack them. Technical intrusions exploit deficiencies in system design, configuration, or management.

Most attacks are based around one of five basic problem areas:

1. inherent security defects
2. misuse of legitimate tools
3. improper maintenance
4. ineffective security
5. inadequate detection systems

Inherent Security Defects are built-in vulnerabilities which are common in software development. Vendors prefer to prioritise getting their product to market, and to rely on patches to fix any bugs at a later stage; some even post source code so developers can make their own patches. Not only are many new products full of holes, but any old product that has not been kept current with the latest patches is vulnerable. However, there are certain common areas that, by design, always seem to need a fix. In general, these include Network Open Shares, any Password system (which can always be cracked), any Remote Login service, some Protocols (like IMAP = Internet Message Access Protocol, or ICMP = Internet Control Message Protocol), and some Utilities (like PING =



Packet Internet Groper). IMAP and POP3 implementations need to run on root in UNIX, so it is fairly easy to obtain 'super-user' privileges on UNIX systems by email. PING is a type of ICMP that is frequently used in Smurf attacks to buffer overflow the system. Windows systems are especially vulnerable to buffer overflows in the space between systems and applications where Windows-compatible applications "talk" with the operating system. Most users see this as a Windows error messages, but sophisticated hackers see it as an opportunity to gain administrator access (while the overflow is on the stack and attempting execution) on distributed systems.

Misuse of legitimate tools is quite the opposite problem. Some software comes shipped with advanced utilities that only network administrators are supposed to use or know about. Almost any piece of server software comes with a Portscan utility which administrators as well as hackers can use to scan for open ports. UNIX utilities work on almost every system. NT software comes with the *nbstat* command, which can be misused by hackers to identify IIS subdomains and users. Other diagnostic tools, such as packet sniffers, are provided out of the box or easily downloaded. Running a packet sniffer for only a short time will record all traffic as it crosses a network interface card. (Passwords are sent in clear text via the network!)

Improper maintenance is a problem area that applies mainly to routers, proxies, and firewalls. These items need frequent maintenance and upgrades, which are often forsaken by administrators because of complexity and cost. Risk assessments are almost never done, and setting up proxy/firewall policies for what is filtered in and filtered out is a full-time job. Even the period after an upgrade may be the most vulnerable time because it mixes old and new vulnerabilities in new ways with these devices. Changing standard passwords on all network devices should be the first job done by administrators.

Ineffective security is a problem in much the same way -- no security policies in place, or security managers new to a certain kind of configuration. Even when firewall rules are appropriately set, applications that are not architected or layered properly put the whole network at risk. CGI-Bin services, for example, are frequently requested by users, but CGI scripts present an easy avenue for attack and compromise, such as modification of Web server content. CGI stands for Common Gateway Interface and consists of PERL scripts which allow dynamic page content including counters and forms.

Inadequate Intrusion Detection is a final problem area. Most organisations unfortunately rely on audit trails or isolated tools to detect attacks. These are obsolete security safeguards in today's world, and do little to actively prevent the creation of backdoors, trojans, and logic bombs.

(13)

Among the most common methods offensives are the distribution of viruses and Trojan horses, Denial of Service attacks, social engineering and identity theft. There are four elementary steps in almost every hacker incident:

1. Chasing information (also called "casing"): Casing (as in "casing the joint") is the process of target acquisition and information gathering. It is also called "footprinting" and involves the

systematic profiling of an organisation's Internet presence and network security. The hacker is essentially probing or mapping out the target for attack. While each hacker is different in how they go about this stage, there are some common items that are probed for.

<i>Items Probed for in Stage One of Hacking</i>	
Internet	Domain name, Network Blocks, Reachable IP addresses, TCP and UDP services, System architecture, Access Control lists, Intrusion Detection systems, Workgroup names, Routing tables
Intranet	Internal Domain names, Networking Protocols, Blocks, Addresses, TCP and UDP services, Architecture, Access Control lists, IDS, Workgroups
Remote Access	Remote system type, Authentication scheme, Telephone numbers
Extranet	Pipeline and Backbone connection, Type of connection, Access control

Much of this information is Open Source. Organisations often put a ridiculous amount of information on their Web servers that can assist hackers, and a few even openly display the security configurations of their firewalls.

2. Scanning security 'holes': Scanning (as in scanning for open ports) is the process of more actively probing or sweeping the organisation's resources. Whereas the hacker may have been in stealth-mode during stage one, this stage exposes them to the risk of detection, and is sometimes called "door-rattling". Also, whereas stage one typically involves the sequential use of separate tools, stage two typically involves the use of packages that provide several tools in one, such as Cheops, which combines ping, traceroute, port scanning, and operating system detection. Port scanning is a common stage two activity that is engaged in if ICMP traffic is blocked. It is perhaps the most popular hacker activity because of the challenge involved in getting past a firewall. It is defined as the process of establishing a connection between two computers to find out what services are in 'listening' mode. This is a handshaking mode (different to open mode) that tells you what upper dynamic or private ports have been reserved by the interface between whatever operating system and applications are being used. There are as many different objectives of port scans as there are hackers, but the general objective is to map out (as in a system audit) each user's operating system (including versions, upgrades, and patches) and specific applications installed (including versions and upgrades). A computer is literally an open book after a port scan because not only does the hacker know if your operating system is vulnerable, but they know which applications you use that are vulnerable. Port scans are mostly intrusive, although a couple of programmes use what is called *banner grabbing* to operate in stealth mode.

3. Enumeration: Enumeration is the process of identifying valid user accounts or poorly-protected resource shares. This kind of hacking activity should always show up in the logs as it involves active connections and directed queries. More sophisticated hackers will cover their tracks, however, by modifying the log-files and any record of their visit. When a hacker discovers a valid user account, it is only a matter of time before they know the password (by using a *brute force*

technique or other method). When a hacker discovers network workgroups or user groups, this is what is meant by resource shares.

4. Covering the tracks: Of course it is necessary for every intruder to clear the logs after hacking into a system. This issue is often neglected by so-called Newbies, who don't know if and how their tracks can be traced.

After the analysis of the ideology, ethics and motivations of hackers, we would like to present a piece of empiric research about a recent incident, in which hundreds of people misused identities.

3.6. A study by the German BKA (Bundeskriminalamt)

On April 14th 1999 an Internet provider based in the area of Münster (Germany) commenced operations. However due to technical and organisational problems, the enterprise was not able to charge royalties for the first time until September of that year. When a number of customers complained about invoices being too high, a quick check of the connection information aroused suspicions that:

- the access data of numerous customers had been hacked
- this access data had been misused
- the data had then been changed
- users had gained access with fake identities

The provider recommended to its customers that they should report this to the police. According to the provider's terms and conditions, the customers were obliged to pay even in the case of account misuse. From the point of view of the enterprise the customers were victims of these punishable acts.

The ever-increasing requests for information and legal proceedings from across the whole country enabled the provider and the police establish connections between:

- fake accounts (fraudulently created using fake identities)
- misused accounts (misuse of genuine customer accounts)
- access data published on Web sites
- signs that hackers had gained the data using so-called "trojan horses"

Further, it was discovered that numerous alleged criminals were using several customer accounts. The alleged criminals were using a dial-up phone number that is valid across the country. With this they built a telephone connection to one of the enterprise's dial-up servers. After the input of valid access data, consisting of the customer number and a password, the system enabled a connection to the Internet. The access data employed by these alleged criminals was either:

- genuine customer data which they had stolen themselves in the past
- and / or genuine customer data which had been stolen by other people and published on the Internet
- and / or fake customer data which they had entered themselves
- and / or fake customer data previously published on the Internet by others

The connection with the Internet was mainly used to surf the Internet at the expense of others. In many cases the connections may also have been used in order to collect additional data, e.g. with the help of so-called Trojan programmes. What's more, the alleged criminals would often change the passwords of the Internet accounts they had abused so that the rightful owners would no longer be able to gain access.

According to the final calculations, the connection costs caused by misuse of the individual accounts came to roughly €1.5 million. The provider reported a total loss of €4.5 million, and individual customers were left up to €12,000 out of pocket.

By analysing all available data the police committee was able to identify more than 3,600 suspects; preliminary proceedings were then instigated against them.

Some of the alleged criminals had hacked the data used by their targets to access their Internet provider. As far as is known, "Trojan horses" - programmes that broadcast every keystroke made on an affected computer back to the originator - were employed. The data that was collected, e.g. account access authorisations in the form of user names and appropriate passwords, was published on pertinent Web sites where Internet hacks and cracked passwords can commonly be found (fakeZ Web sites, "hacker" sites). Users of those pages could use these accounts to log on to the Internet via the affected provider with a stolen identification and the appropriate password. The user whose account had been hacked and then misused was subsequently charged for the costs of this Internet session.

The study

In this context, the German Federal Bureau of Criminal Investigation (Bundeskriminalamt, BKA) decided to conduct an educational study about this incident. All the people involved - namely those who had misused the identities of other people – received a questionnaire. The BKA wanted to gain a better understanding of the behaviour, social background and intentions of the intruders.

Altogether, 663 questionnaires were sent back to the BKA by the offices working on the topic. 64 questionnaires contained virtually no information, several suspects having exercised their right to refuse to give evidence (according to the police headquarters in Münster this followed advice from the suspects' lawyers).

However 599 questionnaires were analysable – at least in part. For the purposes of the analysis some of the criteria were restructured, re-categorised and summed-up in groups.

The focus was on the following discriminating variables:

- gender of the alleged criminal
- age of the alleged criminal
- circumstances in the alleged criminal's life/background
- placement of a "Trojan horse"
- intention of the alleged criminal
- whether the alleged criminal knew that his/her crime could be traced

The gender variable is still a fairly conspicuous variable in the context of Internet crime, presumably because the number of women interested in the field of computers is significantly smaller than the number of men.

At a sample of N=599 only 35 cases were assigned to women. However those 35 female alleged criminals differed considerably from the male alleged criminals in certain areas. The differences in the following variables were statistically significant:

- On average, the female alleged criminals were considerably older than the male alleged criminals. The men averaged 22.2 years old, the women 34.7. The average deflection (standard deflection) regarding women was more than 12 years.
- Of course, the above has a natural impact on the findings regarding the suspects' social situations. The comparatively much older females were generally not living with their parents anymore.
- The speed of the computers used to commit the crimes also varied. The male alleged criminals tended to own up-to-date computers, with their female counterparts using rather older machines.
- The periphery items possessed by the suspects revealed significant differences as well. The female alleged criminals spent roughly half as much on periphery items as the men – and the same applies for the costs of upgrades.
- The female alleged criminals only used approximately half the number of hacked accounts as the males (on average 6.8 for the females, 14.1 for the males)
- The motivations of the females were centred mainly on "trial and error" or economic reasons.
- Only two women (~ 5%) acknowledged that they were aware they were committing a criminal act [compared to 179 of the male alleged criminals (~ 32%)].
- However, when respondents were asked if they knew whether their activities could be traced, there was no statistically-significant difference between men and women.

Regarding the age and the circumstances of the alleged criminals, the following results are eye-catching:

- The average age pattern diverges from the classical "teenager". On average, the offenders were approximately 23 years old.
- The '16-21' age group was represented most frequently.

- It is conspicuous that a total of 72.2 per cent of the alleged criminals lived with their parents while the crimes were committed.

However, it would be wrong to presume that the age of consent (18 years old) causes a definitive change in moral conduct and behaviour. This period in our lives is often the signal for other factors to enter the reckoning, each of which may carry their own natural consequences on what we do and how we live. These could include: the advent of financial autonomy; change in academic environment; related interactions with friends and colleagues; time-management; employment; relocation to a new area.

Some differences of note:

- the older alleged criminals have more experience with computers
- the older alleged criminals have much more money to spend (€387 on average, compared to €129 for the younger alleged criminals)
- the older alleged criminals had spent considerably more money on upgrades since the crime had been committed
- the younger alleged criminals used considerably more hacked accounts (an average of 15.7 accounts compared to 7.6 for the older groups)

When examining the amount of financial damage inflicted on the victims, it was the older criminals who – surprisingly – achieved the most, although the difference was not significant (an average of €429 compared to €382 by the younger offenders).

Research into the motivation of the offenders is also interesting. Of 301 cases where economic reasons were stated as the motivation, a sizeable majority (251) were aged under 22.

"Trial and error" seems to be more common with younger groups as well. From 192 alleged criminals that quoted this option, 151 were under 22 years old – a huge 79.7%.

Summary of the results concerning the age of the offender

Life-circumstances change dramatically after the age of 21. This also impacts behaviour in the field of crime. Older alleged criminals have more experience, presumably because they have had more time to work with the computer than their younger counterparts. Older alleged criminals also have more money to spend because they earn money themselves. This is often spent on computer upgrades.

The question concerning motives showed that younger hackers were primarily interested in economic gain, and they had used more of the hacked-identities in order to achieve this.

Usage of Trojan Horses

Unfortunately, the question as to whether the alleged criminals used "Trojan horses" ultimately proved fruitless. The hypothesis behind the question is that such a group may have a higher criminal potential, but this hypothesis could not be certified.

The group that used "Trojans" comprised just six people – two of which submitted minimal data (presumably this was a refusal to give evidence). Calculations to establish if this group differed from those that did not use "Trojans" did not reveal any significant differences that would characterise the group in the analysed variables.

Moreover, the small group of "Trojan horse" users was fairly heterogeneous and spread over the whole country. It was presumably *not* a homogenous group of offenders disposed – and with access – to regular face-to-face contact amongst one another.

The question remains as to whether informational connections were built up via 'chats' and if experiences were circulated. 'Chats' are conversations over the Internet on specialised topics in specialised conversation rooms (so-called "chat rooms"). Such informational exchange cannot be excluded from this group of offenders because they stated chat rooms as mediums. But this does not mean that those involved knew one another as individuals in the conventional sense, as in chat rooms *aliases* are commonly used instead of real names.

Four members of this group stated that they did not publish account details on the Internet. For two people there was no data available. This means that the alleged criminals who did publish details on the Internet are either not represented in the sample, or can be drawn from one or both of the two people about whom no data is available. An alternative explanation, of course, could be that one or more people did not tell the truth. The question of intent was evenly distributed among these alleged criminals. Half of them knew the act was punishable, half of them did not.

The question of 'tracing' revealed a surprising lack-of-awareness amongst these alleged criminals. Only one person knew that the activities could be tracked. If one presumes that the use of "Trojans" would require a considerable amount of computer knowledge, one could naturally expect that this group of offenders in particular would have known better about the conventional logging opportunities. This presumption is obviously wrong.

The alleged criminals who used "Trojans" mostly stated economic reasons as their motivation for the crimes, in common with the other groups:

The motivations were distributed as follows:

Motivation	Cases	in %
economic reasons	307	51.3
trial and error	198	33.1
technical opportunities	72	12
other reasons	49	8.2
fooling around	16	2.7
acceptance of the group	9	1.5
competition	6	1
acceptance on the Internet	4	0.7
intelligence service	2	0.3
spying on someone	n/a	0
harming someone	n/a	0

Summary regarding the motivations of the alleged criminals

The key motive reported was "economic reasons" – or enrichment – and even in combination this was the most frequently cited cause as well.

"Trial and error" was an important motive for beginners at first. However, in the combination "trial and error and economic reasons", the shortage of money played the more important role.

The analysis became even more interesting when the "economic reasons" motive was subdivided into two alternative groups ("yes" or "no") and the resulting average damage costs were compared: The cost of damage was reduced by more than 50% in the group not motivated by financial gain - a significant finding. On the other hand both groups hacked into very similar numbers of accounts.

The alleged criminals' intentions – and their awareness of being traced

Information about intent - combined with insight into whether the suspects knew that their actions could be traced - are available in one sub-group (N=472). If this sub-group is kept in mind it becomes clear that a total of 230 alleged criminals neither knew that their actions could be retraced nor that what they were doing was punishable (48.7 per cent of this sub-group).

76 people, on the other hand, knew that their activities could be retraced and also knew that they were committing a punishable offence (16.1 per cent).

103 people knew that they were committing an offence but did not know about the possibility of being traced (21.8 per cent).

Finally, 63 people knew that their actions could be retraced but did not understand that they were guilty of an offence.

If the typical offender-group (male and under 22 years old; N=373) is considered in isolation here, the distribution looks very similar. There are no significant differences to the total sample.

Distinction between different types of alleged criminals

Splitting out the alleged criminals in two dimensions makes sense: subdivision by gender and by age. Age is divided into "under 22 years" and "over 22 years" due to the different circumstances of life.

Amongst the female alleged criminals there were no significant differences between those who still lived with their parents and those who stood on their own feet. The group consisted of 35 people. The relevant criteria distinguishing this group have been explained earlier.

Amongst the male alleged criminals there were significant differences.

On question V8 - "What are the alleged criminals engaged in above all?" - the groups [male over 22 years old and male under 22 years] differ considerably. This can also be explained by the different lifestyles:

- 18 per cent of the younger alleged criminals did team sports, compared with only 7 per cent of the older ones
- 36 per cent of the younger alleged criminals met in cliques; just 9 per cent of the older ones did likewise
- 35 per cent of the younger alleged criminals enjoyed TV, video and music; this compares with only 17 per cent of the older ones

There were no significant differences elsewhere in responses to question V8. By distinguishing between age and gender the following typical profile of the offender can be collated:

The typical offenders (N=373)

- gender: male
- age: between 16 and 21 years
- lives with his parents
- motivation: financial gain or curiosity (trial and error)
- has a middle or higher education
- has medium-to-high knowledge of computers
- is a student or trainee
- got his computer knowledge as an autodidact
- uses the computer in his spare time
- often meets in cliques or busies himself with TV, videos and music
- caused an average €388-worth of damage
- chat rooms may have brought his attention to this possibility of committing an offence (other alternatives: friends or Web sites)

There is not a great difference in examining whether the alleged criminals knew they were committing a punishable act [43.9% were aware, 56.1% were not]. However more than 70% of the alleged criminals believed such methods could not be traced.

This group of typical offenders has a few idiosyncrasies which do not simplify the accessibility for media campaigns:

Intra-group contact was very much *ad hoc* and informal, and not founded in any form of solid integration in social structures. Social contact often took place via chat rooms, cliques or amongst individual friends – and, for very few, via associations (e.g. only a small number are active in the field of sports). So the group of offenders has to be regarded as high individualised.

The atypical offenders

A comparatively atypical profile can be found in the group of males who are over 22 years old. In this group the characteristics of the single variables follow no perceivable pattern. This seems to be logical as the bandwidth of possibilities for different lifestyles considerably enlarges with increasing age, as therefore do one's commitments, circumstances and thinking.

Female offenders

The female alleged criminals make up their own, distinct group, differing from the other two types in several of the variables. Indeed, the female alleged criminals were a fairly homogeneous group. In this segment hardly any differences were found between the age-groups.

Where did the offenders get their information?

- 40% of the total sample with available data got their information from FakeZ Web sites. (N=185)
- 37.4% of this sample got their information from communicating in chat rooms.
- 14.5% got their information from personal contacts.

The remaining options (totaling 7.2%) are statistically irrelevant.

If this group is divided into the single groups "Female", "Male over 22" and "Male under 22" the following is revealed:

Female (N=17):

- FakeZ Web sites: 17.6%
- personal contacts: 23.5%
- chat rooms: 47.1%

Male over 22 years (N=87):

- FakeZ Web sites: 46%
- personal contacts: 13.8%
- chat rooms: 29.9%

Male under 22 years (N=342)

- FakeZ Web sites: 38.6%
- personal contacts: 14.0%
- chat rooms: 39.8%

It is evident that chat rooms were used most frequently by the younger male and the female alleged criminals to gain their information. The older alleged criminals informed themselves instead via the FakeZ Web sites. Personal contacts were also relevant for female alleged criminals.

As a starting point for the prevention of further offences in this field of crime, the technical possibilities of being traced and the possible momentous criminal proceedings that would follow should be spelt out to the main group (male under 22 years).

As most of the alleged criminals obtain their information about the possibilities of misusing third party accounts via chat rooms, the opportunity to use this medium as an educational forum should be explored.

As an extension to this, FakeZ Web sites should also be considered for educational campaigns, as this medium is also used regularly to find the necessary information.

Summary

It is interesting that the "circumstances of life" variable explains a considerable part of the variance in this field of crime. On the other hand, the gender variable was a classical discrimination variable; other studies have already proved that female alleged criminals behave differently and show other preferences.

Due to these mere variables it was possible to create a 'typical profile' which exceeded all expectations.

And, contrary to expectations, the *originators* of the crimes did not distinguish significantly from the other alleged criminals, the *users*.

More surprising were the media over which the information was communicated. Hereby chat rooms ranked first, followed by those fakeZ Web sites ("hacker sites") on the Internet. For economically discriminated people those sites seem to offer attractive alternatives even though they are illegal.

The question of intent and traceability showed unexpected short-sightedness even amongst those alleged criminals who dispose of *good computer knowledge*.

With the help of educational campaigns in the context of preventative measures, naivety could be transformed into irrefutable knowledge that such crimes involve a high risk of detection for those who commit them.

As suggested media for these campaigns, the chat rooms and hacker sites that provided the information the alleged criminals were looking for would be recommended. If measures are taken, these media will respond (as they have responded in the past), not least because the alleged criminals tend to publish their (bad) experience there ("I was caught"). This also leads to a kind of self-regulation process because potential offenders are deterred by these measures.

3.7. Conclusion

Technological protection from external threats is indeed important, but human problems can not be solved with technological solutions. Especially if we take a closer look at the kind of methods the hacker community is using, it becomes evident that the most vulnerable piece of the puzzle is the human being itself. Kevin Mitnick, the only hacker to have been on the FBI's "most-wanted" list, and who was seen as a high-tech criminal, mostly used social engineering to obtain other people's identities.

Most importantly, this chapter showed us that we have to distinguish between hackers and criminals. Companies, organisations and governmental institutions should fear the criminals in the context of identity theft. Those are the people who have been pursued and prosecuted, and stricter regulations and laws will be implemented according to incidents that occur. In tandem with this, though, we have to study the criminals, their intentions, their motivations. We all have to gain a better understanding of their social and psychological background in order to find solutions to protect society and the individual.

Companies have to think about "best practice" approaches, whereas institutions have to fulfill the requirements for protection. This will still remain a challenge according to the fact that in the information age, the Internet is still often an anonymous space. The founders – in postulating freedom and liberty - initiated *the* uncommitted communication platform. But if identity theft incidents continue to grow, regulations will have to be implemented and intruders will have to be investigated. And it will be hard for the people who allow justice to prevail to distinguish between the good and evil hacker. The community therefore is inherently in the middle of nowhere...

4. Best Practice

Identity theft, particularly the fraudulent use of online identities, also facilitates online crimes: industrial espionage, computer hacking, cyber-terrorism, large-scale network attacks and the theft of identity information. One of the main culprits here is the widespread practice of using passwords as the sole means of establishing and authenticating an individual's online identity. Notoriously easy to steal or guess, passwords enable an intruder to access any resources the legitimate user is entitled to see and to probe the entry points to more secure resources – all with little fear of being detected. As a consequence:

- consumers lose their reputation and credentials
- enterprises lose money
- civil society is undermined

Deeply systemic in nature, identity theft is a natural consequence of our information-driven society. Over the course of a lifetime, the typical citizen willingly surrenders personal information to dozens or even hundreds of different entities. All this data ends up being stored electronically, in countless locations, and often with little protection. Additionally, identity information travels freely through the



traditional mail system – for example, in the form of credit card offers and bank statements – where it can be easily diverted.

As a result of this wide distribution, even those individuals who don't own a computer are vulnerable to theft. Identity information can be stolen by neighbours, roommates or troubled family members; by an unscrupulous colleague who knows our habits; or by a merchant who copies down our credit card numbers. Low-tech thieves rummage through mailboxes and dustbins, and high-tech thieves pilfer corporate databases. Recently there has been a dramatic increase in scams that use official-looking but fraudulent e-mail, Web-sites and hard-copy documents to trick people into disclosing sensitive information.

Whether identity information is stolen by high-tech or low-tech methods, technology often facilitates and accelerates the crimes that ensue. For example, stolen personal information is often sold to third parties via shadowy Web sites and credit card numbers can be used to make purchases online in a matter of minutes. At this point the real costs begin to mount for consumers and enterprises.

Fastest Growing Crime in the World!

Incidence of Identity Theft in the U.S. grew by more than 40% in 2003 over the previous year. The FTC (Federal Trade Commission) estimates 4.7% of the U.S. population, or 10 million people, were victims of identity theft over the last year, with total losses of US\$53 billion; the victims losses make up US\$5 billion of this, with the remaining losses being picked up by businesses.

Identity theft has become the "Best Practice" for criminals, offering many benefits to the perpetrator, including;

- The anonymous nature of the crime - allowing criminals to hide their true identities while they pursue illegal activities
- The ease in committing the crime in this technological era
- The relative ease of financially supporting themselves with fraudulent loans or credit card purchases

The Effects

Many Identity theft victims use words such as 'haunted,' 'devastated' and 'violated' to describe their ordeal, feeling victimised by the process. Many victims do not discover their identity has been stolen until they are turned down attempting to obtain credit. Others don't find out until they receive a call from collection agencies or government agencies when debts have been incurred.

Identity theft victims are often unable to get new credit cards or loans because their credit ratings have been destroyed through the process.

The average financial loss of a victim who suffered through new accounts being opened was \$1,200, and \$500 on average for all victims of ID theft. Time spent in resolving problems stemming from ID theft ranged from 1 hour to over 240 hours, with a direct correlation to the amount of time it took to discover any misuse of information. Difficulties experienced as a result of having personal information misused include problems obtaining or using a credit card; being harassed by



collectors; rejection of finance; banking problems; insurance rejection; having utilities supplies cut off; civil suits filed; and criminal investigations.

Victims: What would have helped?

Once victims have completed the long process of recovery from identity theft, **prevention measures were cited as the second most important action that would have helped** them (only “better investigation by law enforcement” was cited by more). These prevention measures are in the form of better awareness on their own part as to how to prevent and respond to identity theft. Specific areas where greater awareness was cited included taking greater security precautions in handling their personal information, such as destroying materials that contain personal information instead of simply putting them in the trash; not placing personal information on the Internet; and securing their personal information in their homes and at work. Maintaining greater vigilance, including more careful monitoring of their mail, billing cycles and credit reports was also cited. Lastly, knowing who to contact, and notifying the affected companies and credit reporting agencies more quickly when they detected something wrong, was identified as an important factor in recovering from identity theft.

How do criminals get your Personal Information?

In a survey conducted by the FTC, only 50% of all victims knew how their personal information was stolen - the other 50% still have no idea!

There are many methods in which personal information can be stolen. The first list shows how we can control or take measures to prevent the theft:

Information carelessly divulged by victim: Creative scams by thieves can trick us into handing over personal information, such as the thieves calling you pretending to be someone from your bank, utility company or another company that would already have your information, and asking you to confirm your details with them for security reasons. Thieves could also call other people, claiming to be someone they are not, to verify your personal information. ‘Phishing’ scams on the Internet or via physical mail are designed to extract your personal information - identity thieves are masters at deception and persuasion.

Old fashioned theft: Physically stolen wallets/purses are still a favourite for identity thieves as they contain so much personal information. ‘Dumpster diving’ is also popular, where thieves will rummage through bins in search of pre-approved credit card offers, bank statements, utility bills or anything similar containing personal information. Thieves will also search for mail in mailboxes that may contain bank and credit card statements, utility bills, cheques and – once again – any other mail that contains personal information or account numbers.

Unsecured or observed transactions: Unsecured credit card transactions over the Internet, phone or by mail provide an easy method for thieves to steal your details. Physical location transactions are susceptible to shoulder surfing or skimming.



Family, friends, colleagues, neighbours: Leaving your personal information around the home, at work or in the car for people to see, provides easy opportunities for theft of personal information - who is watching? Allowing people to overhear telephone conversations while you give out personal information is also another easy way to shed information - who is listening?

Internet Related Fraud: Internet Fraud is designed to extract your personal information, and poor Internet security allows hackers access to your computer where personal information might be found. A great deal of freeware is designed to spy on your habits and personal information, collect it and send it to central databases. (Download utilities, MP3 exchange utilities, etc.)

This second list shows methods of personal information theft over which we have little or no control:

Fraudulently obtained credit reports: Thieves posing as landlords, employers and loan officers might gain access to your credit report which contains a gold mine of personal information.

Dishonest employees with access to your personal information: Over our lifetime, we give our personal information to dozens or even hundreds of different entities: utility companies, financial institutions, insurance companies, telephone companies, accountants, solicitors, motor vehicle departments, manufacturers (warranty cards), etc. Information held by these entities is freely available to employees of the entity. These employees may have a criminal mind themselves, but more often than not, criminal fraud rings search people out who have access to consumers' personal information and offer to supplement their income in exchange for this information.

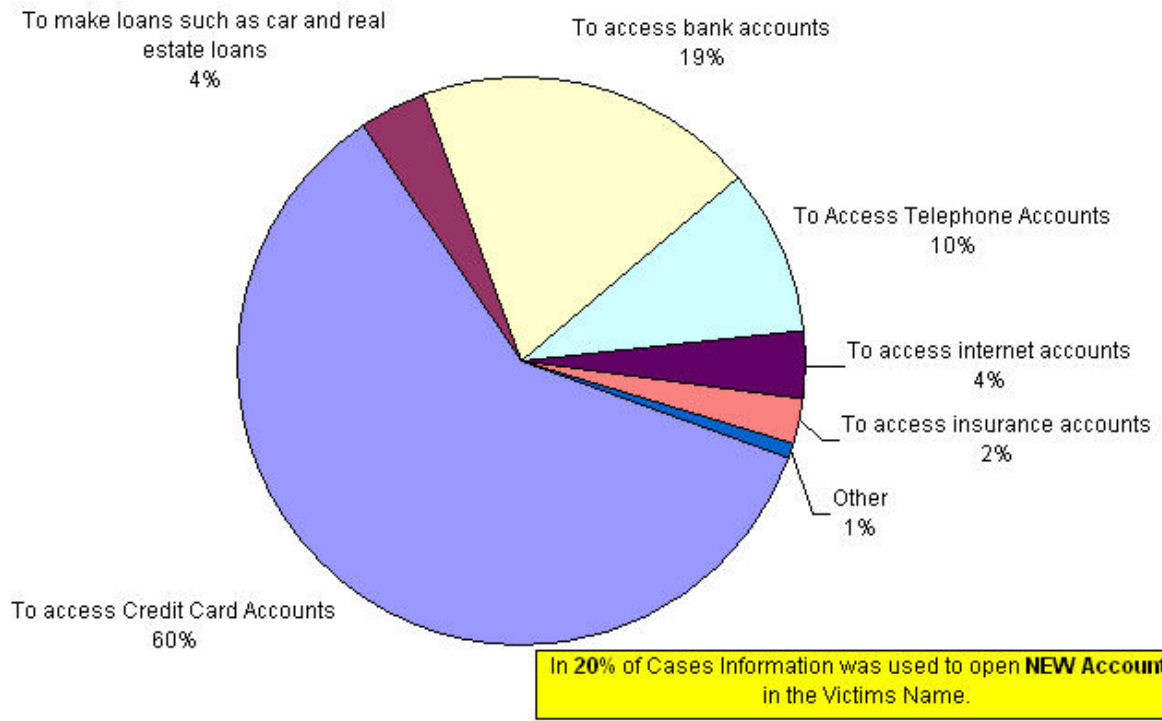
Hackers in Corporate Databases: High-tech thieves can hack into corporate databases and steal consumers' personal information. In France in 2002 there were more losses from targeted attacks over the Internet than from physical accidents within investigated companies. ("Study of losses – CLUSIF 2002")

What do the Thieves do With Your Stolen Information?

It is difficult to precisely pin down how stolen Information is used. However, the FTC commissioned a survey on Identity Theft during 2003 - the following information comes from this survey.

Here are some general methods of how stolen information was used.

How Stolen Information Was Used

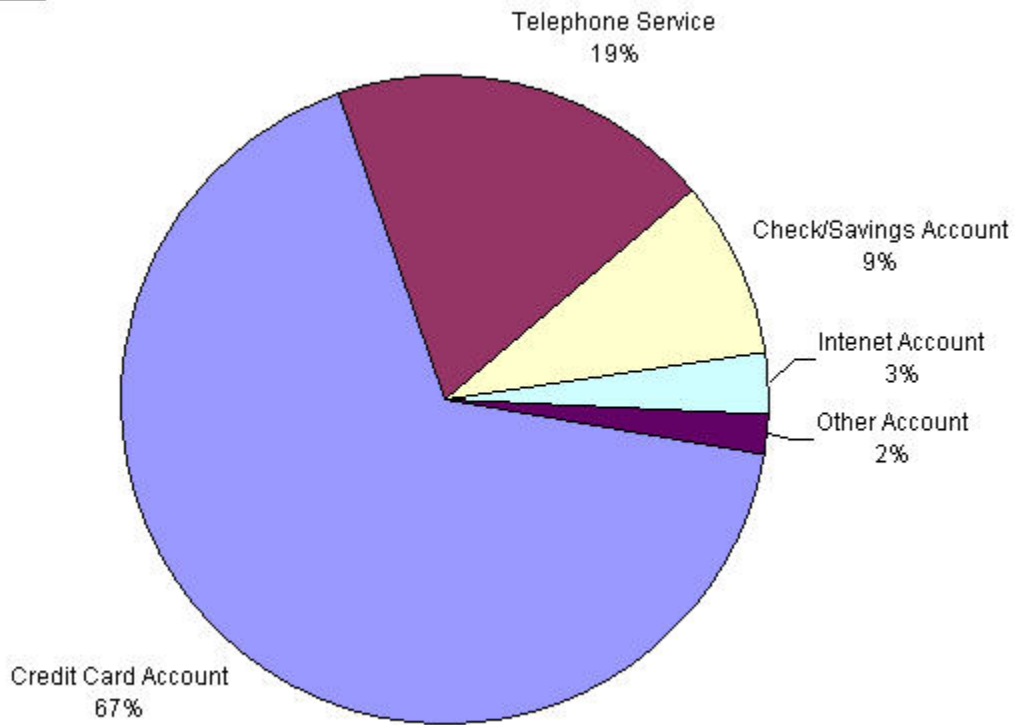


Source: Federal Trade Commission - Identity Theft Survey Report -

Of the Existing Accounts, the following graph details how this information was used:

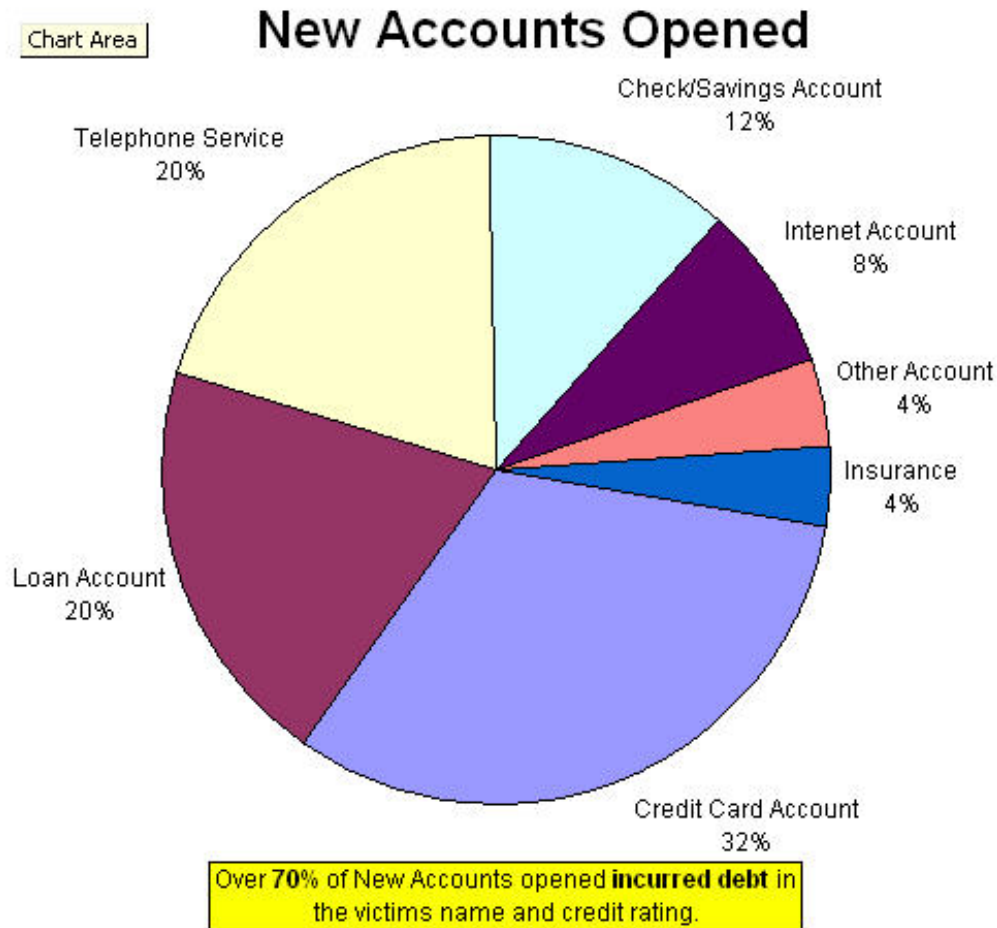
Chart Area

Existing Accounts MisUsed



Source: Federal Trade Commission - Identity Theft Survey Report

The following graph details what types of new accounts were opened:



Source: Federal Trade Commission - Identity Theft Survey

Other Uses for Stolen Information include:

- Employment - getting a job using the victim's name and identity
- Social security
- Tax returns
- Medical
- Residential leases
- Securities & investments

- Bankruptcy fraud
- Illegal immigration and obtaining miscellaneous government identification documents

4.1. Best Practice: Individuals

FraudWatch International sees itself meeting the needs of consumers by providing education on prevention measures and providing information on what to do if consumers become victims.

Tips for Prevention

- Never give out your personal information over the phone unless you have initiated the call and completely trust the caller. This includes credit card and bank account numbers.
- Always question the identity of people / companies that initiate contact with you - via email, mail, telephone or even in person - remember, ID cards, letterheads and business cards can easily be falsely created.
- Do not carry your extra credit cards or other important identity documents in your purse or wallet except when necessary.
- Minimise the amount of credit cards you own - cancel unused credit accounts.
- Keep a photocopy of all cards (both front and back) kept in your wallet or purse in a safe and secure place. This makes it easier to contact every relevant institution in the event that your purse or wallet gets lost.
- Never leave your purse or wallet unattended - at work, church, restaurants, parties, or shopping trolleys.
- Direct all mail you receive to a post office box or secured box. This is especially relevant for bank and credit card statements, utility bills etc.
- Safeguard all card transaction receipts - do not throw them out at points of purchase or in public. Shred them at home.
- Cut up and dispose of all inactive or old credit or ATM cards. Even expired cards can be of benefit to thieves.
- Safeguard all bank and credit card statements, and all utility bills. Do not simply throw these in the bin or recycling bin - shred them when you no longer require them.
- Never simply throw out pre approved credit offers - always shred them.
- Reconcile all bank and credit card accounts immediately when you receive them. Challenge any unauthorised transactions immediately.
- If you don't receive a statement, notify the bank immediately.
- Check you have authorised all charges on utility and telephone bills before paying them.
- Protect your Social Security Number - this is not a number just anyone can have if they ask, always ask why companies or people might want your SSN.
- Do not print your SSN on your cheques.
- Order your Social Security Earnings and Benefits Statements once a year to check for fraud.
- Never write down your PINs - memorise them - if you do need to write them down, do not keep it in the same place as your card (e.g., wallet or purse)

- Be aware of shoulder surfers when you are using your credit card or ATM card. Always ensure you keep your PIN safely hidden from others.
- During physical card transactions, never let your card out of your sight - this is especially true for restaurants. It is best to hold on to your card and enter it into the machine yourself.
- Never let a waiter disappear with your card, even if he is processing your transaction - skimming is very popular in restaurants.
- When making Internet transactions, ensure you are using a secure server and you completely trust the company you are dealing with.
- Never leave your personal information around the home, at work or in the car. Even a friend or neighbour could succumb to the temptation of stealing your personal information if they see it lying around.
- Always be careful of who is listening to telephone conversations when you are giving out personal details. Who can hear you? Even at home if you have windows and doors open. Who is listening at work when you call your utility company and they need to verify your identity?
- Remove your name from the marketing lists of the three credit reporting bureaus to reduce the number of pre-approved credit offers you receive.
- Monitor your credit reports.

4.2. Best Practice: Companies

Most identity theft precautions and warnings are aimed at the wrong targets. Although consumers are ultimately responsible for protecting themselves and their information, they lose direct control over that information at precisely the point when it becomes an attractive target for thieves. During an online transaction, the consumer hands direct control over to a merchant for the furtherance of that transaction. When it has been completed, the consumer's personal information becomes a data file, residing in the online organisation's network. The consumer is now completely dependent on the organisation to effectively maintain the security and confidentiality of that data.

Federally regulated industries have made some good progress in holding organisations responsible for the protection of personal consumer information. Financial institutions directly regulated by banking agencies and credit-union authorities are further required to protect such data from theft, misuse and unauthorised alteration. These organisations are required to apply specific security control measures to customer data, such as controlling employee access to customer data by job function, performing background checks on employees that require access to customer data, and encrypting customer data in transit and in storage. These requirements provide a solid security foundation for the corporate computing environment.

At a minimum, organisations can take a few simple steps to improve data security:

- Implementing a Security Policy.
- Classify customer data as sensitive.
- Create or revise sensitive data-handling policies and procedures to include items such as:
 - o Limiting access to customer data based upon job function.
 - o Locking file drawers and cabinets that store customer data printouts.

- Securely destroying customer data on all forms of media - they have to use strong magnetic devices to destroy the data from electronically stored information (shredding and formatting is not enough!), shredding printouts and paper files; etc.
- Keep customer data available on the public-facing Web server only as long as needed (presumably, for the length of the transaction).
- Create update routines for all of your servers, to supervise available security patches and implement them.
- Pass customer data from the Web server to a database server.
- Locate the database server on an isolated network segment.
- Limit physical and logical (electronic) access to the database server by:
 - Restricting logical access to customer data through authentication measures.
 - Routinely reviewing user accounts and privileges to accommodate staff turnover and changes in job function.
 - Perform background checks on employees who have access to customer data.
- Enable logging on critical systems.
- Routinely review logs for unusual activity.

These control measures are not comprehensive but, working together, they can quickly and significantly reduce the risk of a successful exploitation of critical assets and data. They represent a "must-do" security checklist for all organisations that seek to limit their liability and protect their customers from the growing threat of identity theft.

Identity theft is a complex phenomenon that calls for vision and leadership across all sectors. A multi-level response is required, one that addresses the various dimensions of the issue: laws and public policy, business practices in key industries; IT security practices; procedures for helping victims restore their good name; the response by law enforcement and the criminal justice system; and changes in consumer behaviour.

Evaluate vulnerabilities to online identity fraud. In addition to understanding where identity data is vulnerable, organisations need to assess their potential exposure to the fraudulent use of online identities. How many of your mission-critical resources — networks, applications and data sources — are only protected by passwords? How easy would it be for a hacker or other intruder to steal, guess or crack a legitimate user's online identity? What kinds of resources could they access simply by gaining entry to your intranet? How likely would it be that such an intruder would be detected and caught? How much damage might they do before drawing attention? How easy would it be for a legitimate user — such as an employee or partner — to commit illicit acts and escape detection?

Through this assessment process, an enterprise gains a baseline understanding of their current environment and vulnerabilities and can begin to redesign business and IT security practices to reduce their risk of identity theft and online identity fraud.

Implement best security practices to thwart identity fraud. Organisations that profess to take identity fraud seriously need to "walk the talk," safe-guarding customer information with the same

high level of protection that is applied to sensitive proprietary information or high-value transactions. This means employing best security practices, such as the latest firewall and anti-virus measures. In addition, there are two critical areas:

- With identity and access management (I&AM) solutions, organisations can create trusted online identities, making it easier to reliably verify with whom they are doing business and allowing them to efficiently manage users' access to protected resources.
- Encryption solutions make data unintelligible to unauthorised users and, in the process, protect identity data from being compromised while at rest or in transit.

For enterprises, there is some good news about identity theft: Many of the investments that have been made in e-security during the last few years can be leveraged to address identity-related crimes and abuses in the online world. Organisations that adopt a more consumer-aware view of identity theft will suddenly see new opportunities to protect their customers and employees by making incremental adjustments to their current security plans.

There are four key elements in securing identities in the IT-world:

- Strong authentication – the verification of identities
- Access Management – controlling who has access to what
- Digital Signatures – authenticating online transactions and communications
- Encryption – protecting identity data at rest and in motion

4.3. Best Practice: Industry

Industry has a duty to care about issues including standardisation or interoperability:

Achieve compliance. Organisations need to understand how current laws and regulations constrain the use of sensitive information today and how pending legislation could impact business and IT security practices in the future.

Develop cross-industry solutions for identity management. As enterprises strive to enhance their internal defences against identity-related crimes, they are also working collaboratively to develop cross-industry approaches for creating, proving and managing online identities. The Liberty Alliance Project is one of the most far-reaching of these initiatives.

The Liberty Alliance is a global consortium of 150-plus businesses, government entities and technology vendors. The alliance was formed to develop a global standard for network identity management, based on the concept of federation: the ability of enterprises to securely share widely distributed identity information in a way that safeguards sensitive information and respects the privacy wishes of the consumer.

Ultimately, the goal is for each user to establish a highly secure online identity that would be recognised and accepted by a wide range of leading enterprises. Users would benefit from single



sign-on (SSO) — the ability to navigate freely among protected e-business sites without having to register every time they encounter a new site or log in every time they return to a site. Businesses would benefit from the growth of e-business revenues, reduced partnering and process costs and faster deployment of innovative new services.

Educate consumers and strengthen enforcement and penalties. Even as enterprises seek long-term remedies for identity fraud, consumer awareness remains one of the most effective tools for battling identity-related crimes in the short run. As the Federal Trade Commission has documented, prompt discovery of identity theft dramatically reduces the total monetary value of fraud that is committed in a consumer's name. Early disclosure also reduces the amount of time and money the consumer must devote to repairing his/her credit reputation.

With these facts in mind, more than a dozen leading companies and trade associations banded together in September 2003 to form the Coalition on Online Identity Fraud. Founding members include well-known technology companies and online merchants (Amazon.com, eBay, Visa, Microsoft), leading security technology firms, and two major industry groups: the Business Software Alliance and the Information Technology Association of America (ITAA). The coalition plans to address four primary areas:

- Educating consumers so they can protect themselves more effectively
- Promoting technology and self-help approaches for dealing with identity theft
- Sharing information about emerging online fraud techniques and
- Encouraging more effective enforcement and penalties for identity-related crimes

5. Conclusion

We have learned that identity-related fraud may have many different causes. A lot of them are not related to computers at all. Most of them are very simple. And, importantly, none should be underestimated. Those related to information technology are particularly serious because they have the potential not only to cause a great deal of reputational damage to the victim, but also significant monetary losses.

“Real” hackers seek to add value to the open source community. Their aim is to help individuals and companies regarding their security policies. Of course from a legislation point of view it is debatable whether their activities are “legal”. This paper has underlined, though, that the problems we are faced with mostly result from the activities perpetrated by other groups. Criminals as well as script kiddies or crackers are the people we need to focus on.

Whereas criminals cause damage for financial purposes most of the time, script kiddies often attack systems just for fun or simply because they are bored. Often these two parties do not possess strong technological or intellectual backgrounds; they use simple – yet effective – means to steal identities, including chat rooms and similar environments. In the rare instances where they do employ programmes (viruses, Trojan horses etc.), generally speaking they will not have created

those programmes themselves; instead they use the intellectual property of others to launch their attacks.

So the whole discussion about hackers, crackers, script kiddies and other intruders will continue. It always will be a small catwalk and academics as well as other experts will always have different opinions regarding the hacker community. However, whatever the arguments, companies as well as individuals must never underestimate the criminal potential of hacking and the danger that inherent in identity theft. Both sides have a duty to educate themselves and each other and keep ahead of the game at all times.

There is obviously a strong correlation between hackers – or *criminals*, it would be more accurate to say - and the theft of identities. The number of incidents perpetrated over the Internet is continuously on the rise, and it is imperative for companies and official institutions alike to think seriously about solutions and best practices.

There are three compelling reasons to address this challenge now:

- **Accountability.** Firstly, it is the ethical thing to do. Individuals have entrusted their personal information to large organisations and are extremely vulnerable as a result. Enterprises, which benefit greatly from such information, need to take responsibility for better-protecting that information. They also need to recognise that doing little or nothing represents irresponsible practice and puts consumers in harm's way.
- **Risk.** By failing to safeguard against identity-related crimes, organisations increase the likelihood of security breaches and all the resulting costs: bad publicity, customer defections, lost business opportunities, remedial costs and legal liability. With the accelerating pace of online incidents, this risk appears to increase on an almost daily basis.
- **Opportunity.** The security measures that are most effective in thwarting identity-related crimes have a much wider strategic benefit. The creation of an e-business environment that is viewed by consumers and businesses as being truly trustworthy sets in place the foundations for accelerated e-business growth. This in turn creates new opportunities to increase revenues, reduce costs and deliver innovative services that confer a significant competitive advantage.

6. References

- 1) Aberdeen Group, CIO Magazine, May 23rd, 2003
- 2) "Criminal statistics", Bundeskriminalamt Germany, 2002
- 3) "Identity theft and the Internet", Stephen Schaefer, 2002, Georgia State University College of Law
- 4) "IEEE Security & Privacy", Bruce Schneier, Vol.1 No.6, Nov/Dec 03, 2003
- 5) "Hacker Psych 101", Jeremy Quittner
- 6) "How to become a hacker", Eric S. Raymond, <http://www.catb.org/~esr/fags/hacker-howto.html>, April 23rd, 2004
- 7) "Hackers. Heroes of the Computer Revolution", Steven Levy, 1984
- 8) "The on-line hacker Jargon File", Version 4.4.7, April 23rd, 2004
- 9) "Study gets hackers to open up", Mariah Moore Khanna, October 2003
- 10) "How to become a hacker", Eric S. Raymond, <http://www.catb.org/~esr/fags/hacker-howto.html>, April 23rd, 2004
- 11) "Homesteading the Noosphere", Eric S. Raymond, <http://catb.org/~esr/fags/hacker-howto.html>, April 23rd, 2004
- 12) "Psychological Theories of Crime and hacking", Marc Rogers, Department of Psychology, University of Manitoba
- 13) "The Modus Operandi of Hacking", Marc Rogers on Dr.O'Connors Criminal Justice Megalinks

General references:

"Analysis and statistics on computer system losses in France – Year 2002"

"Account-Missbrauch im Internet", Jens Vick & Franz Roters, BKA 2003