

SECURITY THREATS AND TRENDS

FEBRUARY 2007

SECODE AB

Secode helps companies and organizations gain insight, competence and thereby control over their operations from a complete IT security perspective. We deliver proactive and perpetual vigilance within two areas: 24/7 Managed Security Services and Security Consulting.

The Company was originally founded in 1986 as System Sikkerhet A/S, in Arendal, Norway. In year 2000, Secode AB was founded in Sweden and started its 24/7 Managed Security Services and Security Consulting. The two companies merged in January 2004, thereby forging the leading Digital Security Company in the Nordic region. In March 2006 the Finnish IT-security company Netsol OY (founded in 1996) was merged into Secode. From the first of January 2007 Secode has established sales-offices in both Denmark and The Netherlands and delivers IT-security services to customers in these countries as well. Secode helps many customers in private and public sectors, from seven different locations, using close to 85 security specialists. These specialists have long experience from building large computer networks and/or up-to-date IT security competence. Secode AB today has more than 100 employees.

All this together makes Secode the leading Northern European Digital Security Company within Managed Security Services combined with IT-Security Consultancy Services.

SUMMARY

The total number of reconnaissance attacks has shown an increase during January. A number of vulnerabilities in Symantec software was published at the end of December, and is mostly the origin of the increased activity.

Focus of the Month takes a closer look at trends amongst the youth.

TABLE OF CONTENTS

INTRODUCTION	3
THREAT LEVEL.....	4
RECONNAISSANCE ATTACKS JANUARY 2006.....	4
TYPE OF RECONNAISSANCE ATTACKS	5
RECONNAISSANCE ATTACKS PR COUNTRY.....	6
INTERNET WORMS AND SPAM.....	7
ALERT STATISTIC.....	8
HANDLED ALERTS	8
REPORTED INCIDENTS.....	9
FOCUS OF THE MONTH – YOUTH TRENDS	10
YOUTH AND PRIVACY	10
YOUTH AND PIRACY	11
HOW TO GET FOCUS ON THE ISSUES AT HAND?	11

INTRODUCTION

This report is based on three main parts; Threat level, Alert Statistic and Focus of the Month.

Threat level is a presentation of what threats organizations are exposed to through their Internet connection. In this threat evaluation, reconnaissance attacks from the Internet against customers of Secode are analyzed and presented.

Alert Statistic is based on alerts from Secode's IDS and IPS tools. An alert appear when a sensor recognizes network traffic that fit the implemented signatures/filters, and in these cases alerts will be transferred to Secode SOC (Security Operation Center). All alerts, both false and genuine, are manually handles by analysts at Secode.

Focus of the Month is an article that focuses on relevant topics within IT Security. This might be topics discussed in media, incidents that can influence the threat level, or changes in the attack pattern from the Internet.

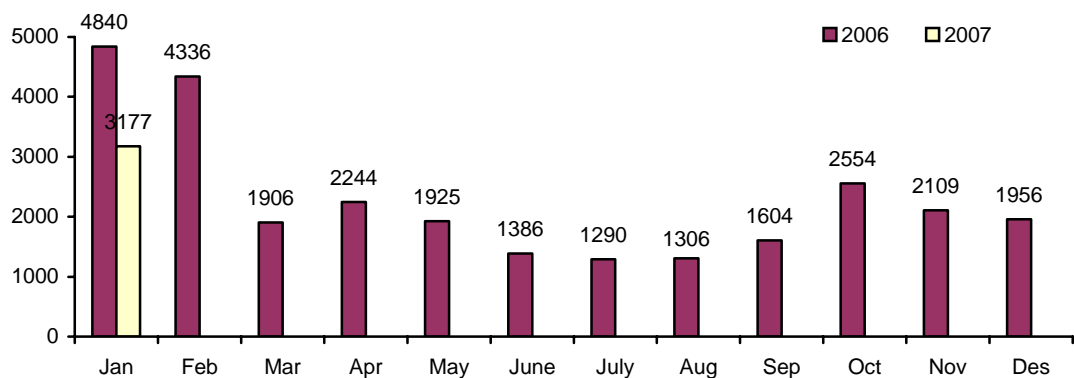
THREAT LEVEL

Due to high activity level, Internet worms and spamming are handled in a separate subchapter; "Internet worms and Spam", and are excluded from the other charts in this chapter.

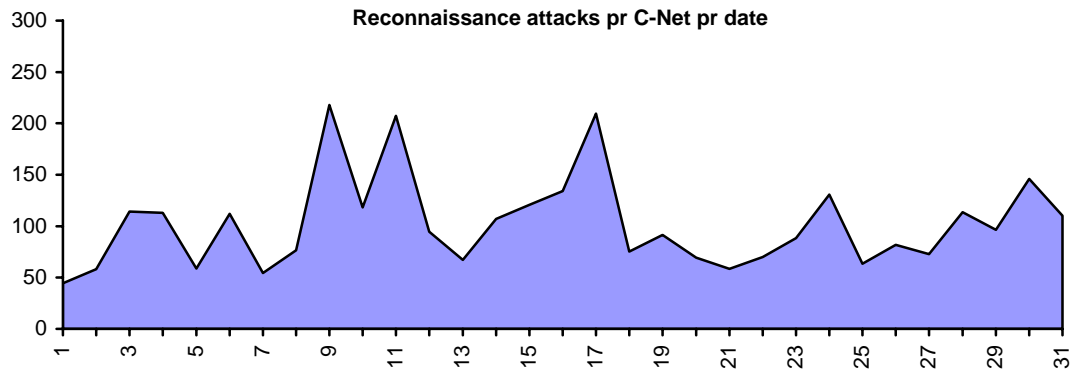
RECONNAISSANCE ATTACKS JANUARY 2006

The statistics below gives an overview of the average number of reconnaissance attacks per network under surveillance. However, the activity level may vary from one network area to another. Despite these variations in the total activity level, we (mostly) register the same kind of attacks in different network areas.

Reconnaissance attacks pr monitored C-Net



Reconnaissance attacks pr C-Net pr date



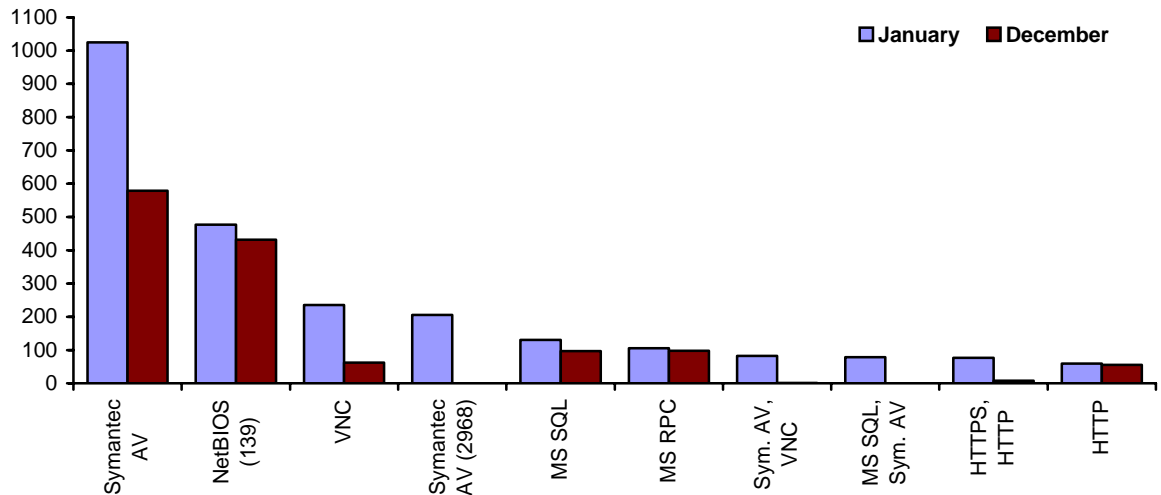
The total number of reconnaissance attacks has shown an increase during January. This activity is mostly due to the Symantec software vulnerabilities published in December. These vulnerabilities have been the origin of several worms and reconnaissance attacks. Several Internet surveillance companies register the same trends.

If we look at the level of activity divided into dates, we see that there are no big peaks. The peaks we do see are mostly due to new attacks against the Symantec software.

TYPE OF RECONNAISSANCE ATTACKS

The diagram below contains a summary of the most common reconnaissance attacks during the last two months, whether it is scans for one single service or combined scans for several services.

Average top 10 incidents pr C-Net



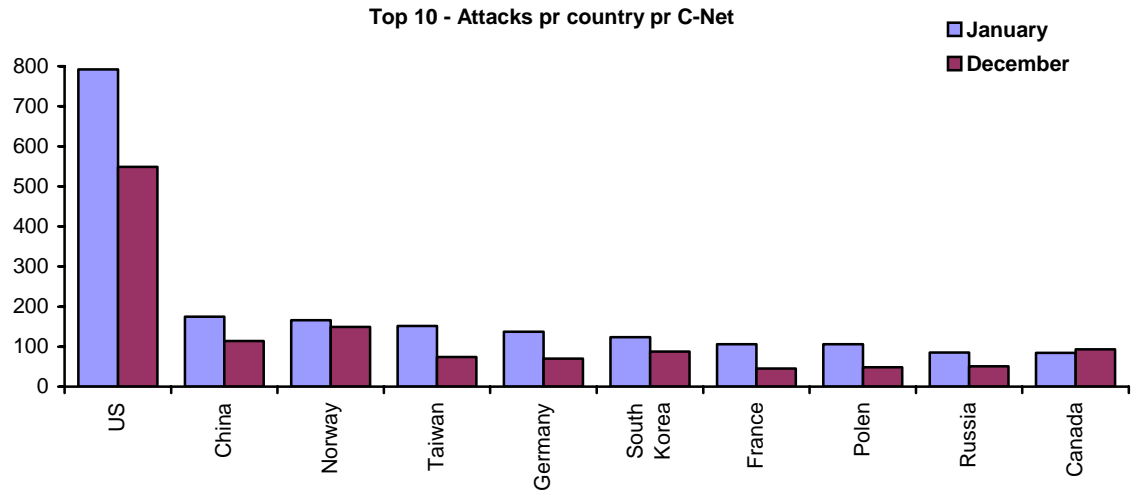
The big increase in searches against tcp port 2967 (Symantec AV) continued through January. This is, as previously mentioned, due to several vulnerabilities in Symantec Antivirus and Firewall which became known in late December. Exploit code has been made available, and there are also registered at least two worms that are responsible for searches against this port.

A new trend emerged in January however. We now see several scans towards TCP port 2968, which is also in use by Symantec for software updating. In addition we also registered that searches against port 2967 is now combined with searches against other services. This trend suggests that worms are the origin of several scans. New worms are often made to exploit several vulnerabilities, this to make it more possible to spread over a large area.

Except the trends mentioned above, there are no surprises in the statistics over reconnaissance attacks. All services, which are not already mentioned, are usually placed at the top of the list. However, all searches against services at the top 10 have increased this month.

RECONNAISSANCE ATTACKS PR COUNTRY

The malicious activity in the statistic below is mainly automated attacks, which comes from infected computers (e.g. Internet worms or viruses). This means that most of the attacks are not directly aimed, but are rather a secondary effect.

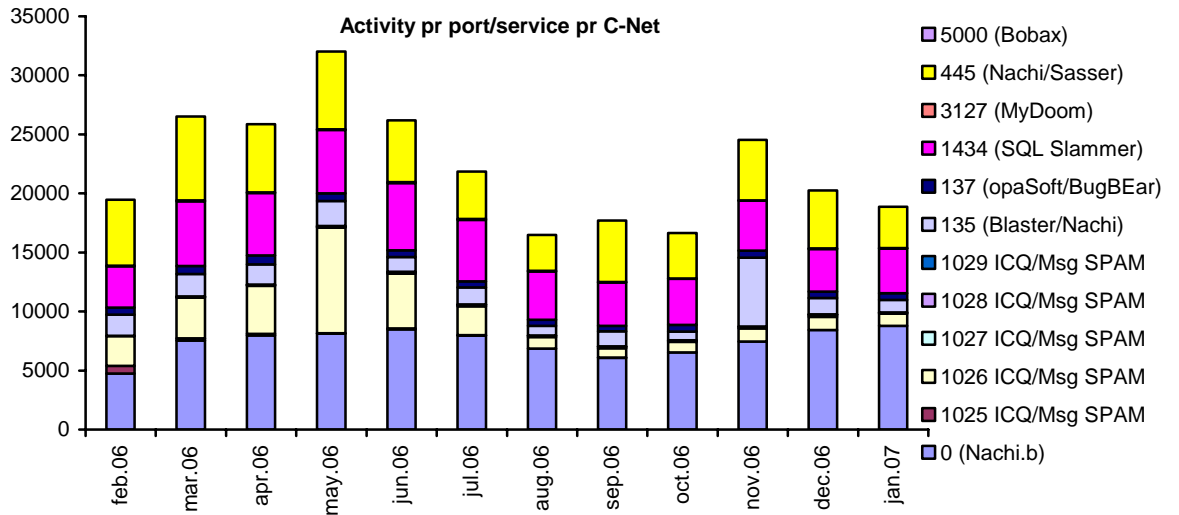


Once again the US is the most aggressive origin of reconnaissance attacks, this month followed by China and Norway. It is registered an increase from all countries, which is most likely due to searches against port 2967. When searches against port 2967 started to spread over Internet, Asian countries and the US was the origin of attacks. Now we see an increase from several countries, including Norway.

The level of traffic in one country will reflect the total level of traffic.

INTERNET WORMS AND SPAM

Because of a high level of activity against certain services, this traffic is presented in a separate statistics. This applies for those services which are most frequently targeted by Internet worms and spamming attempts.



The number of worms is still decreasing slightly this month. It is mostly traffic at port 445 that is decreasing, while the other categories remain stable. The number of worms and spam is still low in comparison with some of the peeks we have seen during the last couple of years.

ALERT STATISTIC

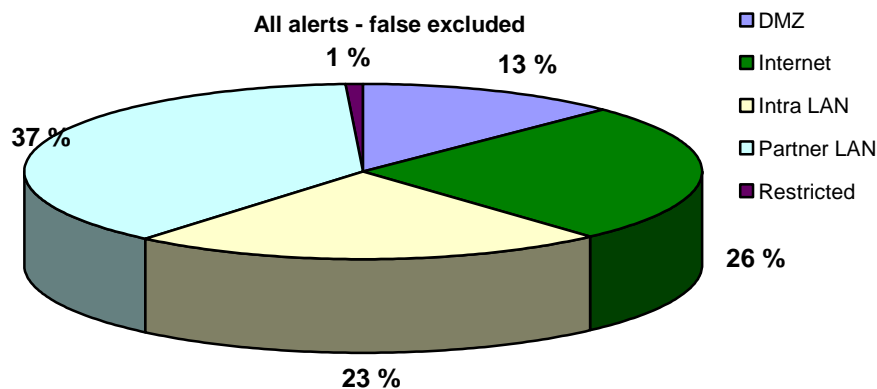
This chapter gives a summary of alerts from IDS/IPS sensors. These alerts are all analyzed by Secode SOC. The statistics shows the distribution of alerts pr net segment that are under surveillance.

HANDLED ALERTS

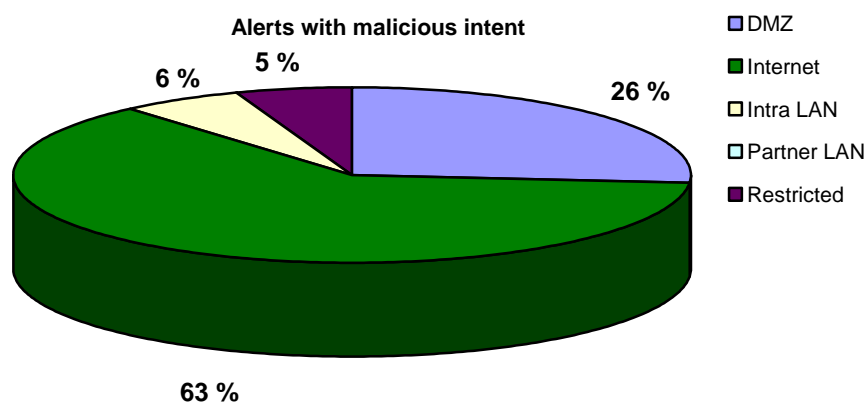
The statistics below shows handled alerts distributed at the different network segments where Secode's measuring points are placed.

The network segments are divided into the following:

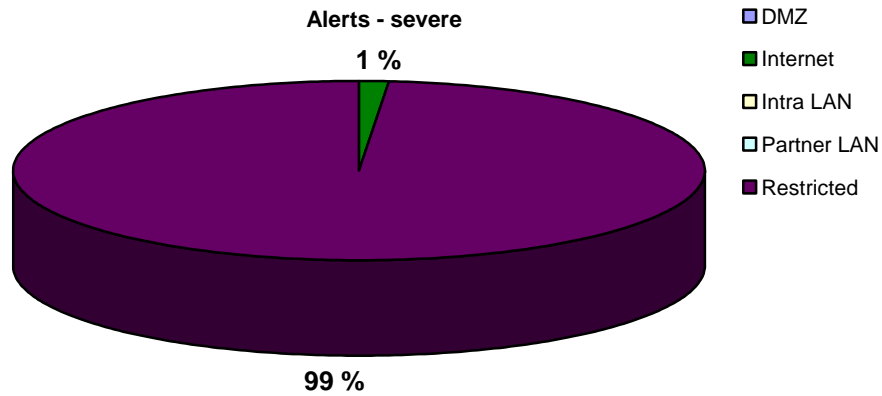
- Internet: the measuring point is located outside the firewall on a network exposed to the Internet
- DMZ: the measuring point is placed inside the network and monitors traffic against services that are exposed to Internet or other unsafe, external networks
- Intra LAN: the measuring point is placed inside the network and monitors traffic between clients, servers and other network equipment
- Partner LAN: the measuring point is located in an environment that is used for communication towards external partners. The partner LAN is without Internet access
- Restricted LAN: the measuring point are located in a limited environment with a very well defined traffic pattern and without Internet access



The diagram above shows the distribution for all genuine alerts.



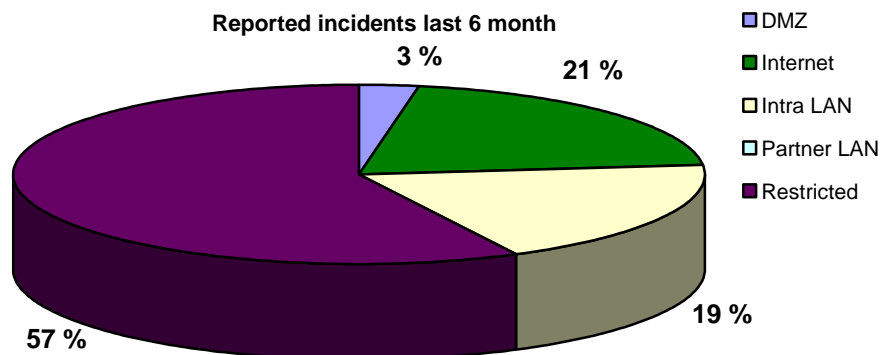
The diagram above shows the distribution for all alerts caused by activity with malicious intent, without the customer necessary being vulnerable.



The diagram above shows the distribution of all alerts caused by activity with malicious intent, and where the customer might be vulnerable or compromised.

REPORTED INCIDENTS

The statistic below shows distribution of incidents reported to customers of Secode the last 6 months.



FOCUS OF THE MONTH – YOUTH TRENDS

This month we have chosen to write about youth trends, and that may leave some of you thinking what use it is for you. By focusing on youth trends we will see signs of trends among other users of the different kinds of media. And, in addition, we can put some security risks in focus. The young people are big users of computer technology and other mediums, and therefore you often see the negative trends here first.

All security problems can be set in content with youth, but at this time we will cover to the subjects; privacy and piracy (illegal downloading).

YOUTH AND PRIVACY

In earlier editions of “Focus of the Month” we have covered privacy and use of e-mail, and privacy with use of blogging. Privacy is still one of the most problematic and widespread security risks on Internet today. One of the reasons for this is that privacy do not get enough focus as part of the total security solution. Companies spend lots of money to protect the company from external attacks, like worms, hackers, Trojans and so on. Companies do not however give focus, and resources, to make employees familiar with what they can do to improve security. It is here privacy is one of the most important aspects. Employees may publish lots of information about themselves on the Internet, which may seem harmless, but in the right hands may be dangerous for both company and person.

In the youth community you will discover how little awareness it is around protecting their personal information. There are few young people who think about possible consequences of posting an e-mail address at a newsletter site, or adding a profile on a blog or contact site. The consequences of senseless use of personal information may be huge, both for the person in question and for companies or organizations. There are several examples of personal information being misused to make bank withdrawals.

Lately the news media in Europe and especially Norway, has focused on privacy. New surveys showing that youth often regrets posting information on the Internet, is the reason for this new focus. As many as one third of all youth regrets posting something on the Internet, and this is often pictures or short movies they have posted on personal profiles or community sites like YouTube. When there are so many young people regretting posting information, it is likely that there are many adults regretting too. Posting pictures on Internet, for example, is not reserved youth, even though youth is often more frequent users of such services.

It is easy to believe that information is more protected then it actually is. Windows Live Spaces is a good example of this. Users have opportunity to decide who should have access to there own profile/blog, and maybe they choose to give access to everybody in there Windows Live Messenger contact list. This does not mean that only these people have access to the profile. There are no guarantees that none of these people do not download information and in worst case spread it. Access may be granted to others by mistake without the owner’s knowledge, or people deleted from the contact list may still have access, also without the owner’s knowledge. In other words, you loose control over your own documents, pictures and so on when they are posted on the web.

In the example above the user have at least some control, which is more than we can say about pictures and videos posted on public sites. This is what most people regret. In the exact moment you post a video or a picture on a site like that, you loose all control over where it may appear next time. In addition, it is more or less impossible to delete it from Internet. In other words, many things that seem alright to post at one time, may not seem so smart at another time. At that point you are most likely in some trouble, because it is more or less impossible to remove all traces. The classical example is when you apply for a job.

At the moment you apply for a job it is likely that the employer will google the applicant to retrieve more information about the person. A webpage built as a prank in your younger days may indicate that you are an “irresponsible person” or similar. Said in another way, information you may have posted on Internet, which may not represent you for who you are, may be used by employers to paint a picture of you. It is not without reason many experts are of the opinion that everybody who applies, and are going in for a job interview, should google themselves to get a picture of what the employer knows beforehand.

The following rule should be in mind when it comes to posting information on Internet; What you post there, will stay there.

YOUTH AND PIRACY

It is no longer a secret that many young people download music, movies, applications and so on from the Internet. As long as it is reachable it will be downloaded, and maybe shared with others. In the news the focus is on why people should stop downloading to stop money losses for the producers, while security issues is somewhat forgotten. Personally I believe that security risks by downloading should be put in the spotlight.

The security risk in itself is pretty huge by downloading from Internet, since there are no way of knowing exactly what the files contains. It is no problem to make a file at a music-file size which looks like a legitimate music-file, while it actually contains malicious code. You may also be unfortunate and receive malicious code from a script on a website or similar, while you are looking for some specific file. In addition, the user will put him- or herself, or, in worst case scenario, the company, in a situation where they are at the wrong side of the law.

New research has shown that many people make use of the company account at the Internet to use “illegal” services. In other words, there are many people sitting at work in different companies, using the computers there to download music, movies, porn and so on. With this in mind, how do you believe it would be in the future if we did not get young people to start thinking about security? Our mutual goal must be that new employees will be so aware about security issues around downloading, that they do not risk using company accounts for this purpose.

HOW TO GET FOCUS ON THE ISSUES AT HAND?

The Council of Europe has determined that 28 January the “Data Protection Day” should be celebrated as a yearly event. In connection with this, a campaign for giving young people in Norway knowledge about privacy issues has been established. This is an important step in the right direction, but it is not enough.

For some time now there have been a campaign running on cinemas and similar about piracy. The response I have registered about this campaign is that the young people know that it is illegal, but it does not help them when they can not afford to buy legally. This certainly applies for software applications. More and more use computers at school, and therefore have their own laptop. The problem is that the youth can not afford to fill it with legal software for the daily use. If the school demands that the students uses Microsoft Excel in economics it is a highly difficult task to convince teachers that OpenOffice Calc is as useful. Teachers in general do not have the knowledge needed to make such a decision, and this applies to many students to.

What I am trying to get out in the open here, is that it is of course important to put focus on what is legal and what is not, and which laws you can look at for protection and which you should not break, but it is not enough. Young people are not interested in knowing if they break a law, they are however interested in knowing what is their profit by keeping to the law, in comparison with the slight chance they may get caught. In other words, the focus should be on what the youth get out of following the law. One example may be that by downloading illegal music, a virus may infect the computer, and this may result in increased

expenses on computer equipment because this may be reduced or destroyed, while with legal downloading you are guaranteed virus free files. Another example may be if you pay for publishing pictures at a photo album at Internet you get file protection and backup as part of the service. By doing this you give something back to the users when they pay for the services. This combined with increased general focus on privacy and security among the youth, and adults for that matter, would give the extra argument to follow the law.

Of course many of these suggestions lies on a higher level and may even have to be implemented on a national level to profit, but as an individual you can do much good by taking security issues, privacy and alternative solutions into consideration.