Confederation of European Computer User Associations

Confédération Européenne des Associations d´Utilisateurs des Technologies de l´Information

info@cecua.org www.cecua.org

European Network and Information Security Conference

The user: A neglected species?

Dr. Jon Thorhallsson,
President CECUA (Confederation of European Computer User Associations)

Vilnius November 24-25 2005

The theme of this Conference is Readiness for Handling Network and Information Security Incidents. I will be speaking about this from the user perspective.

We seem to be facing an interesting paradox; Internet is everywhere, everybody is potentially an Internet user, nevertheless the user is a neglected species. Why is that so? Because the Internet still is considered a technical issue and actions and decisions are made without taking into account the people and the citizens. Therefore, we have a social divide on top of digital divide.

But now we will return to the theme of user readiness for handling network and information security incidents. First what is an incident? What is a user incident? For this presentation I will use the following definition:

Any user network experience which is out of the ordinary or different from what the user expects is a user incident.

Also when I refer to user **I mean end user.**

So the question of user incident from the user perspective boils down to what is it that the user expects? Anything the user does not expect is an incident.

I will start out by recalling examples of what the user does not expect. Throughout this presentation I will be referring to examples from the international press to substantiate my case. Mostly I will be using Danish and German sources and also some from USA. Why German and Danish? Because I want my examples to cover the broad scope of the EU, Germany is a large EU member state with 70 million people and Denmark one of the smaller ones with 4 million people. Most other member states are somewhere in between. And I am also using sources from the USA as an Internet pioneer and also a trendsetter.

So what does the user see in his paper or hears on radio and sees on television? Is what he experiences what he expects?

No, the user definitely does not expect to be confronted with news like this:

"Nordea paniklukker efter netbank-kupforsøg"

"Nordea har lukket sin netbank og alle sine internettjenester i Sverige efter et storstilet forsøg på at lokke oplysninger ud af kunderne via e-mail, også kaldet phishing."
COMPUTERWORLD 041005

... Nordea Bank shuts down Internet banking in Sweden after phishing attack...

"Ebay-Hacker kauft für 400.000 Euro ein"

"Mit einem geknackten Passwort des Internet-Auktionshauses Ebay hat ein Unbekannter in einer Nacht mehr als 1000 Mal eingekauft. Insgesamt orderte der Hacker Waren im Wert von fast 400.000 Euro auf den Namen eines 67-Jährigen aus dem sauerländischen Iserlohn. Horst Lukas ist sichtlich verärgert: "Ich bin mit den Nerven am Ende. Ich werde per E-Mail beschimpft, weil ich mich nicht melde", sagt der Rentner."
COMPUTERWOCHE.de 280905

... hacker makes 400 thousand Euro purchases from Ebay using stolen password from a 67 year old retired person .....

"Security breach may have exposed 40M credit cards"
"A hacker was able to access potentially 40 million credit card numbers by infiltrating the network of a company that processed payment data for MasterCard International Inc. and other companies, MasterCard said Friday"
COMPUTERWORLD 170605

Unfortunately those examples are not isolated incidences.

"Integralis warnt vor Sicherheitslücken in Online-Shops"
"Die IT-Sicherheitsfirma Integralis warnt vor gravierenden Sicherheitslecks in Online-Shops. Nach Schätzungen des Unternehmens sind rund die Hälfte aller E-Business-Plattformen angreifbar. Zirka 20 Prozent weisen laut Integralis Sicherheitslücken auf, die das Auslesen oder eine Manipulation der Kundendaten ermöglichen."
COMPUTERWOCHE.de 270905

... 20 % of all online shops are not safe says security company Integralis .....

What do research companies have to say?

"Vertrauen der US-Bürger in Online-Geschäfte lässt nach"
„Das Vertrauen der US-Amerikaner in die Sicherheit von Online-Transaktionen sinkt. Das haben die Marktforscher von Gartner durch Befragung von 5000 erwachsenen US-Bürgern herausgefunden. Als Ursache für den Vertrauensverlust machen sie Meldungen über den Diebstahl von Kreditkartendaten aus sowie auch die zunehmenden Betrugsversuche durch Phishing. So wären die etwa 73 Millionen US-Amerikaner, die das Internet nutzten, in den vergangenen zwölf Monaten mit 50 verschiedenen Phishing-E-Mails konfrontiert worden. Das sei eine Zunahme um 28 Prozent gegenüber den zwölf Monaten zuvor. 2,4 Millionen Internetnutzer haben den Angaben von Gartner zufolge bisher durch Phishing Geld verloren. Allein in den vergangenen zwölf Monaten seien 1,2 Millionen US-Bürgern 929 Millionen US-Dollar durch Phishing abhanden gekommen."
heise online 230605

... USA citizens e-commerce confidence is going down because of reports on stolen credit card data and more and more phishing says Gartner research company .....

This is what the user sees day in and day out in the media. Those are hard fact INCIDENTS and from real life. Is it surprising that the user becomes nervous and stays away from the Net?

This is not only a USA attitude. Europeans share the same views. This is confirmed by Forrester Research.

Factors that Would Persuade Internet Users in Europe to Start Using or Use More

Online Banking, 2005 (as a % of respondents who don't bank online regularly)

Guaranteed security	**34%**
Extra 2% interest for using online only	30%
If the nearest branch closed	15%
A 5% charge for using a branch teller	12%
If someone showed you how it worked	12%
If online banking was easier to use	11%
If there was a free telephone technical support	11%
Faster Internet access	11%
BDM News 031005 Source: Forrester Research, March 2005 Provided to Paul DiModica by eMarketer.com under contract.	

What about the authorities?

"Polizei registriert steigende Kriminalität beim E-Commerce"

"Die Polizei registriert einen steigenden Waren- und Warenkreditbetrug beim Handel im Internet. Im vergangenen Jahr seien auf dem Gebiet des E-Commerce in Deutschland 270.000 Straftaten verübt worden, teilte die Zentrale Geschäftsstelle der Polizeilichen Kriminalprävention der Länder und des Bundes am Dienstag in Stuttgart mit. Im Vergleich zu 2003 entspricht dies einer Zunahme von 45.000 Fällen. Bei 42 Prozent aller Straftaten handele es sich um betrügerische
heise online 160805

... The police confirms 114 thousand e-commerce fraud cases in Germany alone ...

"Der Diebstahl von Bank-Zugangsdaten verursacht in Deutschland Schäden in siebenstelliger Höhe."

Den 16 Landeskriminalämtern liegen mehr als Tausend Fälle vor, in denen im Zusammenhang mit betrügerischen Überweisungen von Online-Konten ermittelt wurde, wie FOCUS berichtet. Teilweise laufen die Verfahren noch.
Der geschätzte Schaden durch das so genannte Phishing summiert sich alleine in Deutschland auf 4,5 Millionen Euro.

Focus 231005

... Theft of bank access codes results in loss of tens of millions of Euro in Germany alone .....

And who is the loser? The **USER**?

“Banken nicht immer kulant”

”FOCUS ist allerdings ein Fall bekannt, in dem ein Geprellter vorerst auf dem Großteil seines Schadens sitzen bleibt. Einem Diplom-Ingenieur aus Bietigheim-Bissingen wurden mit einer Spionagesoftware die Zugangsdaten zu seinem Online-Konto entwendet und **4657** Euro gestohlen. Seine Hausbank will ihm lediglich **500** Euro erstatten.”
Focus 231005

… the banks are not always co-operative, 500 Euro compensation for 4.557 Euro theft…

All those examples are taken from the media, the media the people daily read and see. Those are most definitely incidents the user does not expect to experience or hear about. Those incidents make him insecure and keep him or her away from the Net. Consequences are: **THE INTERNET HAS GOT A BAD REPUTATION.**

What can be done? Let us look back at what the media are saying

---

Integralis again

„Häufigste Gründe für die ungenügendenSicherheitsmaßnahmen seien der stetige Kostendruck, mangelnde Ressourcen und Unwissenheit, so der IT-Security-Spezialist. "Die meisten Betreiber von Web-Shops unterschätzen die Bedrohung, der sie ausgesetzt sind, bei weitem", erklärt Matthias Straub, der E-Commerce-Experte von Integralis. In der Regel genügten fünf Minuten, um über einen gängigen Internet-Browser erste Sicherheitslücken eines Online-Shops auszuspähen. Außerdem scheuten viele Unternehmen die Kosten, um zusätzliche Sicherheitsmaßnahmen zu ergreifen. Die Vogel-Strauß-Mentalität sei hier weit verbreitet. "Tatsächlich bieten heute keine anderen IT-Systeme eine vergleichbar große Angriffsfläche auf niedrigstem Sicherheitsniveau", konstatiert Straub.“
COMPUTERWOCHE.de 270905

… cost cutting, lacking resources, underestimating threats …..

“SA-Konferenz:
Diskussion über die Frage zur Haftungsverantwortung bei Sicherheitsmängeln

Bruce Schneier, eine Größe im Bereich der Sicherheit, hielt bei der RSA-Konferenz in Wien eine Rede über die Frage, wer verantwortlich ist bei Sicherheitslücken. Seiner Meinung nach sind Softwarehersteller und Internet-Provider haftbar zu machen.

Nach Meinung von Bruce Schneier, dem „Sicherheits-Guru“, gehören Internet-Provider und Softwarehersteller zu den Verantwortlichen bei Sicherheitslücken und müssten entsprechend haftbar gemacht werden. So sein Fazit, das er jetzt in der Abschlussrede der RSA-Konferenz in Wien zog: „Derzeit tragen jene die Kosten für Sicherheitslücken, die unter ihnen leiden.“ Es herrscht nach Meinung Schneiers eine großer Missstand bei der Sicherheit von Unternehmen, denn in der Regel geben die Unternehmen Unsummen dafür aus, von Softwareherstellern verursachte Sicherheitslücken zu flicken oder abzufangen.

Auch Privatpersonen müssten sich selbständig um die Sicherheit ihrer Rechner kümmern. Nicht zuletzt würden auch Regierungen damit belastet, Anwender weiterzubilden, damit diese den Umgang mit häufig benutzerunfreundlicher und unsicherer Software in den Griff bekommen. Unverständnis ernten die Softwareunternehmen, die die Vielzahl verfügbarer technischer Lösung zur Sicherheitssteigerung nicht anwenden – deshalb sei es an der Zeit, mit gesetzlichen Regelungen die Softwareunternehmen in die Pflicht zu nehmen bzw. vor Gericht zur Rechenschaft zu ziehen. Ähnlich soll es, so Schneier, Internet-Providern ergehen.
Doppelklicker.de 241005

.... who is responsible for security holes? ....
..... Software producers and Internet Service Providers should be made liable ....
... users have to become self-reliant.....
... governments are responsible for educating users.....

Conclusion: Incidents include both business and technical issues. They need to be resolved by the industry, voluntarily or not. I will come back to this point later.

Is that all? No by all means.

The media again

"Phishing-forsøg mod Nordea kom fra Korea"
"To falske Nordea-hjemmesider er sporet til Korea under efterforskningen af det store phishing-angreb på banken tidligere på ugen."
COMPUTERWORLD 051005

.. Nordea bank phishing attack came from Korea .....

"Bredbåndslande haler ind på spam-USA"
"USA er fortsat det land, hvor størstedelen af verdens spam-mails bliver udsendt fra. Fremstormende bredbåndsnationer som Sydkorea og Kina haler imidlertid ind på USA hjulpet frem af forældet Windows-software**."**
"Størstedelen af alle udsendte spammails kommer fortsat fra USA, men den amerikanske andel er kraftigt dalende, viser en opgørelse fra sikkerhedsfirmaet Sophos."

"Selskabet har opgjort 26 procent af det sidste halve års spam-mails til at komme fra systemer i USA."
COMPUTERWORLD 141005

... most of spam comes from USA but South Korea and China are picking up ...

This is definitely a global issue. Sweden has no jurisdiction over Korea. Sweden is a EU member. EU also has no jurisdiction over Korea. The perpetrators will probably never be brought to court. This is a global issue and can only be solved at that level. But it will take time. In the meantime users and businesses are the prey.

What can we do? Can we can start at home. Some examples from USA.

“Spam-Gesetzgebung in den USA zeigt Wirkung”

„.....Es sei deutlich zu beobachten, dass der rigide Umgang mit gefassten Spammern in den USA abschreckende Wirkung entfalte. "Provider, die untereinander Informationen zur Bekämpfung von Spam austauschen, sowie die Verabschiedung des CAN-SPAM-Gesetzes in den USA, haben in Nordamerika dazu beigetragen, die Aktivitäten der Spammer einzudämmen. Einige besonders eifrige Versender dubioser Werbe-Mails sahen sich dadurch sogar gezwungen, sich entweder aus dem Geschäft zurück zu ziehen oder ihren Standort in andere Länder wie China und Südkorea zu verlagern", erläuterte Jens Freitag von Sophos.“

„Kaum eine Rolle für die Spam-Belästigung spielen nach wie vor die europäischen ISPs. 3,46 Prozent stammen aus Frankreich, 2,22 Prozent aus Spanien und 1,55 Prozent aus Großbritannien. Deutschland ist mit 1,26 Prozent sogar Schlußlicht des Negativrankings.“
heise online 121005

... anti spam law in USA is showing effect .....

”**The state of California has passed the country's first antiphishing law, making this form of identity theft punishable by thousands of dollars in fines.”**

“The law, entitled the Anti-Phishing Act of 2005, was proposed by state Sen. Kevin Murray and signed into law on Friday.”

“Under the Anti-Phishing Act, these victims may seek to recover either the cost of the damages they have suffered or $500,000, whichever is greater; government prosecutors can also seek penalties of up to $2,500 per phishing violation.”
COMPUTERWORLD 241005

.... anti phishing law in California first for USA .....

The USA is a frontrunner when it comes to passing laws with the trend setting State of California paving the way. We have to wait and see how effective the anti phishing law will be.

We are in Europe. What are the Europeans doing? What is the EU doing?

Answer; Very little. **Practically nothing.**

In spite of all the incidents listed above we seldom see reports in the media about perpetrators being brought to justice and sentenced. And in the rare event the sentences are light, very light.

The only reports on severe sentences come from the USA. USA has the lead on the EU. Why is that?

The EU Commission does not seem to understand the seriousness of Internet incidents. It still looks at those incidents as pranks, something kids love and is a part of the growing up process. Something they grow out of, something like graffiti. European graffiti sentences are light. In California the mayor of Log Angeles according to media reports wants to hack off the fingers of the graffitiers.

We have conflicting laws in the EU. We have the Data Protection directive which causes conflicts. An example.

The CECUA server in the UK was hacked more than once. The CECUA General Secretary asked his Internet Service Provider who was hacking him. The Internet Service Provider answered that he could not tell him because of the Data Protection law. He should talk to the police. So he did. And the police told him to buy a firewall.

If the hacker had smashed the office door or broken a window and stolen something from the office the police would have been out in full force looking for the thief. That would have been a "real" break-in. But hacking is an intangible break-in and the police either feel it is a prank or they are not competent to handle it. So they take the easy way out.

We have an anti-spam directive, the opt-in compared to opt-out in the USA. But most of the spam comes from the USA or Korea or China anyway. Any serious spammer will move his operation out of the EU and into those jurisdictions. Again spamming is an international and global issue.

We have no anti-phishing directive yet. Has anybody heard if the EU planning it? Please tell me.

So what is the Commission doing? Anything?

What should be done? Let us go back to the experts.

Integralis again

…… cost cutting, lack of resources, threat underestimate …..

SA-Konferenz again

…. who is responsible for security holes? ….
… Software producers and Internet Service Providers should be made liable ….

Today anybody can set up an Internet Service Provider company and start selling. He can do as much cost cutting and underestimate the threats as he sees fit..

Also any company can sell its software and point fingers at the competition.

Should we require the Internet Service Providers to obtain a license, a license like airlines with requirements they must satisfy and also an overseeing authority? Would that be a way to raise the standard and at the same time make users less vulnerable to attacks? Would this reduce the number of incidents? Something to be looked into?

Should we do the same with software producers? Should we require them to have their products certified before they bring them to the market?

Some people will say that this is a step backward to introduce controls. Other will say that the market has failed and it is in public interest of regulate them. This is clearly something for the EU to do since most Europeans buy their Internet Services from European providers. It is a European issue.

But there is also an international or global issue involved. Let us go back once more.

... most of spam comes from USA but South Korea and China are picking up ...

EU member states obviously and EU also have no jurisdiction over USA, Korea or China. This is clearly a global issue which can only be resolved at the global or international level. The nations of the world need to sit down and discuss this issue and resolve it. The EU plays an important role here on behalf of the member states with several hundred million users. So do also USA, China, India, Korea, etc. But until the nations of the world have reached an agreement and are prepared to reinforce it incidents like spamming and phising etc. will continue to plague us. It is not enough that EU, USA, Korea and China agree. As long as there is one single nation staying outside the agreement the spammers and phisingers will simply move there and establish themselves outside of anybody's jurisdiction and continue to pursue their trade. Maybe the World Summit on the Information Society will be successful in solving this issue? Until then users will not have confidence in the Net and many will stay away from it with all its potential and wonderful opportunities.

Few words about CECUA.

CECUA was set up over 30 years ago with the encouragement of the European Commission to be a federation of national Computer User Associations from all member states of the European Union and the Council of Europe.

With widespread introduction of personal computers and the Internet, CECUA realized that all citizens were becoming "computer users" and also members of the Information Society. This process has mainly been driven by the IT&T industries with their own agenda. CECUA as the only independent European user organization has provided counter balance by promoting and advocating user issues from the user perspective at various levels, e.g. Commission, Committee of the Regions and European Parliament. The message has been well received and CECUA is an active member of the European Internet Foundation with an international high-level expert support group.

In 1997 CECUA formed an ICT Partnership with CEPIS, Eurochambres, YES, MIDEPH, EUIF in conjunction with ISPO of the European Commission, to run the highly acclaimed conference "**The Citizen and the Global Information Society**" in the Spring of 1998 in Brussels.

This Conference examined the fears, concerns and hopes of citizens in the global information society and as a result produced a draft "Bill of Rights for European Citizens" which set out many issues which needed to be addressed to create a safe and trustworthy Net for European Citizens to work and play. The term "citizen" here includes individuals and corporate citizens as well as governments, commercial interests etc.

The draft "**Bill of Rights**" was widely publicised in order to stimulate debate and to encourage major European players to co-operate and work together to create a safe Internet environment.

The main provisions of the draft "**Bill of Rights**" can be divided into three main areas:

- Security Issues (right for redress, the basic rights as a citizen, right of access to public information, right for secure access, data and information, freedom from

conduct which violates the rights of personal citizens, governments and moral values)
- Cultural Issues (the right to use one's own alphabet, to use one's own name)
- Administrative Issues (transparent charging, reliable and affordable service etc.)

Even though these issues were raised nearly six years ago, there has been very little progress. In fact the situation is much worse now. There is serious lack of Trust and Confidence.

In the late 1990s the Commission adopted the position that "Industry knows best" and very much left it to the industry to keep users informed. As we have seen above the industry has failed to live up to expectations. CECUA has struggled to keep independent and deliver the message on numerous conferences and seminars and from the CECUA website www.cecua.org

Information and Communication Technology is an integral part of the Lisbon agenda and network and information security are key issues. Users need to be prepared for incident experiences and how to deal with them. They need some assurances like the CECUA "Bill of Rights" introduced after the Conference in 1998. If they are not prepared they will lose faith in the network and information with serious consequences for us all.

While CECUA has been struggling very much alone in the past there could be a change in the wind.

Business paradigm shift: Transfer of service to customers to reduce costs

Business desperately wants to reduce costs to stay competitive in a global business environment. ICT has proven to be a very useful cost reduction tool in the past. Before year 2000 business invested a lot in new ICT to be sure of no year 2000 problems and also to improve business processes. Now they have gotten all they can out of that investment. Further cost reductions are only possible with further investment in ICT. People are a major cost item. They can cut down on people by letting customers do the work employees did before. With more ICT they can do it. This is of course not what their advertising says. Advertising emphasizes better service whenever you want it and wherever you are. For this to become a success they have to convince the masses of customers to make use of those new services. They have to overcome the lack of confidence of customers in the Internet. Business has become the new driver of the Internet. Business has good contacts to Commission, Committee of the Regions and the European Parliament and Member States Governments and would be able to initiate new approaches through new channels. Although they are not the real end users they are users of the Internet and real POWER users.

Back to the media.

„Studie: Aufklärung über sicheren Online-Handel dringend nötig"

„Im Online-Handel ist nach einer Studie die Aufklärung der Käufer über Sicherheitsmaßnahmen dringend nötig. Vor allem gelegentliche Nutzer sind in Sachen Sicherheit nur unzureichend informiert. Das ergab eine am Dienstag in Hamburg vorgestellte repräsentative Studie von TNS Infratest im Auftrag des Online- Auktionshauses eBay. "Dabei fehlt es zumeist an den grundlegendsten Dingen", sagte Jens Krüger, Direktor von TNS Infratest. Wenig-Nutzer seien deshalb anfälliger für Betrügereien, weil sie mit Sicherheitsmaßnahmen nicht vertraut sind.

Rund zwei Drittel der Befragten gaben allerdings an, sich mit dem Thema noch nicht richtig befasst zu haben. Dabei ist die Sicherheit bei Transaktionen im Internet für mehr als 90 Prozent der Nutzer

wichtig oder sehr wichtig. Dennoch sind 35,7 Prozent der Befragten keine Sicherheitsvorkehrungen bekannt. Bei gelegentlichen Internet-Käufern liegt der Anteil sogar bei 45,6 Prozent."
heise online 081105

... users need to be kept informed about the secure e-commerce .....

.... for more than 90% of users e-commerce security is very important ....

... about 40% of users know nothing about e-commerce self protection...

"eBay sieht Sicherheit als wichtigen Erfolgsfaktor"

"Auch in der virtuellen Welt kann es keinen 100-prozentigen Schutz vor kriminellen Aktivitäten geben. Deshalb ruft eBay seine Mitglieder zur Eigenverantwortung auf: "Die Menschen müssen lernen, dass es so etwas wie einen gesunden Internet-Verstand gibt", sagte Stefan Groß-Selbeck, Geschäftsführer von eBay Deutschland, heute auf dem Jahreskongress der Initiative D21 in Bremen"
heise online 241105

... for eBay security is a business critical success factor .....

..... in the virtual world there is no 100 % guaranty against criminal activities....

.... ebay calls for self-reliance .....

.... people must develop an Internet common sense.....

---

eBay is certainly among the new drivers and we welcome their involvement. Other new drivers include banks, insurances, etc., all real POWER drivers.

But to become really successful the stakeholders have to work together towards a common goal: **SECURE INTERNET ENJOYING TRUST AND CONFIDENCE OF THE USERS**.

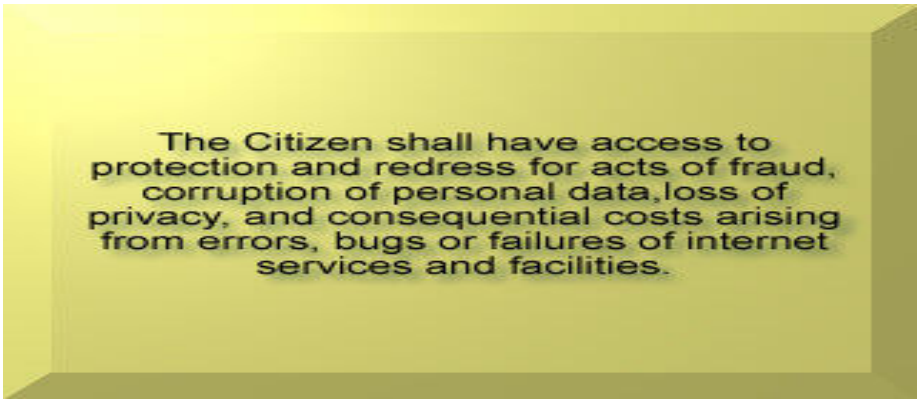
Let me recall the stakeholders:

Governments, Industry, Businesses, Users

The EU and the member states have an important role to play to bring them together and support their efforts. Also the European Parliament needs to be involved. The Commission needs to rethink their position and become proactive again, not only reactive.

ICT is an integral part of the Lisbon agenda and network and information security are key issues. Users need to be prepared for incident experiences and how to deal with them. They need some assurances like the CECUA "Bill of Rights" introduced after the Conference in 1998. If they are not prepared they will lose faith in the network and information with serious consequences for us all. That really would be a shame because the Internet and the Web are wonderful, not only for business, but also for education and leisure.

Let me finish by coming back to the Bill of Rights. The Bill of Rights is just as relevant now as it was in 1998. It has been used again and again to address user issues and to evaluate measures taken. For example it was used earlier to evaluate the Universal Services Directive and the results were presented to the Committee of the Regions. I would like to mention article 9, Right to Redress.



One of the many concerns the end users have is what to do in case they do not get delivered what they thought they were buying on the Internet. The seller can be in another country and subject to a foreign jurisdiction. How can the end user get his or her right? The users and the Power users need this issue to be resolved and ASAP. Until it is done there will be a serious lack of trust and confidence in e-commerce. Let us work together toward a common goal:

SECURE INTERNET ENJOYING TRUST AND CONFIDENCE OF ALL USERS