

## Pre-Reading

---

### *Internet Crime – Why should a CISO care?*



## SESSION 11

---

**Monday, September 8th, 2008 – 12:00 until 16:15**  
**Zürich**

---

An initiative to engage in strategic dialogue on IT security

**Microsoft**®      **accenture**  
*High performance. Delivered.*

Internet crime is an expression that covers a very wide area of criminal activities from phishing via identity theft and spamming on the customer side to exploiting software bugs via distributed Denial of Service attacks and targeted espionage on businesses. Internet threat reports state that internet crime has arrived at a stage, where these attacks are no longer executed by individuals in an opportunistic way, but are run by criminal organizations almost like businesses with financial interest. The increase in crime comes from technology based attacks, social engineering attacks and attacks focusing on the human/computer interface alike.

### Findings from the MELANI information assurance report

It is quite obvious that increased social engineering attacks and targeted espionage are topics that should be evaluated by a CISO and relevant actions should be taken, but what about the problems posed by organized crime (criminal syndicates) controlling Internet crime activity? Are these topics that require a CISO's attention and probably a change to the strategy or are the internet users and thus the customers out of scope for the CISO and organized crime is a topic for governmental activities but not for companies? Should a CISO care about these kinds of internet crime and the recent changes?

### Organized defense for an organized crime

Although threat reports like the semi-annual report from MELANI<sup>1</sup> are available, detailed information on successful or unsuccessful attacks is quite rare. This is because businesses want to keep this kind of information to themselves. For organized crime this is a big advantage, as the information exchange between enterprises is very limited. Attacks that have been successfully detected and prevented by one company might still work elsewhere. New attack patterns might be recognized too late, as a few events in one enterprise will not trigger an alert to others, but similar events across a large number of enterprises might do.

The value chain enterprises are incorporated in is also introducing new risks. Compared to the past the value chain and the number of incorporated enterprises have increased. Processes are heavily linked between different enterprises. Attacks at the value chain are affecting all dependant enterprises and one weak link might introduce a risk to all enterprises and thus giving the saying "one for all and all for one" a whole new meaning.

Does this mean organized crime should be tackled with an organized defense?

---

<sup>1</sup> <http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=en>

### Aviation Information sharing

Sharing information on defects and incidents is a common thing in the aviation sector. Looking at the rules of the aviation regulations from the United States, reporting certain kinds of defects is mandatory and in addition the Aviation Safety Reporting System (ASRS) also allows voluntary reporting of further defects and incidents, that will then be anonymously published to all aviation companies.

Having the collected information available will help to draw other conclusions than it would be possible with a single company's information alone, but taking this approach and applying it to internet crime is currently raising more questions than it solves. Some of the questions are:

- Will such a database provide any benefit for the businesses or is it just creating unnecessary costs?
- Which formal steps would be required to get the Board of Directors' approval to security relevant data?
- Which organization might be the right one to maintain such a database and to anonymize the data?
- How much (if any) incentives from government would enterprises see as beneficial?
- Which kind of governmental involvement should be absolutely avoided

At the next SSE event, we will discuss how and whether a solution similar to the ASRS database might apply to internet crime and where the obstacles are.

### Organized crime targeting end users

A CISO's responsibilities include ensuring information security within an enterprise and protecting the enterprise against financial risks from hacker attacks. Usually the line is quite clear where the responsibilities start and where they end. Will this have to change in the future due to the changes in internet crime? The focus of organized crime on the end user can be relevant in two aspects. End users might be customers or they might be employees.

### Targeting employees in their private life

Criminals can target employees of a company both at work and at home. Creating the link between the employee as a private person and as part of the enterprise is often very easy. For example a private email address might be used on community pages where the company name is listed as well, or the business email is used for a personal website. Being able to identify the employee as an end user and to attack him in his private life might expose the enterprise to new risks. Employees might be using identical or similar passwords privately and within the enterprise. An attacker who can capture the password in a private context might therefore be able to get access to enterprise information as well. Accessing company resources from a private computer might also allow an attacker to retrieve credentials. Especially *whaling* (e.g. "phishing" targeted at



executives) a new development where highly visible top executives are specifically targeted also need to be considered. Looking into these scenarios CISOs should reevaluate where the line between protecting the enterprise and protecting the employee exactly lies.

### **Organized crime targeting the customers**

Most internet users are not familiar enough with security to understand the attacks happening and the risks they are exposed to. When using websites of a company for business transactions or basic communication they rarely care about security implications or attack possibilities. Enterprises are aware of fines and liabilities from fraudulent credit card transactions. In addition further risks to the enterprise should be evaluated as well. Possible risks are loss of trust from the customers, lost customers, delayed or denied payments as well as involvement of the enterprise in criminal investigations.

Classifying and quantifying the risks is a complex issue and as such making a decision on how far customer protection must go is as well. How do the decisions and strategies of the CISOs change as attacks at end users are executed in an organized way? Is the risk drastically increased as a company might come into the focus of organized crime? Security Analysts like Bruce Schneier are challenging enterprises to see this as their responsibility<sup>2</sup>. But what can enterprises realistically do, and who draws the line between acceptable inconvenience and security?

### **Conclusion**

The recent developments in internet crime raise a number of questions that might challenge CISOs to look for new strategies or to start new alliances in defending their enterprises. Please join us in the upcoming SSE round table to discuss the challenges ahead and the impact this might have at the CISO agenda.

---

<sup>2</sup> <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9079720>

---

## Round Table discussion topics

The following list of topics will be discussed in the round table discussions.

### **Would a database comparable to the Aviation Safety Reporting System (ASRS) be beneficial for IT Security events?**

- Is there a similarity between the ASRS database and information sharing for security events?
- Which aspects covered in the ASRS database do not apply to security events?
- What content and information would such a database require to be beneficial?
- Would more information be beneficial at all and if so, to whom?
- Is there a benefit in alliances for security event sharing, combined strategies, technologies?

### **If a database like the ASRS Database does exist, where would be the obstacles implementing it?**

- Information sharing is most times limited by company policies. Where would such a database conflict with existing company policies?
- Which rules does the body who owns the database need to apply to?
- What would be required, to change the enterprises mind on security event information sharing?
- What would be required to convince the board of directors to allow such cooperation?

### **Where is the line in responsibility for internet crime regarding the customers?**

- Which risk is an enterprise exposed to if the customers are exploited?
- Where does the responsibility of a CISO to protect the customers end?
- Can customers be protected at all?
- How can the costs of an attack be measured so that the balance between invested money in countermeasures and risks can be established?
- Which responsibilities should be covered by government?

### **Where is the line in responsibility for internet crime regarding employees?**

- Is there a risk to the enterprise if an employee is exploited, for example if the enterprise password is used for a private account as well?
- Where does the responsibility of an enterprise end in protecting the employees?
- Which measures have been taken to prevent targeted social engineering?
- Do Web 2.0 applications that link the employee to the enterprise (like XING) extend the risk to, the enterprise?

---

## THE WORKSHOP

The primary goal of this Swiss Security Exchange session is to discuss the findings from the MELANI semiannual report and evaluate the relevance for CISOs.

The workshop is structured into the following main parts.

- 1. Welcome lunch and networking**
- 2. Introduction** by Laura Koetzle, Vice President, Forrester Research
- 3. MELANI - findings from the semi-annual Report** by Marc Henauer, Head of MELANI/Cybercrime
- 4. Work session I** – Round table Discussions as outlined
- 5. Group discussion of the results from work session I followed by an interactive group wrap up**
- 6. Closing and Apéro**

**Christian Georg**

Accenture, Content Advisor Swiss Security Exchange

**Urs P. Küderli**

Microsoft, Content Advisor Swiss Security Exchange

**Prof. Dr. Bernhard Hämmerli**

Acris, Content Advisor Swiss Security Exchange



## **BUSINESS DECISION MAKERS CONFIRMED FOR September 8th**

---

<b>Surname</b>	<b>Forename</b>	<b>Company</b>
Ameri	Amir	UBS AG
DiLena	Patrik	Raiffeisen
Gerber	Markus	Hilti Corporation
Gourinchas	Olivier	Hilti Corporation
Grab	Heribert	Siemens
Haering	Kurt	EFSI AG
Hörler	Andreas	Schweizerische Nationalbank
Koch	Stéphane	Intelligentzia
Lubich	Hannes P	British Telecom
Maher	KAMAL-RIZK	Scor
Mayencourt	Nicolas	dreamlab
Olsen	Rainer	Credit Suisse Group
Schenk	Marc-André	Nestlé
Small	Mike	CA
Toggweiler	Daniel	The Swatch Group LTD
Trenta	Giampaolo	Julius Baer & Co. Ltd
Winzer	Ralf	Helsana
Wuchner	Andreas	Novartis Pharma AG
Ziegler	Pius	KPMG Switzerland



---

## ORGANIZATION

### Executive Producers Swiss Security Exchange:

**Christian Georg** Accenture GmbH  
**Rene Hanselmann** Microsoft GmbH

### Facilitator:

**Laura Koetzle**, Vice President, Forrester Research

Laura primarily contributes to Forrester's offerings for the Security and Risk professional. She is an expert on operating system security, security architecture, network security, and security incident response, and she chairs Forrester's Security Forum event in the Americas.

Previously at Forrester, Laura served as research director for both the Security and Risk Management and the IT Operations and Infrastructure research teams.

Laura works with Forrester's clients to solve technical, strategic, and organizational IT security problems. She has redesigned network topologies, created new IT security incident response procedures, and reorganized IT security groups.

Laura's work has enjoyed wide exposure in the media, including *The New York Times*, *The Wall Street Journal*, *BusinessWeek*, and *The Economist*. Laura has also appeared on CNN, CNBC, CBC, and National Public Radio, and she is a frequent speaker at national and international executive conferences.

### Previous Work Experience:

Prior to joining Forrester, Laura was a senior technologist at Razorfish, a New York consultancy, where she led teams of software developers responsible for eCommerce fulfillment systems, wireless content delivery applications, and real-time trading system interfaces for Fortune 500 clients. Before working at Razorfish, Laura built XML content management systems at PC World Communications in San Francisco. While living in Buenos Aires, Argentina, Laura worked as a translator.

### Education:

Laura holds an A.B. in literature and a certificate in Latin American studies from Harvard University. She also attended the University of Buenos Aires.