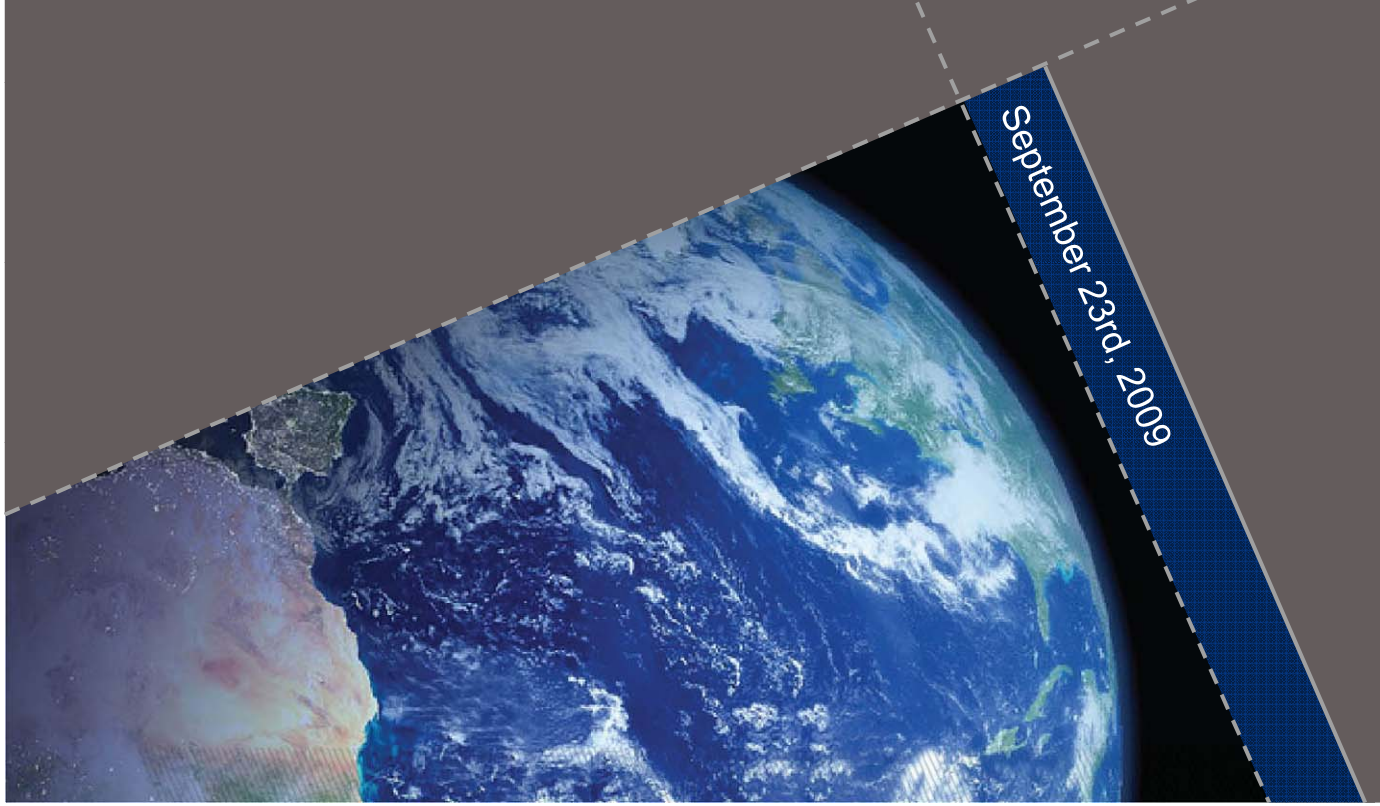
Cyber-insurance: a financial perspective to incident response

VB 2009

Geneva



CHARTIS

Agenda

One of the goals of (IT) Security is to maintain business tools and resources of a company, to preserve the making of profit and turnover, not for the lack of security per se

- ✓**Business Dependency**
- ✓**Recent Cases (extortion, Vx infection)**
- ✓**Insurance basics**
- ✓**Underwriting Process**
- ✓**Cost assessment**

Pascal LOINTIER
Regional Information Systems Risks Adviser, CHARTIS
President, CLUSIF
+ 33 (0)6 72 69 38 24
Pascal.lointier@chartisinsurance.com

Cybercrime Trends, reminder

CHARTIS

✓Professionalization

Range and amount of attacks (cf. Bugbear virus, Anserin Trojan and banks)

✓Commercialization

Customized tools (Trojan Horses, botnets)

Web sales (keyloggers, credit cards, personal data, etc.)

…

✓Sophistication

Exploit processing: FastFlux, Mpack, Domain tasting abuse…

Tools *designed for* criminal/profitable activity and not only for “hacking” (cf. RBN)

Do not forget…

CHARTIS

✓**Recurrent blunders and (threat of) personal data disclosure**

Lost laptops, CDs, USB sticks…

✓**Business dependency**

We are leaving in an Information Society (Administration, Corporate, Citizen)

> At least 4 Information Systems:

- Management, Outsourced, SCADA and industry IT networks, VoIP…

> and personal data disclosure penal and commercial risks

✓**Different ways to process a risk**

Acceptance

Mitigation

Transfer (cyber-insurance, complementary to ITsec policies)

Avoidance

Recent case: Payment Terminal Fraud

CHARTIS

✓New England (USA), March 2008. Hannaford a grocery store chains discovers a credit card breach.
Around 4.2 million numbers were hacked (card number, expiry dat but not the cardholder name). The information obtained was sent overseas.
The breach began in December. 300 servers were affected, in stores in Florida (106), New England (165) and in franchises (24).
Consequences

1.800 proven cases of fraud over the course of March

Re-issuing fees for approx. 100,000 cards

$5 million class action suit led by a firm law

Millions of dollars invested in security: encryption of data in transit, 24-hour monitoring system

Hannaford compliant with the PCI-DSS standard… which was quickly modified to account for the operating mode!

Recent case: Data theft and Ransom Demand

CHARTIS

- **✓Saint-Louis (USA), November 2008. Express Scripts a company which manages medical prescription information is blackmailed via e-mail (threat to release 75 patient files, information on millions of patients is stored on database).**
- **✓Ransom amount is not disclosed to the public but as some consequences**

Creation of a crisis website to inform patients and manage complaints

Identity restoration service offered by consultant/security firm

Commitment to pay any monetary losses

Use of an investigation firm

$1 million reward offered helped to catch the blackmail artists!

Recent Case: Virus infection

CHARTIS

✓**Lille (France), June 2007. An IT contractor infects the local network using a crack software on a USB stick.**
IT staff tried to fix the problem during week-end, at first by themselves then with help of a local software supplier (not an AV specialist)… but local network of the headquarter of this company will stay down for the whole next week…
5 days out of work for all employees (hundreds of people).

Initial loss assessment is € 500k...

Recent Case: Virus infection

CHARTIS

✓**London (UK), September 2009. « An Ealing council employee infected the UK local authority's IT systems with the Conficker-D worm after he plugged an infected USB into a work computer …**

incident took several days to clean-up and landed the west London council with a bill of £500,000 in lost revenue and repairs, … Because IT systems were borked, the council was unable to process more than 1,800 parking tickets, at an estimated cost of £90,000, libraries lost out on £25,000 in fines and booking fees, council property rent went uncollected, and £14,000 was spent in overime sorting out delayed housing benefit claims…

Costs to the council included urgent work to recover computer systems and prevent the virus from spreading »

(http://www.theregister.co.uk/2009/09/04/ealing_council_mystery_malware/),

Consequences, 1st assessment

CHARTIS

✓**Direct damage:**

Restoration costs for data, resources, etc.

✓**Collateral damage:**

Salaries (extra hours), expert fees, etc.

✓**Indirect damage:**

Lack of profit, penalty fees, notoriety, loss of contracts…

✓**Possible legal and 3rd party damage:**

Penal code, specific regulations, class action suit…

✓**Unexpected budget for security improvement (the good point ☺)**

Cyber-insurance 101: insurance rules

CHARTIS

- ✓Occurrence should be hazardous
- ✓No profit for insured (just refunded to previous asset amount)
- ✓Cause of loss and perimeter of cover must be defined in agreement
- ✓Initial Loss Estimate (insured asset amount) based on probable loss (cf. “reasonable”, “maximum” cause of loss)
- ✓Prejudice has to be quantified by Insured (i.e. potential issue for consequences of theft/data disclosure)

Handicaps…

✓**No financial impact assessment by many companies**

No financial dashboard for security incident for around 70% of SMI-SMB in France (cf. CLUSIF “Information Systems Threats and Security Practices in France, 2008 Edition”, www.clusif.fr)

✓**Lack of information sharing within a company between people in charge of ITsec and Financial Department (except to address security budgets ☺)**

✓**Simple vision of impact or insurance use: « just to restore the data… just to patch the backdoor.. Just to refund the victimized customers… »**

Cyber-insurance 101: to rephrase…

CHARTIS

✓Insurance as a financial tool to be refunded of

Restoration costs

Business impact

✓Insured covers (some of…)

1st risk direct damage to insured

- (hardware (property), intangible assets)

3rd Party liability

✓Cause of Loss

Accidental

>Natural or industrial event (e.g. fire)

>Error (data manipulation)

Malevolent

✓Underwritten options: direct loss (restoration), indirect losses (business impact)

Cyber-insurance 101: options

Basics

- Data restoration (the basement…)
- Extra Expenses
  - Restoration (extra hours, trip and accommodation)
  - Production (more expensive means for production)
- Business Interruption (lack of profit)
- Fraud (financial assets, goods and equipments) and overbilling
- Ransom (extortion)
- Professional liability
- Property (hardware)

Extras

- Expert fees
- Penalty fees (contractual liabilities)
- Loss of benefits from interest (or interest to be paid)
- Supplier deficiency (same cause of loss)
- Outsourced processing cover (“pour le compte de”)
- Investigation costs
- Crisis communication and image reconstitution

…

In accordance with domestic regulations and/or underwritten cover

Underwriting process

CHARTIS

✓Only one simple question “what if…Information System is done?” (without assuming about security counter-measures)

✓Information sharing between CFO (or Business Units Managers), RM (Risk Manager in charge of insurance covers), CISO, CIO

✓4 steps process

- Identify core business (cf. initial goals of ITsec, to preserve activity)
- IT dependency (immediate, >24h, no serious Business Interruption)
- IT Architecture description
- Security policies (tools, procedures, *incident response*)

✓Insurance proposal (cf. “variables”, next slide)

Cyber-insurance: Underwriting parameters

- ✓**Domestic regulations**
- ✓**Expected insurance options b/o Customer**
- ✓**Exclusions** **(standard clauses, lack of security practices (e.g. BCP for BI))**
- ✓**Risk assessment**
  - Security practices (and financial audits and controls)
  - Incident Response and mitigation process
- ✓**Security requirements** **(backup, antivirus, password, etc.)**
- ✓**Coverage variables**
  - Asset amount (and/or insured cashflow)
  - Perimeter
  - Deductible
  - Exclusion
  - … Premium

Cyber-insurance: fraud cases average range € 20k – millions…

CHARTIS

- ✓Tampered PC (control cable installed during a fake robbery) and bank transfer of millions of € (stopped)
- ✓Physical keylogger, €400m (stopped ☺)
- ✓Forged fund transfer signature
- ✓Phishing activity (“2nd generation”) and compromised PCs, $1.1m bank refunds 250 customers
- ✓$50,000 in micro-payments, eTrade

Fraud matrix (indicative)

CHARTIS

FRAUD	"standard"	usual	seldom
DIRECT & INDIRECT LOSSES			
Data & Service restoration			✓
Discovery/investigation		✓	
Extra Expenses (crisis management)	✓		
Extra Expenses (production)			✓
Business Interruption			✓
Brand and Notoriety		✓	
Hardware and IT infrastructure			n/a
Financial Fraud (refunding)	✓		
Cyber-extortion (ransom)		✓	
Lack of Supplier / Outsourcing			✓
Penalty Fees			✓
.../...			
SERVICES			
Expert Fees	✓		
Pre Loss Analysis		✓	
Post Loss Mitigation Measures		✓	
.../...			

In accordance with domestic regulations and/or underwritten cover. Indicative scenario and impact

Cyber-insurance: virus success stories range € 20k – 1m w/o Business Interruption assessment

CHARTIS

- ✓**Developer's laptop, infected in Australia… major impact for file servers in western Europe (CodeRed)**
- ✓**USB stick with a crack software… infected, 5 days out of work for all employees in HQ**
- ✓**Botnet, dDoS and ransom**

Virus matrix (indicative)

CHARTIS

VIRUS	"standard"	usual	seldom
DIRECT & INDIRECT LOSSES			
Data & Service restoration	✓		
Discovery/investigation		✓	
Extra Expenses (crisis management)	✓		
Extra Expenses (production)		✓	
Business Interruption		✓	
Brand and Notoriety			✓
Hardware and IT infrastructure			n/a
Financial Fraud (refunding)			✓
Cyber-extortion (ransom)			✓
Lack of Supplier / Outsourcing			✓
Penalty Fees			✓
.../...			
SERVICES			
Expert Fees		✓	
Pre Loss Analysis		✓	
Post Loss Mitigation Measures	✓		
.../...			

In accordance with domestic regulations and/or underwritten cover. Indicative scenario and impact

Cyber-insurance: internal sabotage range € 100k – millions… w/o BI assessment

CHARTIS

- ✓Logic bomb
- ✓Zombies and compromised PCs to disrupt stock prices
- ✓Massive Data deletion
- ✓SysAdmin and withheld passwords… pending case

Sabotage matrix (indicative)

CHARTIS

INTERNAL SABOTAGE	"standard"	usual	seldom
DIRECT & INDIRECT LOSSES			
Data & Service restoration	✓		
Discovery/investigation	✓		
Extra Expenses (crisis management)	✓		
Extra Expenses (production)			✓
Business Interruption			✓
Brand and Notoriety		✓	
Hardware and IT infrastructure			✓
Financial Fraud (refunding)			✓
Cyber-extortion (ransom)		✓	
Lack of Supplier / Outsourcing			✓
Penalty Fees			✓
.../...			
SERVICES			
Expert Fees	✓		
Pre Loss Analysis			✓
Post Loss Mitigation Measures	✓		
.../...			

In accordance with domestic regulations and/or underwritten cover. Indicative scenario and impact

Cyber-insurance: extortion range €100k – 1M

CHARTIS

- ✓dDoS threat via e-mail then execution (ransom of €100k not paid), prejudice €150k, 3 weeks of interruption
- ✓Cyber-espionage, selling trade secrets
- ✓Unlocking Bank databases, $200k

Extortion matrix (indicative)

CHARTIS

EXTORTION	"standard"	usual	seldom
DIRECT & INDIRECT LOSSES			
Data & Service restoration			✓
Discovery/investigation	✓		
Extra Expenses (crisis management)	✓		
Extra Expenses (production)			✓
Business Interruption			✓
Brand and Notoriety		✓	
Hardware and IT infrastructure			✓
Financial Fraud (refunding)			✓
Cyber-extortion (ransom)	✓		
Lack of Supplier / Outsourcing			✓
Penalty Fees			✓
.../...			
SERVICES			
Expert Fees	✓		
Pre Loss Analysis			✓
Post Loss Mitigation Measures		✓	
.../...			

In accordance with domestic regulations and/or underwritten cover. Indicative scenario and impact

Insurance contribution to RoSI

CHARTIS

✓RoSI definition

Various ones, no magic formula as a result

✓Purpose

To justify

To orientate

To prioritize: compliancy and/or (?) security

CLUSIF

Menaces informatiques et pratiques de sécurité en France

Edition 2008

Club de la Sécurité de l'Information Français

✓Clusif' French National Survey, 2008

Lack of financial impact analysis (French SME)

End-user security awareness a minima (as for new employee training, training efficiency assessment)

✓Possible Contributions via incident analysis

Prevention

Mitigation

Crisis Management Costs

Financial losses

Cyber-insurance: conclusions

✓**Post loss analysis** **(Financial impact dashboards, again…)**

✓**Check that your insurance broker is « computer literate », otherwise no taste for cyber-extortion, dDoS, etc.**

✓**Look for an insurance company, "computer literate" too and do not only focus on premium but**

Range of cover (cause of loss and asset amount)

Risk understanding (helping to mitigate)

… to prevent any denial "that was not the intent of the cover": mutual clear understanding of insured losses scenarios

Cyber-insurance: conclusions - 2

CHARTIS

✓**Existing solutions** available from large (and specialized) insurance companies

✓Pre-mandatory **information sharing** between Risks Managers, CEO, CIO, CISO…

✓Covers (have to be) adapted/**customized** to fit specific requests and/or expectations

✓**Dynamic process**: business increase (and related financial needs), rising threats, evolving exposures and solutions