2016 SGPC Annual Conference
2016/09/29 Paris

Welcome… in the bunker where internet started!

Denis Kessler
CEO, SCOR SE

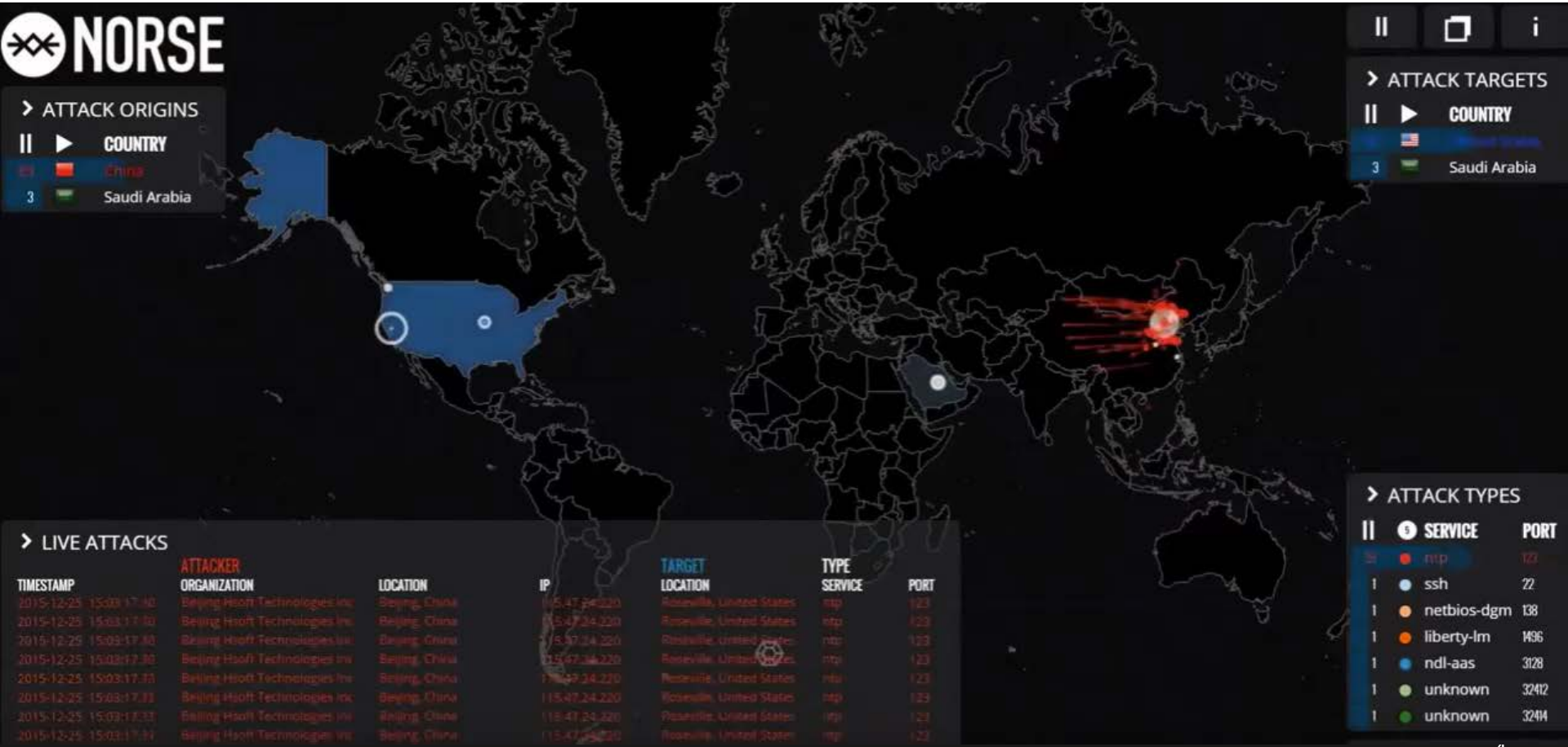
SCOR
The Art & Science of Risk

Acts of God, Acts of Man, Acts of the Devil: The risk universe is expanding

SCOR
The Art & Science of Risk

Early this morning, a regular day on the internet

25 december 2015



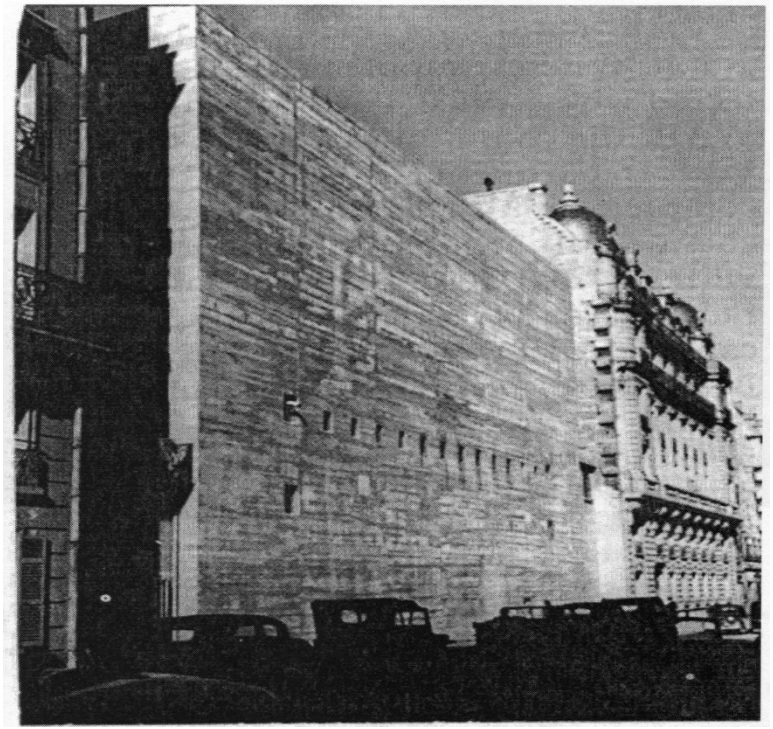
1 **The Cyberspace – A man-made environment that has deeply transformed the society and the economy**

2 Cyber Risk characteristics - So present and so unknown

3 How do I think about Cyber as CEO of a reinsurance company?

SCOR
The Art & Science of Risk

The Cyberspace started here!



SCOR building in 1944

29, rue la Pérouse

- During World War II, this place was known as as the German Signal Blockhouse
- After Liberation, the 805th US Army Signals Detachment installed SIGSALY, a 50 tons voice encryption system for direct encrypted links to London and Washington

This Auditorium, with a SIGSALY terminal in 1945

SCOR
The Art & Science of Risk

Source: John D. Paul

Cyberspace: A man-made environment inherently vulnerable

- Cyberspace is a man-made environment created in the late 60's
- Security was not a primary concern

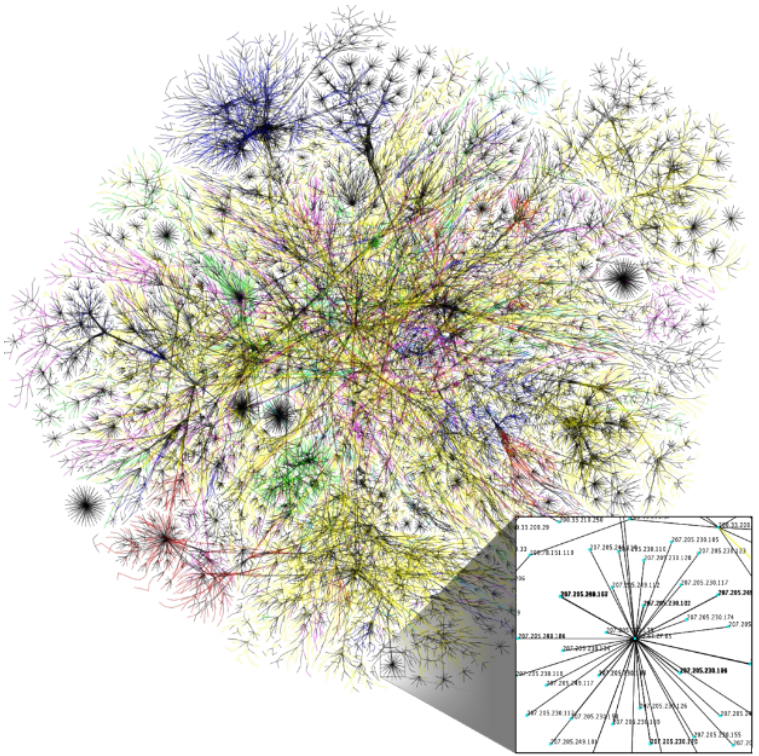
September 1981

Internet Protocol
Introduction

The Options provide for control functions needed or useful in some situations but unnecessary for the most common communications. The options include provisions for timestamps, security, and special routing.

Internet Protocol Definition (1981): security is an unnecessary option

- First « virus »: 1988, the Morris Worm
  - Infected 10% of the Internet
  - US Government Accountability Office estimated damages at $100 000 - $ 10 000 000



A portion of Internet routes by The Opte Project

SCOR
The Art & Science of Risk

Cyberspace has deeply transformed the society and the economy

- In less than 60 years, digital technologies have deeply transformed our societies
- The global economy benefits from digitalization
  - Traditional business sectors transformed by digital innovations (e.g. banking)
  - New business sectors have emerged (e.g. online gaming – market volume of $35B in 2013 and forecast of $56B in 2018)
  - Growth of intangible assets (volume & value)

Social Networks


Connected Health

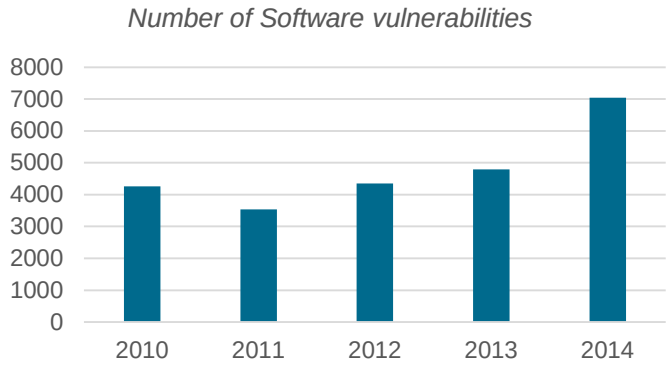

Connected Cities

Connected Cars

SCOR
The Art & Science of Risk

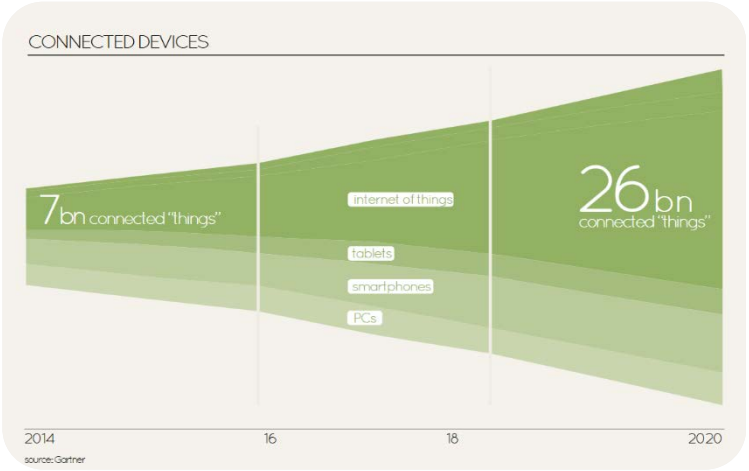
Digitalization creates new vulnerabilities

- The value of intangible assets is increasing
  - Branding, reputation
  - Intellectual Property (e.g. Defense, Pharma)



Source: National Vulnerability Database

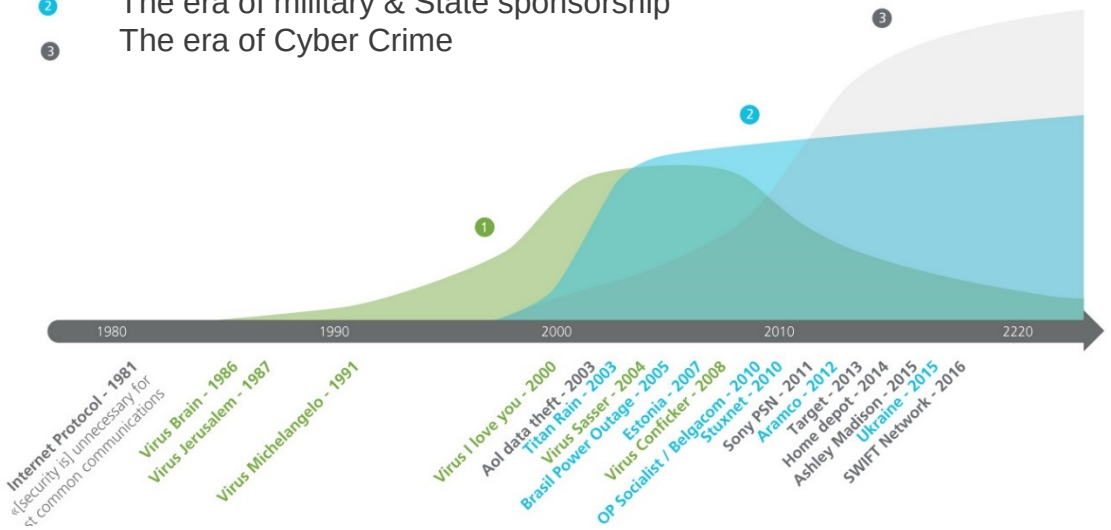
- The attack surface is growing:
  - Connected objects (e.g. cars, planes, power stations)
  - Connected services (e.g. mobile banking, tax payment)



SCOR
The Art & Science of Risk

Since Internet inception, cyber threats have constantly increased

1. The era of viruses
2. The era of military & State sponsorship
3. The era of Cyber Crime



Global Drug Trafficking

$411B per year

Cyber crime

$388B per year

Nat Cat

$130B per year

- Attackers are well organized
- Efficient defenses are difficult to implement

1) *Norton Symantec report 2012 - http://uk.norton.com/cybercrimereport/promo*

1 The Cyberspace – A man-made environment that has deeply transformed the society and the economy

2 **Cyber Risk characteristics - So present and so unknown**

3 How do I think about Cyber as CEO of a reinsurance company?

SCOR
The Art & Science of Risk

Cyber risks are recent and developing very fast

- Only 25/30 years, with little historical data
  - No regular reporting on cyber breaches
  - No organization empowered to collect, anonymize and build statistics with cyber breach data
- However, initiatives are being implemented in the US, the UK, France…
  - US Dept. of Homeland Security: Cyber Information Sharing and Collaboration Program
  - UK Cyber-security Information Sharing Partnership
  - FR Law on critical infrastructure protection

Evolution of Cyber threats, BAE System Applied Intelligence

CSP A CATALYST FOR COLLABORATION

SCOR The Art & Science of Risk

Cyber risks are pervasive

Cyber has consequences on all risks and all business lines

Business interruption	*Contingent business interruption*	*Data and software loss*
Cyber ransom and extorsion	*Intellectual property theft*	*Incident response cost*
Network Security	*Reputational damage*	*Regulatory & Legal Defense costs*
Communication and media misuse	*Legal protection*	*Assistance coverage*
Claims against Directors and Officers	*Environmental damages*	*Physical asset damage*
Financial theft and/or Fraud	*Breach of privacy*	*Bodily injury and death*

CRO Forum Concept Paper on a proposed categorization methodology for cyber risk

And yet there is very little certainty on these consequences

- Invisible and delayed effects
  - Most cyber attacks have no physical consequences
  - Median number of day before detection: 229
  - Cyber attacks can be anonymously performed from anywhere
- Sophisticated cyber attacks are stealthy (cyber espionage) and difficult to detect until it is too late.
- 66% of cyber attacks are discovered by external parties.
- A risk without borders: no frontiers, no specific business sectors, no size are immune to cyber risks - all organizations are exposed, everywhere.

SCOR
The Art & Science of Risk

Cyber risk has severe impacts

Financial impact

Other Banks may have been affected

SWIFT, the financial network

2015: Hackers stole **$12m** from Ecuador's Banco del Austro

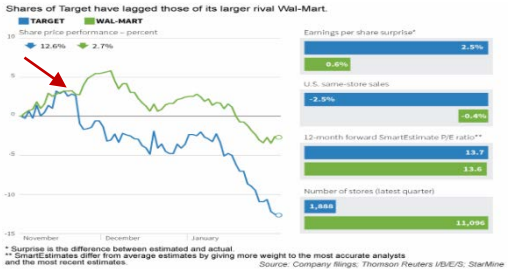
Feb. 2016: Hackers stole **$81m** from Bangladesh national bank

Impact on infrastructure

December 2015: A carefully designed cyber attack caused a power outage in Ukraine. 3-6h of black-out impacting 80.000 homes

The black-out was short because technicians were able to switch back to manual mode and restore power

Impact on reputation and governance



- Target's share price drops after 40m credit card numbers and 70m personal information stolen by hackers in 2013
- CEO Fired

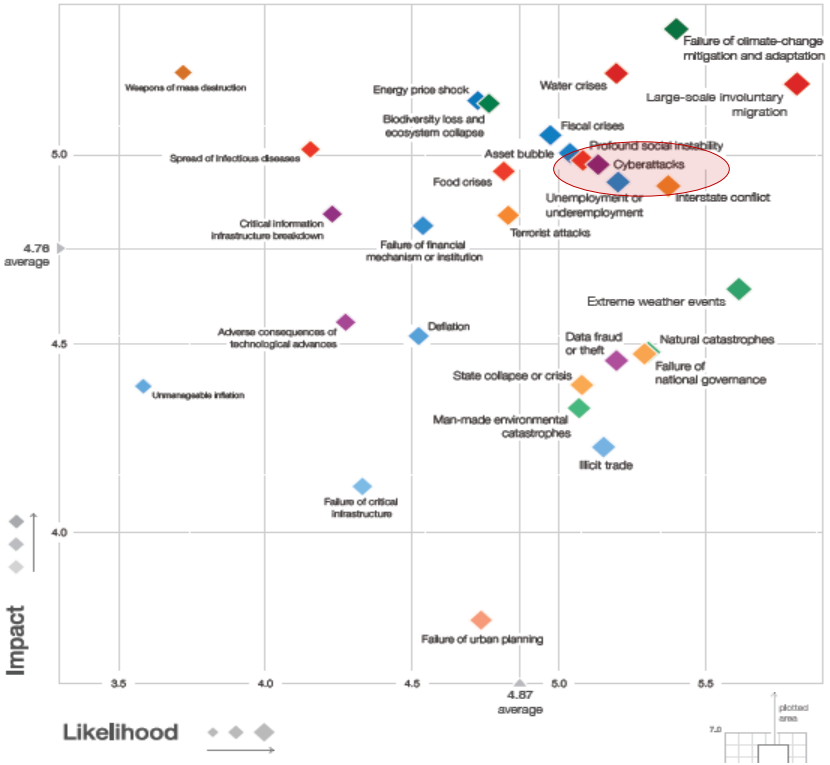
While both lines trace the difficulties in the retail sector the separation observed illustrates just how damaging a cyber event can be.

SCOR
The Art & Science of Risk

As interconnections and digitalization increase, are « cyber catastrophes » more likely?

Which scenarios for a cyber catastrophe?

- Cyber risks has high impact and likelihood, above terrorist attacks and not so far away from large scale involuntary migration!
  - WW concentration of IT providers (Microsoft Windows market share: 90%)
  - Massively and increasingly interconnectedness
- Catastrophes could result of attackers targeting
  - Core systems (SWIFT, Oracle, Google…)
  - Key infrastructures
  - Key databases



World Economic Forum Global Risk Report 2016

1. The Cyberspace – A man-made environment that has deeply transformed the society and the economy
2. Cyber Risk characteristics - So present and so unknown
3. **How do I think about Cyber as CEO of a reinsurance company?**

SCOR
The Art & Science of Risk

What keeps me awake at night?

	Key expectations	How can SCOR manage its exposure to cyber risk?
Clients	Clients expect SCOR to protect their critical data	Know and monitor SCOR's cyber exposure and cyber breach scenarios
Regulators	Regulators have strong requirements on personal data security	Ensure cyber protection means are commensurate with the threat
Investors	Investors expect SCOR to efficiently protect against cyber attacks causing operational or reputational damages	Implement a high and identical level of protection across SCOR Group and efficient business continuity planning
Rating agencies	Rating agencies expect SCOR to have a very strong cyber operational risk management	Ensure that SCOR is ready to deal with a cyber crisis. Adequate investments to update protection systems

Who is driving the decision?

Source: Lloyd's cyber survey report – Aug 2016

REUTERS

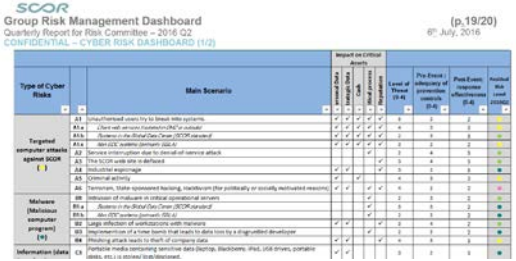
September 13th, 2016 - New York Governor Andrew Cuomo on Tuesday issued long-anticipated proposed **cyber security regulations for banks and insurers in the state**, the first of their kind in the United States by any state or federal agency, the governor said in a statement.

SCOR
The Art & Science of Risk

SCOR's exposure to cyber risk is well managed

SCOR consistently improves its Cybersecurity

- Already in 2012, SCOR started a major program to enhance its cyber security: the "Data Protection Program"
- SCOR produces a Cyber Risk dashboard, shared with the Risk Committee of the Board


SCOR
Group Risk Management Dashboard
Quarterly Report for Risk Committee – 2016 Q2
CONFIDENTIAL – CYBER RISK DASHBOARD (1/2)
(p.19/20)
6th July, 2016

Type of Cyber Risks		Main Scenario	Impact on Critical Assets: Data unrelated to Clients	Impact on Critical Assets: Clients' Data	Impact on Critical Assets: Critical process	Impact on Critical Assets: Reputation	Level of Threat (0-4)	Pre Event : adequacy of prevention controls (0-4)	Post Event: response effectiveness (0-4)	Residual risk Level (CCS/QC)
Targeted computer attacks against SCOR	A1	Unauthorised users try to break into systems.	✓	✓	✓	✓	4	3	3	
	A1a	*Client-web servers hosted in UNIQ or outside*	✓	✓	✓	✓	4	3	3	
	A1b	*Systems in the Global Data Center (SCOR standard)*	✓	✓	✓	✓	3	3	3	
	A1c	*Non-GDC systems (primarily SSG-4)*	✓	✓	✓	✓	4	3	3	
	A2	Service interruption due to denial-of-service attack				✓	3	4	3	
	A3	The SCOR web site is defaced				✓	3	4	3	
	A4	Industrial espionage	✓	✓		✓	3	3	3	
	A5	Criminal activity	✓		✓		4	3	3	
	A6	Terrorism, State-sponsored hacking, Hacktivism (for politically or socially motivated reasons)	✓	✓		✓	4	3	3	
Malware (Malicious computer program) [*]	B	Intrusion of malware in critical operational servers				✓	4	3	3	
	B1a	*Systems in the Global Data Center (SCOR standard)*				✓	3	3	3	
	B1b	*Non-GDC systems (primarily SSG-4)*				✓	3	3	3	
	B2	Large infection of workstations with malware	✓	✓		✓	4	3	3	
	B3	Implementation of a time bomb that leads to data loss by a disgruntled developer				✓	3	3	3	
	B4	Phishing attack leads to theft of company data	✓	✓		✓	4	3	3	
Information (data	C1	Portable media containing sensitive data (laptop, Blackberry, iPad, USB drives, portable media, etc.) is stolen/ lost/destroyed.	✓	✓			3	3	3	

Cyber Protection Systems

- SCOR has implemented systems and security tools meeting financial sector standards
- In addition to this, SCOR's IT network is continuously controlled by a *Security Operation Center* under CIO's responsibility

SCOR is protected by Cyber insurance cover

- Depending on the type of event affecting SCOR's data and systems, the insurance program covers SCOR's own damages, third party liability and costs and services related to crisis management

SCOR
The Art & Science of Risk

Challenges have to be met to benefit from the (re)insurance growth opportunity that cyber represents

Opportunities

- ✓ Become an actor of the fast growing (re)insurance market
- ✓ Bring tangible solutions to clients
- ✓ Leverage digitalization to enhance SCOR's operations
- ✓ Improve knowledge of intangible risks

Challenges to overcome

- Need to raise cyber expertise in the market
- Improve Risk Management process & quality of information provided to risk carriers
- Collect data & Build risk models
- Manage risk aggregation and exposure to Cyber Cat

1) Footnote