Technical Book 2015

Information Systems Committee

CYBER RISKS

A guide to risk assessment and insurance solutions

In partnership with CESIN

AMRAE L'ASSOCIATION

About the AMRAE

Risk Management has considerably evolved over the last number of years. The strategic, operational, financial, social, security and legal risk dimensions are continuously changing, and hence the limits of their insurability. Prevention, retention levels, reduction, protection or risk transfer to an insurer are some of the possible strategies to be considered within Risk Management.

Given the current economic climate, analyzing risks and learning to manage them has become crucial in providing competitive advantage.

AMRAE (The Association for Corporate Risk and Insurance Management) has consolidated itself since its creation in 1993 to become today a benchmark reference for enterprises. It has around 1,000 members from 700 private or public organizations.

AMRAE helps these enterprises in their strategic and operational initiatives and their performance through the management of their risks.

AMRAE Association brings together the key actors of the risk profession - Risk Managers, managers of risks from internal control and internal audit including legal and insurance functions. Through its scientific committees, its publications and numerous specific events, AMRAE produces, for these experts, methods to develop their performance and their professional evolution, in order to help them to better serve their enterprise's strategy.

With AMRAE Training, the Association provides their professional training needs via high-level certified degrees.

AMRAE Meeting organizes the annual risk conference, attended by over 2,200 professionals. These three days constitute the essential 'rendez-vous' for the risk management profession and their financing partners.

About the CESIN

The CESIN "Association of Information and Digital Security Experts" is a so-called "Association loi 1901" that was founded in July 2012 for the purpose of professionalization, promotion, and sharing in the field of information and digital security.

The CESIN is an information and experience sharing organization that fosters cooperation between information and digital security experts and between the latter and government bodies.
The CESIN sponsors workshops and working groups, carries out awareness raising activities, provides advice, and organizes conferences, colloquia and congresses.

The CESIN participates in well thought-out activities in France aimed at promoting information and digital security. The organization also drafts possible laws, guides and the like.

The CESIN has around 200 members from all areas of activity comprising the following: active members, who are in charge of information and digital security in their respective organizations; associate members; representatives of various government authorities in charge of nationwide information and digital security; jurists who are experts in the field of ICT (information and communication technology) security.

We would like to take this opportunity to thank all those who have contributed to the realization of this manual.

We would like to thank the following: the members of the Cyber Insurance working group, which works under the aegis of AMRAE's Information Systems Committee; risk managers from the banking, industrial, and service sectors, among others; CESIN members who helped develop this manual; and in particular the following individuals:

- François Beaume, Chair of the AMRAE Information Systems Committee, Deputy Group Risk Manager and Insurance Director, Bureau Veritas

- Alain Bouillé, President of the CESIN

- Hélène Dubillot, Senior Scientific Coordinator for AMRAE

- Fabrice Morgaut, Insurance and Risk Manager, Transdev

- Pascal Richard, Head of Non-Life Insurance, Société Générale

We would also like to thank the insurance brokers who allowed for updating of the state of the market in Appendix 2 of this document.

Table of contents

Editorial

Dear AMRAE members,

The issue of digital-risk management has become ever more pressing in recent years. Not a week goes by without an illustration of the reality of this problem surfacing in the media.

Apart from the operational-impact dimension of the problem, recent events have underscored that, in the wake of attacks by cyber criminals, the responsibility of certain business leaders and their organizations has been called into question. For other companies, this type of risk has in fact resulted in their demise.

These risks are undermining current boundaries, in that company information systems and the data of which they are composed are being increasingly externalized in the cloud, using a chain of providers comprising a mixture of co-contractors and subcontractors that are external to the companies in question. This in turn is eliminating the relevant physical and geographical boundaries, and is complicating the task of delegating responsibility. This profound change in the landscape of company information systems and the new usage modalities resulting from this change has given rise to new so-called cyber risks.

These changes are forcing risk managers in particular to take into account the consequent additional complexity when it comes to the risk assessments carried out by such managers with the relevant corporate entities. It is essential that risk managers learn as much as possible about the ins and outs of this new complexity, in collaboration with the heads of departments such as the information system department, information security department and data privacy department.

Unlike liability and damage risks, covering these new risks will require the insurance industry to make certain changes. Managing these risks – which today is done via constellations of specific types of insurance that is referred to as cyber insurance – will also entail a redefinition of the boundaries between the various insurance sectors.

In light of this new situation, in early 2014 the AMRAE Information Systems Committee established a joint working group with the CESIN "Association of Information and Digital Security Experts", for the purpose of defining a methodology and creating a tool and practices that will help risk managers and various information system stakeholders to accomplish the following:

- Identify and assess cyber risks in light of the actual cyber risk landscape.
- Identify currently available risk mitigation instruments.
- Analyze the solutions offered by current insurance products.

- Define the possible need for additional cyber insurance cover.

The present document contains the results of these activities, along with an update of the state of the cyber insurance market.

We trust that you will find this manual useful. We would welcome the opportunity to discuss with you any feedback you have about using it, so as to continue to optimize the methodology proposed here.

Yours sincerely,

François Beaume

Chair of the AMRAE Information Systems Committee

Goals and methodology

Having been established in early 2014 under the aegis of the AMRAE Information Systems Committee, the Cyber Insurance working group is composed of risk managers from the banking, industrial, service, and high-tech sectors (among others), as well as an information system security manager member of the CESIN ("Association of Information and Digital Security Experts").

The main goal of this working group was to define the general cyber insurance needs of companies. The group's work was initially carried out via the sharing of experiences among its members, followed by realization of a survey of partner insurance brokers concerning their take on the following:

- Cyber risk;

- The needs of businesses for cyber insurance;

- The overall state of the cyber insurance market.

The information that was gathered formed the basis for the realization of cyber risk assessment matrix and for the assessment of enterprise insurance coverage. This first step was necessary in order to then determine the extent of the need for specific cyber insurance, and to define the scope of such insurance.

The multi-disciplinary nature of these assessments, which need to fold in risk management as a function of information systems in their diverse dimensions, makes their realization a complex undertaking. This first phase aimed to identify actual cyber risks, to quantify the impact of such risks, and to describe the currently available means for mitigating them.

Using this initial assessment as a starting point, the working group then investigated, with the relevant in-house specialists, which additional preventive measures could be implemented in order to, if possible, mitigate the incidence and/or intensity of cyber risk.

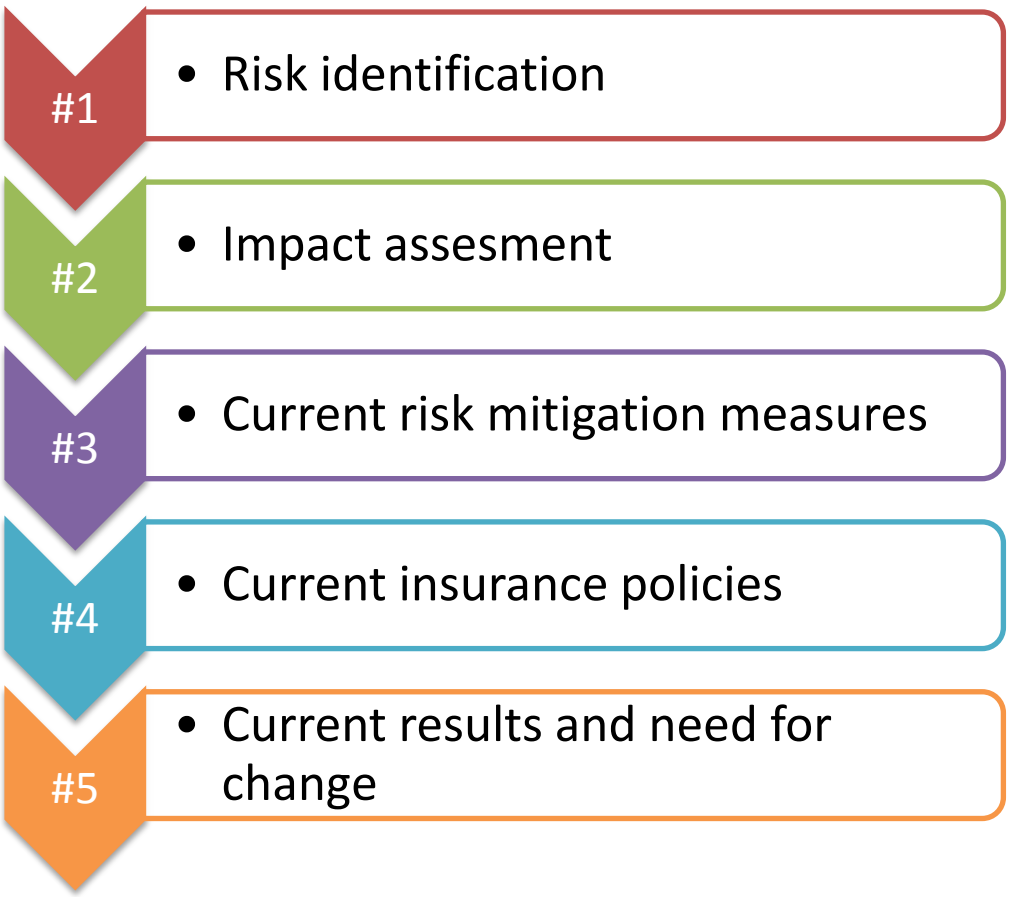
This initial assessment also allowed for the following: definition of the coverage (in terms of damages, liability and the like) that can potentially be provided by current insurance policies; and determination of the need for additional coverage that could potentially be provided by cyber insurance policies.

Cyber risk assessment matrix

The working group's work culminated in the realization of an Excel matrix (see Appendix 1).

This table is intended as a tool for risk managers that will enable them to lay the groundwork for a precise assessment of the cyber risks faced by their respective organizations. This table is available to AMRAE members as a download in the *Commission Systèmes d'Information* section of the AMRAE website's *Espace Membres*.

The table is built around five key phases:



Phase 1: risk identification

Risk identification involves precise description of an indicative list of cyber risks scenarios that the company may potentially face. This list, which was based on exchanges within the working group, of course needs to be customized, amended or augmented, depending on the risk landscape of the company in question, its areas of activity, and the geographical areas in which these activities are carried out.

Each risk needs to be objectified in order to render it understandable in an identical fashion to the various assessment stakeholders.

In the interest of ensuring optimal understanding of cyber risks scenarios, each term that is used should be explained and conveyed to company information system and risk management specialists, and the same term should always be used for each such concept. The exchanges that took place within our working group showed how crucial it is to arrive at a shared understanding of each term that is used, in order to allow for scenario sharing.

Phase 2: impact assessment

In this phase, the impact typologies of each risk are listed. This impact description is divided into two parts:
- Impact on individual insured parties (i.e. the entities forming the object of the assessment),

- Impact on third parties.

A financial evaluation of the types of impact that were identified is then added to this description.

Phase 3: current risk mitigation measures

This phase centers around current risk management and mitigation measures and/or measures of this type that are deemed necessary. These measures are also described.

What is essentially involved here is drawing up a list of the preventive and protective measures that have already been implemented within the company. This allows for the following: "refinement" of the impact intensity assessment; moving on to quantification of the impact of residual risks; and making the connection with the current cover described in phase 4.

Phase 4: current insurance policies

This phase enables risk managers to describe the cover provided by the company's current insurance policies. The following types of policies need to be described during this phase:

- Property Damage and/or Business Interruption (PDBI)
- Comprehensive General liability and/or Professional liability

- Fraud
- Other (depending on the particularities of the company being assessed)
- Cyber insurance

This phase is realized by indicating the following for each identified risk and each policy listed:

- Costs and expense items covered,
- Costs not covered by these policies, but which could be covered by providing a benefit,
- "Ideal" limits amounts,
- The limits of current policies.

Phase 5: current results and need for change

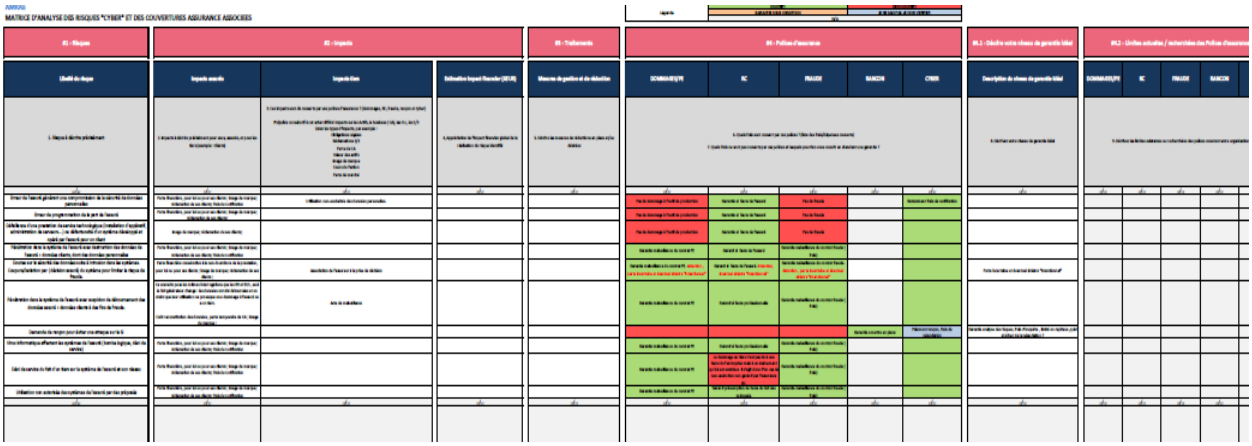
This phase (not included in the risk assessment matrix) involves an assessment synthesis that allows the efficiency of current financing and risk mitigation solutions to be called into question, as follows: Is this system suitable and as efficient as planned?

The response to such questions may potentially culminate in the realization of one or more action plans, for the purpose of either augmenting or optimizing current risk management/risk mitigation measures – the goal being to adjust the benefits and limits of current policies, or to provide a dedicated "cyber" benefit whose scope will be defined using the results of the assessments described above.

Conclusion

The aforementioned phases comprise key phases in the Excel risk assessment matrix, which we created in order to enable risk managers to better assess their needs.

A facsimile of this table (see screenshot below) can be found in Appendix 1. AMRAE members can download the table from the *Commission Systèmes d'informations* section of the *espace membre* on the AMRAE website.



The field of cyber insurance coverage is expanding nearly as quickly as cyber risks themselves – an evolution that demonstrates the rapid growth of demand in this market. Hence, our working group will continue with its work, at a minimum in order to ensure the continued relevance of the present manual, and to keep it updated.

Other issues such as the following remain to be addressed as well: implementation of cyber insurance policies in multinational corporations; structuring cyber insurance policies in such a way that they meet the needs of risk managers; the possible involvement of captives in underwriting cyber risks (only 1% of current captives underwrite cyber risks, according to Aon Global Risk Consulting's 2014 Captive Benchmarking Tools).

Appendix 1: Matrix

A facsimile of the Excel risk assessment matrix can be found in the pages that follow.

AMRAE members can download the table from the *Commission Systèmes d'informations* section of the *espace membres* on the AMRAE website.

Phases 1 and 2:

characterization of risks and the impact thereof (risks 1 through 5)

	1. Risks	2. Impact		
Ref.	**Risk name**	**Insured impacts**	**Impact on third parties**	**Estimated financial impact (in euros)**
Explanation of the table	1. Risk to be precisely described	2. Impacts to be precisely described on you, insured parties, and third parties (e.g. customers)	3. Are these impacts covered by your damage, liability, fraud, ransom, and cyber insurance policies? Damage resulting from this deferred purchase. Impact on assets, revenue, legal obligations, and one third claims. List the following types of impacts, for example: legal obligations; one third claims; revenue loss; asset value; brand image; share price; market share loss	Assessment of the overall financial impact in case of realization of the identified risk
R1	Impossible to use debit cards in stores, owing to, for example, the collapse of telecommunication networks.	Merchants' lost sales, and loss of bank commissions	Deferred purchase: damage resulting from non-purchase (e.g. missed sales or promotions; not possible to exit parking lot; revenue loss; customer claims)	
R2	Publication of malicious or defamatory information in the digital media of an insured party (e.g. websites, intranet, blogs, Facebook)	Damage to the company's reputation; revenue loss; share price decrease	In cases where a website is used to harm a third party: liability lawsuit for inadequate site monitoring; calls for a boycott; criminal penalties. Revenue loss; customer claims; brand image/e-reputation	
R3	Attack on third party companies by a party that hacks into the insured systems.	Damage to the company's reputation; revenue loss; share price decrease	Liability lawsuit for inadequate site monitoring; calls for a boycott; criminal penalties. Revenue loss; customer claims; brand image.	
R4	Hacker steals information from an insured party (e.g. a copy of the insured party's customer database)	Notification expenses; customer claims; downtime; brand image; calls for a boycott; loss of revenue to competition; debit-card replacement costs	Fraudulent use of company's data; identity theft; false payments; fraud; etc.	
R5	Copy of usable data such as debit card data	Notification expenses; customer claims; extortion attempts; brand image; calls for a boycott	Fraudulent use of company's data; identity theft	
.../...	--	--	--	--

Phases 1 and 2:

characterization of risks and the impact thereof (risks 6 through 15)

	1. Risks	2. Impacts		
Ref.	**Risk name**	**Insured impacts**	**Impact on third parties**	**Estimated financial impact (in euros)**
Explanation of the table	1. Risk to be precisely described	2. Impacts to be precisely described on you, insured parties, and third parties (e.g. customers)	3. Are these impacts covered by your damage, liability, fraud, ransom, and cyber insurance policies? Damage resulting from this deferred purchase. Impact on assets, business, legal obligations, one third claims. List the following types of impacts, for example: legal obligations; one third claims; revenue loss; asset value; brand image; share price; market share loss	Assessment of the overall financial impact in case of realization of the identified risk
--	--	--	--	--
R6	Fraud attributable to the vulnerability of information systems hosted and/or managed by a facility manager	Financial loss resulting from fraud, or from claims by the insured party or on behalf of their customers; brand image	Fraudulent use of company's data; identity theft	
R7	Non-availability of the information system and the service that the facility manager provides for the insured party, following an accidental event affecting IT hardware	Financial loss (for the insured party or their customers) resulting from service downtime; brand image; customer claims		
R8	Breakdown/failure (without material damage) affecting IT hardware and/or the insured party's IT infrastructure installations, potentially causing changes in or destruction of third party data by the insured party.	Financial loss (for the insured party or their customers) resulting from service downtime; brand image; customer claims	Apart from design-basis problems and design flaws	
R9	Doubts about data security following material damage incurred by production equipment on the insured party's premises, or on the premises of a provider/facility manager	The data may no longer be reliable, and it is feared that its use will harm the insured party or a third party Impact: data reconstitution costs; additional costs; temporary revenue loss; brand image	Coverage of all data reconstitution expenses	
R10	Strikes, riots or popular movements causing the destruction of the infrastructure of an insured party, a designated hosting services provider, or a designated facility manager	Financial loss (for the insured party or their customers) resulting from service downtime; brand image; customer claims; material damage	Financial loss (for the insured party or their customers) resulting from service downtime; brand image; customer claims; material damage	
R11	Insured party error that compromises the security of personal data	Financial loss for the insured party or its customers; brand image; customer claims; notification expenses	Unauthorized use of personal data	
R12	Programming error on the part of the insured party	Financial loss for the insured party or its customers; brand image; customer claims		
R13	Failure of a technological service (e.g. insured-party application; server administration) or defect in a system developed and operated by the insured party for a customer	Brand image; customer claims		
R14	Insured party's system is hacked, resulting in destruction of their data and of their customers' data, including personal data	Financial loss for the insured party or its customers; brand image; customer claims; notification expenses		
R15	Doubts about data security after the systems are hacked. The insured party decides to shut down/isolate the system, in order to limit the risk of fraud.	Financial loss (for the insured party or their customers) resulting from service downtime; brand image; customer claims	Insurer involved in the decision making process	
--	--	--	--	--

Phases 1 and 2:

characterization of risks and the impact thereof (risks 16 through 20)

	1. **Risks**	**2. Impacts**		
Ref.	**Risk name**	**Insured impacts**	**Impact on third parties**	**Estimated financial impact (in euros)**
Explanation of the table	1. Risk to be precisely described	2. Impacts to be precisely described on you, insured parties, and third parties (e.g. customers)	3. Are these impacts covered by your damage, liability, fraud, ransom, and cyber insurance policies? Damage resulting from this deferred purchase. Impact on assets, business, legal obligations, one third claims. List the following types of impacts, for example: Legal obligations; one third claims; revenue loss; asset value; brand image; share price; market share loss	Assessment of the overall financial impact in case of realization of the identified risk
R16	Insured party's system is hacked, resulting in suspected misuse of the insured party's data and of customer data, for fraudulent purposes	This scenario raises the same issues as those for R9 through R15: the data is misused and it is feared that this misuse will result in damage to the insured party or a third party: the data has been misused and may no longer be reliable; it is feared that its use will harm the insured party or a third party Data reconstitution costs; temporary revenue loss; brand image	Malicious act	
R17	Ransom demand in exchange for refraining from attacking the information system			
R18	Virus affecting the insured party's systems (logic bomb, denial of service)	Financial loss for the insured party or its customers; brand image; customer claims; notification expenses		
R19	Denial of service attributable to a third party in the insured party's system or network	Financial loss for the insured party or its customers; brand image; customer claims; notification expenses		
R20	Unauthorized use of the insured party's systems by subcontractors	Financial loss for the insured party or its customers; brand image; customer claims; notification expenses		
…				

Phases 3 and 4: descriptions of preventive/protective measures; risk financing via insurance (risks 1 through 7)

	1. Risks	Risk management	4. Insurance policies ,				
Ref.	**Risk name**	**Management and mitigation measures**	**Damage/business interruption**	**Liability**	**Fraud**	**Ransom**	**Cyber**
Explanation of the table	1. Risk to be precisely described	5. Describe mitigation measures that are currently in place or that are desired.	6. Which expenses are covered by these policies (list of (expenses/costs covered)? 7. Which expenses are not covered by these policies, and which ones could you cover by providing a benefit? **LEGEND:** *GREEN = BENEFIT* *RED = NO BENEFIT* *BLUE: Unknown; to be verified*				
R1	Impossible to use debit cards in stores, owing to, for example, the collapse of telecommunication networks.		By the following in particular: - The maliciousness benefit under the business interruption contract, if the shutdown is attributable to a malicious act; provider default benefit in cases of attributable/non-attributable material damages to provider production equipment	Provider liability (bank, EIG, access provider) can be contractually limited; damage attributable to non-purchase is indirect	No data theft or misuse occurred, but it is not possible to enter data; exclusion of debit card from bank's fraud contract		The cyber insurance contract calls for a business interruption benefit, if the event is a cyber-event, i.e. if security is compromised
R2	Publication of malicious or defamatory information in the digital media of an insured party (e.g. websites, intranet, blogs, Facebook)		Maliciousness benefit of the business interruption contract	Benefit in the event of professional misconduct; cleanup costs	The malicious act does not affect any insured-party asset		The cyber contract only provides a benefit in the event of an attack on existing data, and not on added data. To be negotiated.
R3	Attack on third party companies by a party that hacks into the insured systems.		Maliciousness benefit of the business interruption contract; machine breakdown		The malicious act does not affect any insured-party asset		
R4	Hacker steals information from an insured party (e.g. a copy of the insured party's customer database)		No production equipment is destroyed; nor is any data destroyed or stolen , in the penal-code sense of the term	Benefit in the event of negligence on the part of the insured party's data protection entity	The data is not stolen in the penal-code sense of the term. To be indicated in the maliciousness section.		Reconstitution expenses
R5	Copy of usable data such as debit card data		No production equipment is destroyed; nor is any data destroyed or stolen , in the penal-code sense of the term	Benefit in the event of negligence on the part of the insured party's data protection entity	The data is not stolen in the penal-code sense of the term. To be indicated in the maliciousness section.		Limited business interruption coverage
R6	Fraud attributable to the vulnerability of information systems hosted and/or managed by a facility manager		Fraud is not covered by the business interruption policy	Benefit in the event of negligence on the part of the insured party's data protection entity	Fraud benefit covering fraud involving the insured's data that is stored on the facility manager's premises		Can cover facility manager fraud
R7	Non-availability of the information system and the service that the facility manager provides for the insured party, following an accidental event affecting IT hardware		Extension of business interruption (whether attributable or not) coverage to include provider default	Third-party damage is not attributable to company negligence, but rather to an event external to the company. Hence this is a case of non-execution that is not covered by liability insurance.	No fraud		Benefit for information system failure to be extended to include the facility manager

Phases 3 and 4: descriptions of preventive/protective measures; risk financing via insurance (risks 8 through 15)

	1. Risks	Risk management	4. Insurance policies				
Ref.	**Risk name**	**Management and mitigation measures**	**Damages/business interruption**	**Liability**	**Fraud**	**Ransom**	**Cyber**
Explanation of the table	1. Risk to be precisely described	5. Describe mitigation measures that are currently in place or that are desired.	6. Which expenses are covered by these policies (list of (expenses/costs covered)? 7. Which expenses are not covered by these policies, and which ones could you cover by extending a benefit? **LEGEND:** *GREEN = BENEFIT* *RED = NO BENEFIT* *BLUE: Unknown; to be verified*				
R8	Breakdown/failure (without material damage) affecting IT hardware and/or the insured party's IT infrastructure installations, potentially causing changes in or destruction of third party data by the insured party.		Material damages (whether attributable or not)	Third-party damage is not attributable to company negligence, but rather to an event external to the company. Hence this is a case of non-execution that is not covered by the liability insurance.	No fraud		Benefit for information system failure
R9	Doubts about data security following material damage incurred by a production tool on the insured party's premises, or on the premises of a provider/facility manager		Expenses for data reliability research; expenses for the reconstitution of data deemed unreliable	If the reliability of the data is restored, in principle no further third party claims will be possible.	No fraud		Provider benefit
R10	Strikes, riots or popular movements causing the destruction of the infrastructure of an insured party, a designated hosting services provider, or a designated facility manager		Please note that strikes and popular movements are excluded.	Please note that strikes and popular movements are excluded.	No fraud		Please note that strikes and popular movements are excluded.
R11	Insured party error that compromises the security of personal data		No damage incurred by production equipment	Benefit in the event of insured-party negligence	No fraud		Notification expenses in particular
R12	Programming error on the part of the insured party		No damage incurred by production equipment	Benefit in the event of insured-party negligence	No fraud		
R13	Failure of a technological service (e.g. insured-party application; server administration) or defect in a system developed and operated by the insured party for a customer		No damage incurred by production equipment	Benefit in the event of insured-party negligence	No fraud		
R14	Insured party's system is hacked, resulting in destruction of their data and of their customers' data, including personal data		Maliciousness benefit of the business interruption contract	Benefit in the event of insured-party negligence	Maliciousness benefit of the fraud contract (expenses)		
R15	Doubts about data security after the systems are hacked. The insured party decides to shut down/isolate the system, in order to limit the risk of fraud.		Maliciousness benefit of the business interruption contract Please note: uncertain loss and possible "intentional" accident	Benefit in the event of insured-party negligence Please note: uncertain loss and possible "intentional" accident	Maliciousness benefit of the fraud contract Please note: uncertain loss and possible "intentional" accident		
--	--	--	--	--	--	--	--

Phases 3 and 4: descriptions of preventive/protective measures; risk financing via insurance (risks 16 through 20)

	1. Risks	Risk management	4. Insurance policies				
Ref.	**Risk name**	**Management and mitigation measures**	**Damages**	**Liability**	**Fraud**	**Ransom**	**Cyber**
Explanation of the table	1. Risk to be precisely described	5. Describe mitigation measures that are currently in place or that are desired.	6. Which expenses are covered by these policies (list of (expenses/costs covered)? 7. Which expenses are not covered by these policies, and which ones could you cover by extending a benefit?				
R16	Insured party's system is hacked, resulting in suspected misuse of the insured party's data and of customer data, for fraudulent purposes		Maliciousness benefit of the business interruption contract	Benefit in the event of professional misconduct	Maliciousness benefit of the fraud contract (expenditures)		
R17	Ransom demand in exchange for refraining from attacking the information system					Benefit to be implemented	Ransom payment, negotiation expenses
R18	Virus affecting the insured party's systems (logic bomb, denial of service)		Maliciousness benefit of the business interruption contract	Benefit in the event of professional misconduct	Maliciousness benefit of the fraud contract (expenditures)		
R19	Denial of service attributable to a third party in the insured party's system or network		Maliciousness benefit of the business interruption contract (whether attributable or not)	Third-party damage is not attributable to company negligence, but rather to an event external to the company. Hence this is a case of non-execution that is not covered by the liability insurance.	Maliciousness benefit of the fraud contract (expenses)		
R20	Unauthorized use of the insured party's systems by subcontractors		Maliciousness benefit of the business interruption contract	Benefit for presumed negligence by subcontractors	Maliciousness benefit of the fraud contract (expenses)		
....	--	--	--	--	--	--	--

Phase 4: Ideal limits amount; limits that currently come into play (risks 1 through 7)

	1. Risks	Indicate your ideal benefit amount	4.2 Current/desired limits for insurance policies				
Ref.	Risk name	Description of ideal benefit amount	Damages/business interruption	Liability	Fraud	Ransom	Cyber
Explanation of the table	1. Risk to be precisely described	8. Indicate your ideal benefit amount	9. Describe the existing or desired limits for your organization's current insurance policies				
R1	Impossible to use debit cards in stores, owing to, for example, the collapse of telecommunication networks.						
R2	Publication of malicious or defamatory information in the digital media of an insured party (e.g. websites, intranet, blogs, Facebook)	Image-loss benefit Crisis management contracts					
R3	Attack on third party companies by a party that hacks into the insured systems.	Cleanup expenses; investigation expenses, special cyber damages benefit? Special business interruption benefit without damages					
R4	Hacker steals information from an insured party (e.g. a copy of the insured party's customer database)	Business interruption without damages (or entailing intangible damages)					
R5	Copy of usable data such as debit card data	Business interruption without damages (or entailing intangible damages)					
R6	Fraud attributable to the vulnerability of information systems hosted and/or managed by the facility manager						
R7	Non-availability of the information system and the service that the facility manager provides for the insured party, following an accidental event affecting IT hardware						
--	--	--	--	--	--	--	--

Phase 4: Ideal limits amount; limits that currently come into play (risks 8 through 13)

	1. Risks	Indicate your ideal benefit level	4.2 Current/desired limits for insurance policies				
Ref.	**Risk name**	**Description of ideal benefit amount**	**Damages/business interruption**	**Liability**	**Fraud**	**Ransom**	**Cyber**
Explanation of the table	1. Risk to be precisely described	8. Indicate your ideal benefit amount	9. Describe the existing or desired limits for your organization's current insurance policies				
--	--	--	--	--	--	--	--
R8	Breakdown/failure (without material damage) affecting IT hardware and/or the insured party's IT infrastructure installations, potentially causing changes in or destruction of third party data by the insured party.						
R9	Doubts about data security following material damage incurred by a production tool on the insured party's premises, or on the premises of a provider/facility manager						
R10	Strikes, riots or popular movements causing the destruction of the infrastructure of an insured party, a designated hosting services provider, or a designated facility manager						
R11	Insured party error that compromises the security of personal data						
R12	Programming error on the part of the insured party						
R13	Failure of a technological service (e.g. insured-party application; server administration) or defect in a system developed and operated by the insured party for a customer						
.../...	--	--	.../...	--	--	--	--

Phase 4: Ideal limits amount; limits that currently come into play (risks 14 through 20)

	1. Risks	Indicate your ideal benefit level	4.2 Current/desired limits for insurance policies				
Ref.	**Risk name**	**Description of ideal benefit amount**	**Damages/business interruption**	**Liability**	**Fraud**	**Ransom**	**Cyber**
--	--	--	--	--	--	--	--
R14	Insured party's system is hacked, resulting in destruction of their data and of their customers' data, including personal data						
R15	Doubts about data security after the systems are hacked. The insured party decides to shut down/isolate the system, in order to limit the risk of fraud.	Uncertain loss and possible "intentional" accident					
R16	Insured party's system is hacked, resulting in suspected misuse of the insured party's data and of customer data, for fraudulent purposes						
R17	Ransom demand in exchange for refraining from attacking the information system	Benefit for the following: risk assessment; investigation costs; capital limits. What happens if negotiations break down?					
R18	Virus affecting the insured party's systems (logic bomb, denial of service)						
R19	Denial of service attributable to a third party in the insured party's system or network						
R20	Unauthorized use of the insured party's systems by subcontractors						
...							

Appendix 2: State of the cyber insurance market

Extent of coverage improving continuously (up 30%)

Virtually all insurers offer a combination of damage and liability coverage. Competition is intense between insurers that cover damages and those that cover liability. The coherence of insurer responses has improved in multi-layer schemes and for co-insurance. Insurers offer property damage coverage that is more suitable for major risks such as business interruption and provider deficiency. Sublimit ceilings have been increased (i.e. coinsurance is far less prevalent). New products are coming on the market, with wording that tends to be more complex. These hybrid products are now well managed by insurers, who offer various solutions that combine insurance (insemination) and crisis management (services). This type of coverage can take the form of primary coverage, or can entail the augmentation of existing liability or damage benefits. Some brokers now offer related upstream services aimed at helping clients assess these risks. Advent of international programs.

Auto insurance deductibles and trends

The tendency is downward (by 20 to 30 percent), owing to increased competition. Reductions for companies that are smaller and have lower risk. Insurers can now offer higher deductibles. Business interruption deductibles expressed in terms of reduced time or converted into triggering thresholds; a single deductible is applied to all benefits. Crisis management benefits are not subject to a deductible.

Sector not following the trend: distribution

Increased capacity

The theoretical capacity in the continental European market is around €355 million, plus €100 million in the UK. In reality, the greatest capacities earmarked for a given program tend to be around €100 to €150 million.

Competitive pricing

Competition is stiff, and prices are trending downward, owing to the increased competition brought about by the advent of new players. Around 20%, but difficult to quantify in terms of a percentage (not enough time has elapsed since these products were introduced). Reductions for companies that are smaller and have lower risk. Optional reinsurance is having an increased impact on the rates charged by insurers that offer lead underwriting services and whose capacity exceeds €25 million. Impact on US loss statistics outside of the distribution sector.

Further Reading

Cahiers Techniques
Collection Dialoguer
Collection Maîtrise des Risques

Online bookstore
www.amrae.fr/publications

Price for bound copies: €15 (including French tax)

www.amrae.fr

Management des Risques et des Assurances de l'Entreprise
80 BOULEVARD HAUSSMANN 75008 PARIS - TEL : +33 (0)1 42 89 33 16 - FAX : +33 (0)1 42 89 33 14 - amrae@amrae.fr - www.amrae.fr