



CyberRisk: Wisconsin Technical Colleges

Presented By:

David Hallstrom



Arthur J. Gallagher & Co.

Agenda

- ❖ RPS Executive Lines – Who we are
- ❖ Overview and market evolution
- ❖ Why protect against cyber losses?
- ❖ What are cyber risks?
- ❖ Cyber risk management
- ❖ Cyber risk transfer
- ❖ Cyber coverage
- ❖ Who has an exposure
- ❖ Q & A



RPS EL – Who We Are

- ❖ Wholesaler specializing in professional and management liability
- ❖ Established August 1999
- ❖ Specialist and knowledgeable team



Overview and Market Evolution

- ❖ Most property policies exclude cyber/virus/e-risk exposure
- ❖ A market of specialist insurers has grown to fill the gap
- ❖ Specific policies introduced to address ever-increasing exposures – CFC, AIG, Hiscox and many others



Why Protect Against Cyber Losses?

- ❖ Protect bottom line
- ❖ Protect reputation
- ❖ Due diligence
- ❖ Regulatory and legal requirements



What Are Cyber Risks?

- ❖ **Cyber risks are losses and liabilities that a company faces as a result of using the Internet, computer systems and email**
- ❖ **Examples include:**
 - **Liability to a third party due to libel contained in email**
 - **Liability to a third party due to a virus transmitted by you**
 - **Damage to your computer network due to harmful virus or hacker**
 - **Loss of revenue due to downtime of computer systems caused by a virus or hacker**
 - **Theft of your money due to hacking or employee electronic theft**
 - **Threats or extortion relating to your computer systems**



How can you protect the organization?

- ❖ IT Defenses
- ❖ Policies and procedures
- ❖ Risk transfer
- ❖ Cyber coverage
- ❖ Technology partnerships



Cyber Risk Management

IT defenses

- ❖ Firewalls
- ❖ Anti-virus protection
- ❖ Intrusion Detection Systems
- ❖ Encryption
- ❖ Back-ups
- ❖ Content filtering
- ❖ ISO 17799

Note: Most of these defense are reactive and therefore, by their very nature cannot be 100% effective



Cyber Risk Management

Policies and procedures

- ❖ IT security policy
- ❖ Employee internet and email use policy
- ❖ Backup and creation of off-site storage policies
- ❖ Disaster recovery plan
- ❖ Software patches

Note: All polices and procedures rely on human beings and therefore, by their very nature, cannot be 100% effective



Cyber Risk Transfer

- ❖ Traditional property policies were not intended to protect intangible assets such as IP and data
- ❖ Traditional liability policies rely on BI/PD triggers; there is no cover for financial loss arising out of breach of privacy, etc.
- ❖ Traditional liability policies will not cover damage to third parties' intangible property
- ❖ Property, liability and PL policies all introduce virus/cyber exclusions



Cyber Coverage

- ❖ *First and third party coverage available*
- ❖ *Modular policies*
 - **Media Liability**
 - **Network Security**
 - **Professional Liability**
 - **Damage to Your Systems**
 - **Business Interruption**
 - **Electronic Theft**
 - **Threats or extortion**



Media Liability

- ❖ **“Media event” means:-**
 - **any libel, slander, plagiarism, product disparagement or trade libel, or**
 - **any breach of confidentiality or rights of privacy, or**
 - **any breach of any intellectual property rights, or**
 - **any negligent content,**
 - **as a result of electronic communications carried out by you or by any other person, persons, partnership, firm or company acting for you or on your behalf, or purporting to be you or act on your behalf, or**
 - **any breach of any statutory duty relating to electronic communications.**



Media Liability Incident

- ❖ **Eli Lilly is sued after a programming error results in the disclosure of approximately 700 email addresses belonging to participants in the company's Medi-messenger service**



Network Security

- ❖ **“Technology event” means:-**
 - **any third parties’ financial losses arising directly from a hacking attack or virus that has emanated from or passed through your computer systems, or**
 - **any third parties’ financial losses arising directly from their inability to access your computer systems in the way in which you have authorized them to as a direct result of your computer systems’ failure or impairment due to a hacking attack or virus, or**
 - **any third parties’ financial losses arising directly from the loss or theft of data for which you are responsible or held to be responsible.**



Network Security Incident

- ❖ **Georgetown University server is hacked, exposing name, address, date of birth and Social Security numbers of more than 40,000 people**



Damage to Your Systems

- ❖ We agree to reimburse you for rectification costs, subject to our prior written agreement (such agreement not to be unreasonably withheld) which you incur
 - in retrieving, restoring or replacing any of your computer records (or any other computer records for which you are, or you are believed to be, responsible) that you first discover during the period of the policy have been destroyed or damaged or lost or mislaid (and which after diligent search cannot be found), or
 - in repairing, restoring or replacing any of your computer systems that you first discover during the period of the policy have been damaged, destroyed or altered
 - as the direct result of any hacking attack or virus first discovered during the period of the policy.



Damage to Your Systems Incident

- ❖ A member of the IT department of a large international stock broker is denied a promotion. He places a logic bomb in the company's computer system shutting down their trading platform at 9:30 AM every Monday.



Business Interruption

- ❖ We agree to reimburse you for loss first discovered during the period of the policy by reason of any business interruption loss as the direct result of any hacking attack or virus.
 - “Business interruption loss” means the difference between the revenue, including advertising revenue, that you reasonably project has been lost solely and directly as a result of a failure in your capability to use your computer systems or access your computer records and the costs that you would have incurred, but which you have saved as a result of not making those sales (including the cost of raw materials, and other saved costs).
 - This amount shall be determined by the Claims Managers named in the Schedule based on an analysis of the revenue generated and costs during each month of the twelve months prior to the loss and taking into account the reasonable projection of future revenue and costs and all material changes in market conditions which would affect the future revenue and costs generated.



Business Interruption Incident

- ❖ **E*Trade insured loss exceeds \$5 million from downtime due to a hacking incident**



Electronic Theft

- ❖ We agree to pay on your behalf any loss due to your receiving threats, either directly or indirectly, which you first discover during the period of the policy,
 - to introduce any hacking attack or virus into your computer system or your computer records, or
 - to disseminate, divulge or utilise information contained or once contained in your computer system or your computer records, or
 - to damage, destroy or alter your computer system or your computer records.
 - by any person who then demands ransom as a condition of not carrying out such threats.



Electronic Theft Incident

- ❖ Citibank lost more than \$11 million to a hacker using an old computer in an accounting office in St. Petersburg, Russia. Approximately \$500,000 of the money was never recovered.



Threats or Extortion

- ❖ We agree to pay on your behalf any loss due to your receiving threats, either directly or indirectly, which you first discover during the period of the policy,
 - to introduce any hacking attack or virus into your computer system or your computer records, or
 - to disseminate, divulge or utilise information contained or once contained in your computer system or your computer records, or
 - to damage, destroy or alter your computer system or your computer records.
 - by any person who then demands ransom as a condition of not carrying out such threats.



Threats or Extortion Incident

- ❖ A dismissed IT department employee encrypted the entire database of his previous employer and then demanded \$2 million in ransom. The company found out that it would cost at least \$10 million in computer and employee time to undo the damage.



Top 10 Customer Data Loss Incidents

- ❖ CardSystems - 40 million
- ❖ Veteran's Affairs – 26 million
- ❖ Citigroup – 3.9 million
- ❖ DSW – 1.4 million
- ❖ Bank of America – 1.2 million
- ❖ Wachovia/PNC/BoA – 676,000
- ❖ TimeWarner – 600,000
- ❖ Georgia DMV – 465,000
- ❖ LexisNexis – 310,000
- ❖ USC – 270,000
- ❖ Marriott – 206,000



“The Edge” Website Functionality

Risk Analysis

Function	Major Loss Scenarios	Insurance Coverage & Recommendations	Risk Management Recommendations & Sample Incidents
Hyperlinking <i>Used on the worldwide web to link together web pages.</i>	<u>1st Party</u> 1. Infringement by others on XYZ's intellectual property rights. (e.g., Undesired linking by others to XYZ websites) <u>3rd Party</u> 1. XYZ is liable to someone else for infringement of intellectual property rights. (e.g., Copyright, Trademark Infringement) 2. XYZ is liable to someone else for the content/activities of hyperlink destination website. (e.g., Vicarious liability for offensive material)	<u>1st Party Coverage</u> Intentionally Left Blank	<u>1st Party Risk Management Recommendations</u> Start by knowing who is linking to you. This can be accomplished by typing in the search string below at a search engine such as www.google.com link:www.XYZ.com Establish a linking policy in the <i>terms and conditions</i> section of the website. Restrict access and use hyperlinking agreements with all authorized parties. Track all hyperlinks and monitor incoming traffic requests. <u>3rd Party Risk Management Recommendations</u> Always utilize hyperlinking agreements . Post notices waiving liability for actions of third party websites. Notify users when they are leaving the XYZ website. <u>Sample Hyperlinking Incidents</u> 1. Bigger Not Better With Copyrighted Web Photos 2. XYZ:Clumsy Scenarios for Part 1(Hyperlinking)Movie groups want enjoined DVD site to stop hyperlinking



ISO 17799 Compliance

example report excerpts

CYBER RISK INSURABILITY ASSESSMENT
PREPARED FOR

**Acme
Insurance**

NetDiligence

APPLICANT: Acme Insurance
APPLICANT CONTACT: John Doe
APPLICANT CONTACT E-MAIL: john.doe@acme.com
APPLICANT CONTACT PHONE: 555-555-5555

Prepared by: NetDiligence
Date: 10/15/2007

eRisk Assessment Level 1.1

NetDiligence
A Division of Protonet Corporation

October 11, 2007 Page 4 of 11

NetDiligence consultant (NetDiligence) participated in this project. We wish to thank several Applicant employees who have graciously contributed their time and knowledge during the assessment. (redacted)

2.0 The NetDiligence™ Summary Opinion and Detailed Components

The formal opinion, findings and recommendations that appear in this section comprise the key observations prepared for NCM Global Markets in our evaluation of Applicant's digital risk rating in accordance with NetDiligence assessment methodologies and findings as the use of the report issued in Section 6.

2.1 Summary Opinion

The following Summary Statement Opinion has been prepared regarding Applicant's current information security controls with regard to its network, systems, and content:

NetDiligence believes that Applicant's information security controls provide for the management and functional control of information security, privacy, and the legal use of intellectual property in practice. Applicant's operations in addition, (redacted)

Our general findings include the presence/absence of the following baseline safeguards within Applicant's business operations:

SECURITY CONTROL	PRESENT/ABSENT
1. Physical Security: in place and properly managed	YES
2. Access Control: Software in place and properly updated	YES
3. Incident Response: Management process in place	YES
4. System Backup: Backup process in place	YES
5. Software: Data encrypted over public networks	YES
6. Identification of critical data assets	YES
7. Patching: Change management process in place	YES
8. Effective user access/permissions management	YES
9. Inhibit disaster recovery plans in place	YES
10. Legal Review of Information Security Policies	YES
11. Effective privacy policy and signed IP agreements	YES

eRisk Assessment Level 1.1

NetDiligence
A Division of Protonet Corporation

August 16, 2007 Page 4 of 8

SUMMARY RESULTS FROM APPLICANT-COMPLETED NETDILIGENCE SURVEY

Risk Assessment

NetDiligence Rating - Service Report Summary:

Company Name: (redacted)
Survey Completed On: (redacted)
Survey Date: (redacted)

NetDiligence rating is based on a score of 100 assigned based on responses provided by the Applicant. Higher scores indicate better risk management practices. A score of 100 indicates that the Applicant has met all the requirements for ISO 17799 compliance. A score of 0 indicates that the Applicant has not met any of the requirements for ISO 17799 compliance. A score of 50 indicates that the Applicant has met some of the requirements for ISO 17799 compliance.

Security Policy	Present	Score
Is a written policy document available to all employees responsible for information security?	YES	100%

Security Organization	Present	Score
Is a group of individuals responsible for information security management identified, authorized to report and control the organizational information security policy and organization?	YES	100%

Information Asset Classification & Control	Present	Score
Is a system appropriate classification of information assets used to assign the appropriate level of protection to information assets?	YES	100%

Business Processes	Present	Score
Do critical business processes, such as disaster recovery, business continuity, and other critical business processes, have a documented and tested recovery plan?	YES	100%

Physical and Environmental Protection	Present	Score
Is a physical security policy document available to all employees in printed form, design an appropriate level of protection to information assets?	YES	100%



How to Identify Your Exposure

Question	Answer Yes/No	Major exposures	Is cover available under commercial policies?
Do you have a website?	Yes/No	<ul style="list-style-type: none"> Breach of intellectual property rights. Libel & slander Misleading advertising/pricing 	Yes/No Yes/No Yes/No
Do you hold HR/payroll data on your network?	Yes/No	<ul style="list-style-type: none"> Breach of employees' privacy rights 	Yes/No
Do you allow staff to use email and the internet?	Yes/No	<ul style="list-style-type: none"> Libel & slander Damage to your systems due to a virus or hacking attack Damage to third parties systems by you forwarding a virus. Employees creating or sending a virus to your business contacts Employees hacking activities Breach of privacy laws. 	Yes/No Yes/No Yes/No Yes/No Yes/No
Do you allow suppliers to access your network?	Yes/No	<ul style="list-style-type: none"> Damage to your computer systems due to a virus or hacking attack. Consequential loss to your business due to downtime. 	Yes/No
Do you operate a bulletin board, discussion forum or chat room?	Yes/No	<ul style="list-style-type: none"> Libel & slander Breach of intellectual property rights 	Yes/No Yes/No
Do you have sensitive data accessible through your web server?	Yes/No	<ul style="list-style-type: none"> Libel & slander Breach of intellectual property rights Breach of Data Protection Act 	Yes/No Yes/No Yes/No
Do you transact business via your website or rely heavily on Email?	Yes/No	<ul style="list-style-type: none"> Damage to your systems due to a virus or hacking attack Your lost revenue due to a virus or hacking attack Breaches of statutory duties regarding the advertising or sale of goods or services by e-commerce 	Yes/No Yes/No Yes/No
Do you hold/obtain customers' credit card details and personal details on your network?	Yes/No	<ul style="list-style-type: none"> Breach of Data Protection Act. Third parties financial loss due to dishonesty of your Employees 	Yes/No Yes/No



Q & A

David Hallstrom

RPS

312-803-7450

David_Hallstrom@rpsins.com

