

The Journey Towards HPR – What a Risk Manager Should Know

MARIM Borneo Summit
22nd October 2024

©2024 ARTHUR J. GALLAGHER & CO.



Gallagher

Insurance | Risk Management | Consulting

Agenda

1

What is HPR?

2

Key steps towards achieving HPR

3

Going above and beyond – proactive risk management approach

4

Case Study

1

What is HPR?



HPR – Highly Protected Risk

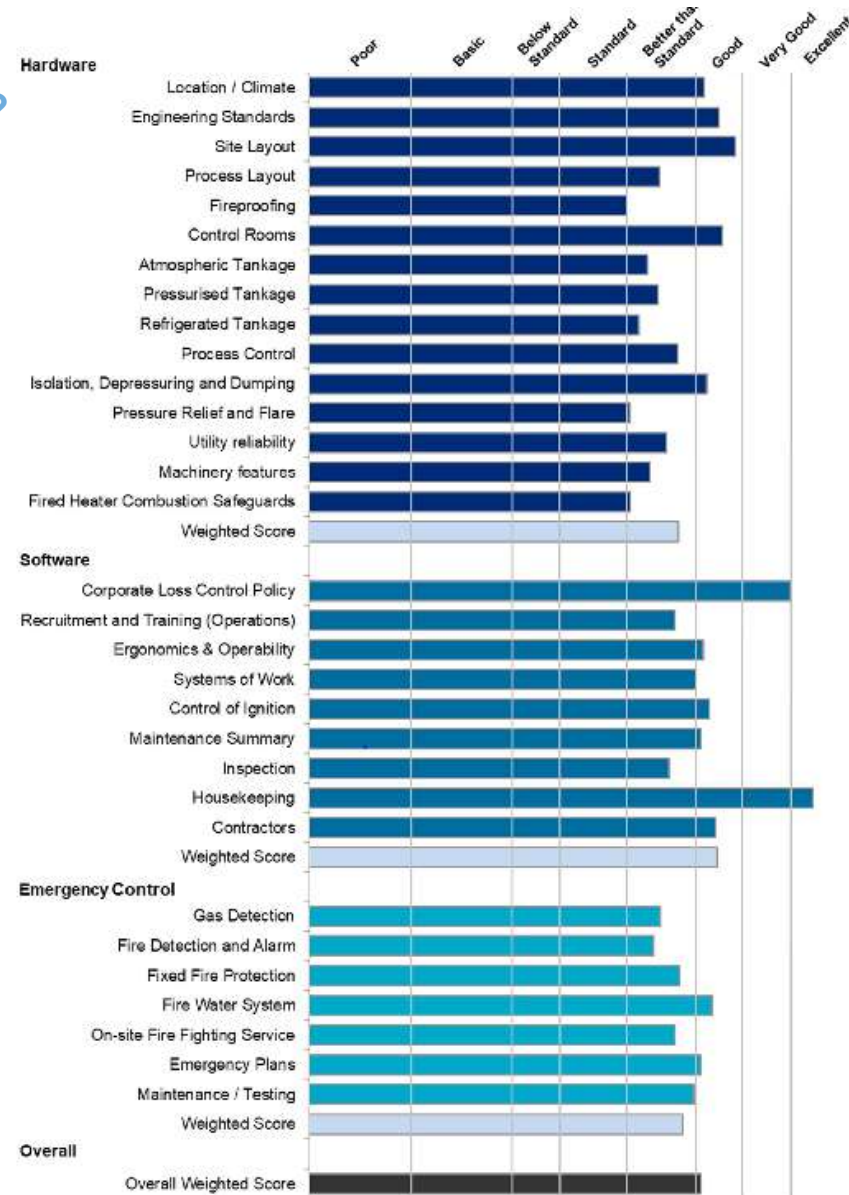
What is HPR?

- A Highly Protected Risk (HPR) is a term commonly used in the insurance industry to describe properties that have exceptional risk management measures in place
- These properties typically have advanced fire protection systems, security measures, and other safeguards that significantly reduce the likelihood of a loss occurring
- HPR properties are often associated with large commercial or industrial facilities, such as power, energy and manufacturing plants, data centers, or high-value properties
- To be considered an HPR facility, there are some basic protection features that are required for the Construction, Occupancy, Protection and Exposure (COPE) of the building
- Adding protection of Natural Catastrophe (NatCat) type perils such as flood, wind, snow, hail and earthquake also qualify as an HPR risk.
- One of the most important items is management's commitment to maintaining and updating the facility, its operations, and the fire systems. These are usually classified as Human Element programs.

HPR – Highly Protected Risk

What is usually considered for an operation to be deemed an HPR?

- **Location / NATCAT exposure**
- **Site Facilities / Hardware**
 - Layout / Construction
 - Control Facilities / Safety System
- **Management / Safety Systems**
 - Organisation
 - Process Safety Management
 - Operations
 - Engineering and Technical Services
 - Maintenance
 - Inspection
 - Occupational Safety
 - Physical Security
 - Cyber Security
- **Emergency Control**
 - Emergency Response
 - Fire Walls and Fireproofing
 - Fire and Gas Detection
 - Firewater System
 - Fixed Protection
 - Mobile Equipment
 - Testing



HPR – Highly Protected Risk

What benefit does a HPR bring from an insurance point of view?

- Lower Premiums;
- Higher Coverage Limits;
- Improved Policy Terms and Conditions;
- Reduced Exclusions;
- Discounts and incentives;
- Tailor-made coverage;
- Improved market relationship.

2

Key steps towards achieving HPR



Key Steps Towards Achieving HPR

To achieve a Highly Protected Risk (HPR) status, a risk manager should take several key steps:

Conduct a thorough risk assessment of your assets

- Identify and evaluate potential risks and vulnerabilities specific to the property.
- This includes assessing fire hazards, security risks, natural disaster risks, and other potential threats

Implement robust risk management measures

- Develop and implement comprehensive risk management strategies and protocols.
- This may involve installing advanced fire protection systems, such as sprinklers, fire alarms, and fire-resistant materials.
- Implementing security measures like access control systems, surveillance cameras, and security personnel can also enhance protection.

Establish preventive maintenance programs

- Regularly inspect and maintain all equipment, systems, and infrastructure to ensure they are in optimal working condition.
- This includes routine inspections of fire protection systems, electrical systems, HVAC systems, and other critical components.

Key Steps Towards Achieving HPR

Develop emergency response plans

- Create detailed emergency response plans that outline procedures for various scenarios, such as fires, natural disasters, or security breaches.
- Conduct regular drills and training sessions to ensure all personnel are familiar with the protocols.

Engage with insurance providers

- Collaborate with insurance providers who specialize in HPR coverage
- They can provide guidance on risk management best practices and offer tailored insurance solutions for HPR properties.

Continuously monitor and update risk management measures

- Regularly review and update risk management strategies to adapt to changing risks and technologies
- Stay informed about industry best practices and emerging technologies that can further enhance protection.

By implementing these measures, a risk manager can significantly reduce the risk profile of a property and increase the chances of achieving a Highly Protected Risk status.

3

Going above and beyond – proactive risk management approach



Proactive Risk Management

To be proactive and identify risks that may not be immediately visible, a risk manager can take the following steps:

Maintain continuous comprehensive risk assessments

- Regularly assess the property, operations, and processes to identify potential risks.
- This includes reviewing historical data, conducting site inspections, and engaging with relevant stakeholders to gain insights into potential hidden risks.

Encourage reporting and feedback

- Establish a culture of open communication and encourage employees to report any potential risks or concerns they observe.
- Implement reporting mechanisms such as anonymous reporting systems or suggestion boxes to gather information on potential hidden risks.

Proactive Risk Management

To be proactive and identify risks that may not be immediately visible, a risk manager can take the following steps:

Stay updated on industry trends and best practices

- Keep abreast of industry developments, emerging technologies, and best practices in risk management.
- Attend conferences, seminars, and workshops, and engage with professional networks to stay informed about new and evolving risks.

Conduct regular audits and inspections

- Perform regular audits and inspections of processes, equipment, and systems to identify any deviations from established standards or potential risks that may not be immediately apparent.
- Adopt a proactive approach in addressing any issues that may arise – preventative rather than remedial.

Proactive Risk Management

To be proactive and identify risks that may not be immediately visible, a risk manager can take the following steps:

Engage with subject matter experts

- Collaborate with internal and external subject matter experts who possess specialized knowledge in specific areas of risk.
- These experts can provide insights and help identify risks that may not be readily visible to the risk manager.

Utilize data analytics and predictive modelling

- Leverage data analytics and predictive modeling techniques to identify patterns, trends, and potential risks.
- Analyze historical data, conduct scenario analysis, and use predictive models to anticipate and identify hidden risks.

Proactive Risk Management

To be proactive and identify risks that may not be immediately visible, a risk manager can take the following steps:

Foster cross-functional collaboration

- Engage with different departments and stakeholders within the organization to gain a holistic understanding of operations and potential risks.
- Collaborate with departments such as operations, finance, legal, and human resources to identify risks that may span across different areas.

Regularly review and update risk management strategies

- Continuously review and update risk management strategies to adapt to changing circumstances and emerging risks.
- Regularly reassess the effectiveness of existing risk controls and make necessary adjustments.

By adopting a proactive approach and implementing these strategies, a risk manager can identify and mitigate risks that may not be immediately visible, thereby enhancing the overall risk management efforts of the organization.

4

Case Study



Proactive Cyber Risk Management

Background: In the mid 2010, Drillco, a regional oil and gas services company, is expanding its digital footprint by integrating advanced technologies and cloud-based solutions to enhance operational efficiency and customer service.

Risk Assessment and Identification

- **Initial Audit:**
 - Comprehensive audit of the current IT infrastructure, including hardware, software, network configurations, and data storage solutions. Collaborates with the IT department to map out all digital assets and their respective vulnerabilities.
- **Threat Landscape Analysis:**
 - Staying updated with the latest cyber threat intelligence reports and industry trends, to understand emerging threats such as ransomware, phishing, and zero-day exploits.

Stakeholder Engagement:

- **Cross-Departmental Workshops:**
 - Organised workshops involving key stakeholders from IT, HR, legal, and operations to discuss potential cyber risks and their impact on business operations, to help in identifying critical assets and understanding the business processes that could be targeted by cyber threats.
- **Employee Feedback:**
 - Conducted surveys and interviews with employees to gather insights on their awareness and experiences related to cybersecurity, which helps in identifying gaps in the current security posture and areas needing improvement.

Implementation of Security Measures:

- **Enhanced Security Protocols:**
 - Based on the audit findings, working with the IT team to implement advanced security measures such as multi-factor authentication (MFA), encryption, and intrusion detection systems (IDS).
- **Regular Updates and Patching:**
 - Ensures that all software and systems are regularly updated and patched to protect against known vulnerabilities.

Proactive Cyber Risk Management

Training and Awareness Programs:

- **Cybersecurity Training:**
 - Develops and rolls out a comprehensive cybersecurity training program for all employees. This includes modules on recognizing phishing attempts, safe internet practices, and the importance of strong passwords.
- **Simulated Phishing Exercises:**
 - To test the effectiveness of the training, the company conducts simulated phishing exercises. Employees who fall for the simulated attacks receive additional training and guidance.

Incident Response Planning:

- **Incident Response Team:**
 - Establishes a dedicated incident response team comprising members from IT, legal, and communications with clear roles and responsibilities established for each team member in the event of a cyber incident.
- **Response Plan:**
 - Develops a detailed incident response plan outlining the steps to be taken in case of a cyber-attack. This includes communication protocols, data recovery procedures, and legal considerations.

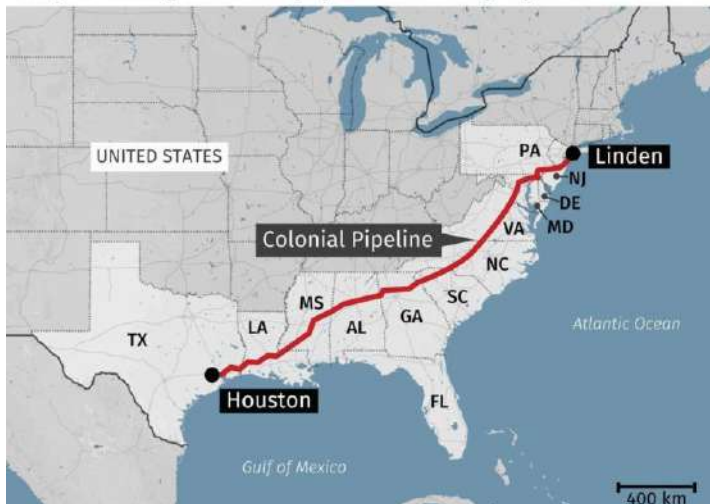
Continuous Monitoring and Improvement:

- **Real-Time Monitoring:**
 - Implements real-time monitoring tools to detect and respond to suspicious activities promptly, and sets up alerts for unusual login attempts, data transfers, and other potential indicators of a breach.
- **Regular Reviews:**
 - Schedules regular reviews of the cybersecurity policies and procedures to ensure they remain effective and up-to-date with the evolving threat landscape.

When things (really) go wrong

On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that afflicted computerised equipment managing the pipeline. The Colonial Pipeline Company halted all pipeline operations to contain the attack

Major U.S. gasoline pipeline hit by cyberattack



- The Colonial Pipeline hack is the largest publicly disclosed cyber attack against critical infrastructure in the U.S.
- The Colonial Pipeline is one of the largest and most vital oil pipelines in the U.S, and comprises more than 5,500 miles of pipeline.
- As a result of the attack, Colonial Pipeline was forced to shut down its operations, leading to fuel shortages and price increases in several parts of the country.
- In addition, the pipeline transports about 45% of all fuel consumed on the East Coast, so the shutdown impacted the U.S. economy significantly. The attack affected the airline industry, where there was a jet fuel shortage for many carriers, and also caused fear of a fuel shortage caused panic-buying and long lines at gas stations in many states.
- The attack began when a hacker group accessed the Colonial Pipeline network and stole 100 gigabytes of data within a two-hour window.
- Following the data theft, the attackers infected the Colonial Pipeline IT network with ransomware that affected many computer systems, including billing and accounting.
- Attackers got into the Colonial Pipeline network through an exposed password for a VPN account. According to the company's testimony, a Colonial Pipeline employee likely used the same password for the VPN in another location. That password was somehow compromised as part of a different data breach.
- The goal for attackers in a ransomware attack is to have the victim pay a ransom, which is exactly what Colonial Pipeline did, for 75 bitcoin, which was worth approximately \$4.4 million in 2021.

When things (really) go wrong

Cyber attacks on the oil and gas industry are growing because the sector is becoming increasingly dependent on technology and automation. This increased reliance on technology makes the sector more vulnerable to cyber attacks, which can cause significant disruptions to operations and potentially have severe consequences for the industry and the broader economy



- The oil and gas sector is a high-value target for attackers due to the sensitive and valuable information it holds, such as intellectual property, financial data, and data on critical infrastructure.
- A supply chain attack on an oil and gas company is a cyber attack that targets the company's suppliers, vendors, or other partners to gain access to the company's systems and sensitive information. This can be done by compromising the security of a supplier or vendor and then using that access to move deeper into the company's network.
- The attackers may use various methods to compromise the security of a supplier or vendor, such as phishing emails, malware, or other forms of social engineering.
- Once they have access, they can steal sensitive information, disrupt operations, or even sabotage equipment.
- In August 2017, Saudi Arabian oil company Saudi Aramco experienced a cyberattack that targeted its Triconex industrial control systems (ICS). The attack caused a shutdown of the company's production systems, resulting in the loss of an estimated 50% of the company's daily production output. It is believed that the attackers were able to gain access to the ICS network through a third-party vendor's system and then used the malware to manipulate the controllers and cause the shutdown.
- In late 2014, a disruptive cyberattack at a steel mill facility in Germany. The attack - which was deployed through a combination of social engineering tactics and malware - compromised several of the steel mill's industrial control components. From there, equipment breakdowns and production outages ensued, resulting in extensive property destruction, with the shutdown of the blast furnace leading to a "massive" property damage at the steel mill facility.



Gallagher

Insurance | Risk Management | Consulting

INTRODUCTION TO GALLAGHER



Global snapshot

FOUNDED IN

1927

with headquarters
in the U.S

REVENUES* OF:

\$10.8BN

8.6%

ORGANIC
GROWTH RATE

LISTED ON THE
NYSE (AJG)

\$62.1BN

market capitalisation

960+

OFFICES GLOBALLY

MORE THAN

53,000

EMPLOYEES WORLDWIDE

ONE OF THE
WORLD'S
TOP 3

INSURANCE
BROKERS

130+

COUNTRIES WHERE
WE ARE ABLE TO OFFER
CLIENT SERVICE
CAPABILITIES

Global presence

Canada

North America

Mexico

Bermuda

Caribbean
Jamaica | Barbados | Dominica | St. Lucia
Antigua & Barbuda | St. Kitts & Nevis
St. Vincent & Grenadines | Grenada
Trinidad & Tobago | Cayman

Colombia

Peru

Brazil

Argentina

Chile

Sweden

Norway

UK & Ireland

Denmark

Netherlands

Belgium

France

Spain

Germany

Switzerland

Italy

Central & Eastern Europe
Czech | Latvia | Romania | Serbia
Slovenia | Bulgaria | Croatia | Bosnia
Slovakia | Hungary | Poland

Turkey

Middle East
Saudi Arabia | UAE | Kuwait
Beirut | Oman | Bahrain

Dubai

India

Sri Lanka

South Africa

South Korea

Japan

China

Hong Kong

Taiwan

Vietnam

Philippines

Malaysia

Singapore

Indonesia

Australia

New Zealand

- Gallagher offices
- Minority stake partner

Specialty broking capabilities

Our London team provides bespoke policy wordings, programme design and placement solutions, and consulting in the following specialisms.



Accident & Health



Aerospace



Alternative Risk Transfer



Aquaculture



Cargo



Casualty



Construction



Credit & Political Risks



Crisis, Terrorism, Kidnap & Ransom



Cyber



Management Liability (D&O)



Financial Institutions



Fine Art



Hotel & Hospitality



Marine



Media & Entertainment



Medical Malpractice & Clinical Trials



Mining



Power & Renewables



Product Recall



Professional Indemnity



Property



Real Estate



Risk Consulting & Analytics



Specie



Sports & Contingency



Travel



Warranties & Indemnities

Q&A

Thank you

©2024 ARTHUR J. GALLAGHER & CO.



Gallagher

Insurance | Risk Management | Consulting

DISCLOSURE

© Copyright 2024 Arthur J. Gallagher & Co. and subsidiaries. All rights reserved: No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Arthur J. Gallagher & Co.



Gallagher

Insurance | Risk Management | Consulting