MARSH

Cyber Risk: Threats and Insurance Protection for the Mining Sector

CONTENTS

[1] SCADA: Supervisory control and data acquisition.

INTRODUCTION

The world's leading mining companies are now unanimous in reporting that cyber threats are a principal risk to them achieving their goals (Figure 1). The use of networked systems has progressively increased across all aspects of mining operations, from exploration and extraction, through processing and logistics, to sales and marketing – while a range of cyber-attacks on the sector and industry at large have stimulated concern.

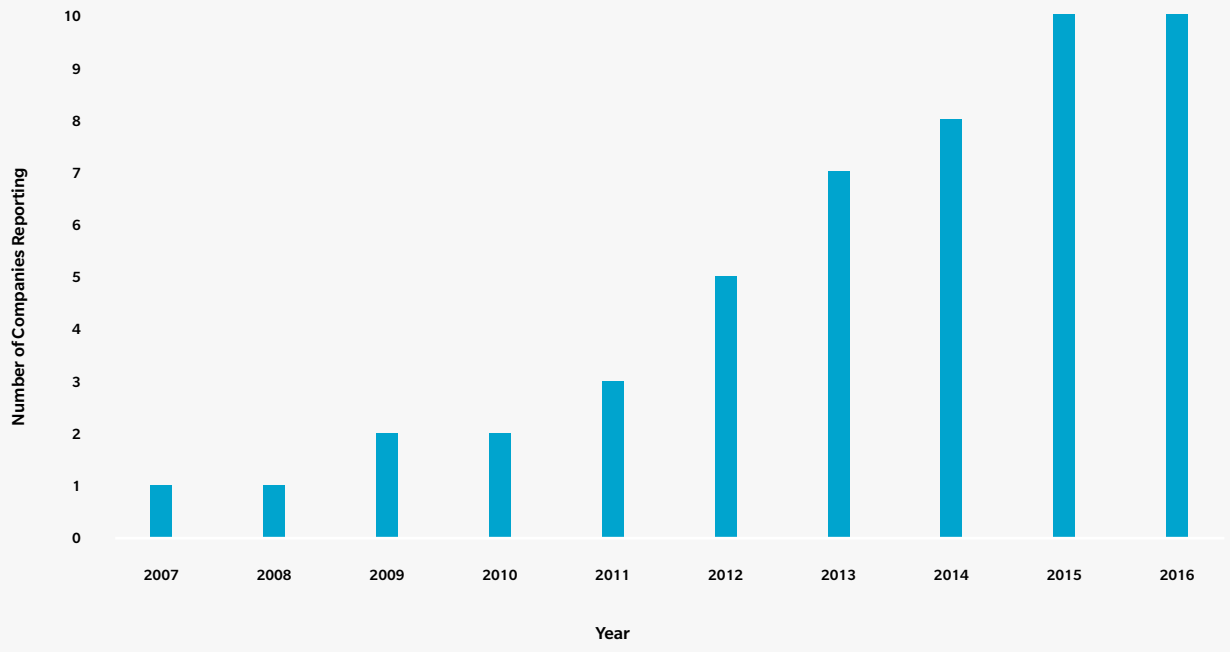
But what particular areas of exposure are faced by mining organizations – and to what extent can insurance markets respond?

In this paper, we highlight specific areas of cyber risk exposure for miners and consider the potential impact on operations. Moreover, we consider how a greater understanding of these risks is now reflected in a growing suite of cyber insurance solutions.

"There are only two types of companies: Those that have been hacked and those that will be."

ROBERT S. MUELLER
DIRECTOR OF THE US FEDERAL BUREAU OF INVESTIGATION (FBI), 2001-2013.[1]

FIGURE 1 **Reporting of Cyber Risk or Information Security Within the Principal Risk Disclosure of 10 Leading Mining Companies**
Source: Marsh



Leading mining companies selected on the basis of market capitalization, Q4 2017.

PUTTING CYBER RISK INTO CONTEXT

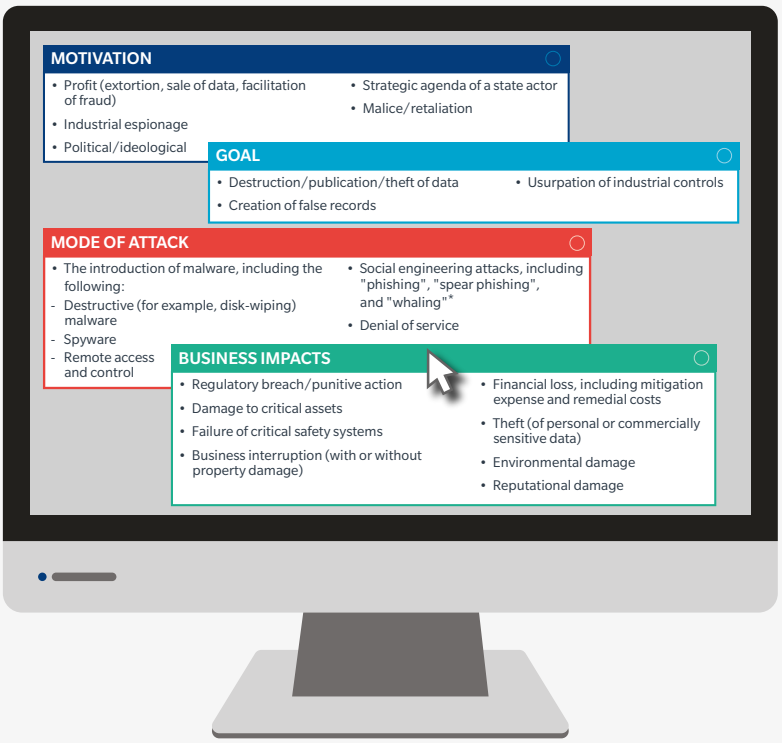
UNDERSTANDING MOTIVATION

The brief and catch-all phrase "cyber risk" applies to a broad range of threats and encompasses a wide and varied range of attacker motivations, goals, modes of attack, and ultimate business impacts.

Attacks can be broadly categorized into two types. The first focuses on specific industry targets with an express purpose to exploit an identified vulnerability, for example, multi-million dollar fraud events in which false payment instructions have been created (and acted upon), and attacks on specific assets and infrastructure, including the widely-publicized usurpation of controls at a German blast-furnace which triggered an explosion during its forced shut-down.

The second category of risk is further reaching: Untargeted or wide-area attacks that indiscriminately impact any business with a vulnerability, resulting in losses across a wide range of industry sectors and geographies.

FIGURE 2 **Making Sense of an Attack**
Source: Marsh



* "Phishing" is the sending of fraudulent emails in order to obtain sensitive or personal information. "Spear phishing" is a targeted form of phishing, aimed at specific individuals within a specific organization, while "whaling" is the most sophisticated of phishing attacks aimed at senior level or high-profile personnel.

SPOTLIGHT

Cyber-attack Examples

- Creation of undetected over-pressure, fire, and subsequent spill from a Turkish oil pipeline.
- Critical safety controls on an offshore installation disabled by a disgruntled employee.
- Forced shut-down of a German blast-furnace, resulting in an explosion which caused major damage to the plant.
- Shut-down of an offshore installation on the African coast, after an attack on buoyancy and stabilization systems.
- A 19-day withdrawal of offshore installation from service to remove malware.
- 35,000 hard-drives wiped at a Middle Eastern energy company. 17 days later, the company continued to give away oil in its domestic market to avoid absolute discontinuity of supply while sales could not be processed.
- Ukraine power grid shutdown, after a phishing attack allowed malware installation.
- Multiple, substantial data breaches, including the publication of sensitive employee, payment, and commercial data.

BEYOND BORDERS

The NotPetya ransomware attack in June 2017 is a case-in-point; an example of a broad-reaching attack illustrating both the difficulties in establishing attack motivation and in the ever-increasing global nature of the cyber threat.

The attack ricocheted around the globe, impacting most heavily on logistics, pharmaceutical, food manufacturing, and consumer goods operations, and resulting in hundreds of millions of dollars-worth of individual losses.

While it has since been established that ransomware entered multiple global networks via a malicious update to MeDoc (a widely-used Ukrainian accounting software program). The "update" reportedly incorporated attack tools developed by the US National Security Agency stolen and released by a hacker group in April 2017; the motivation behind the attack remains unclear.

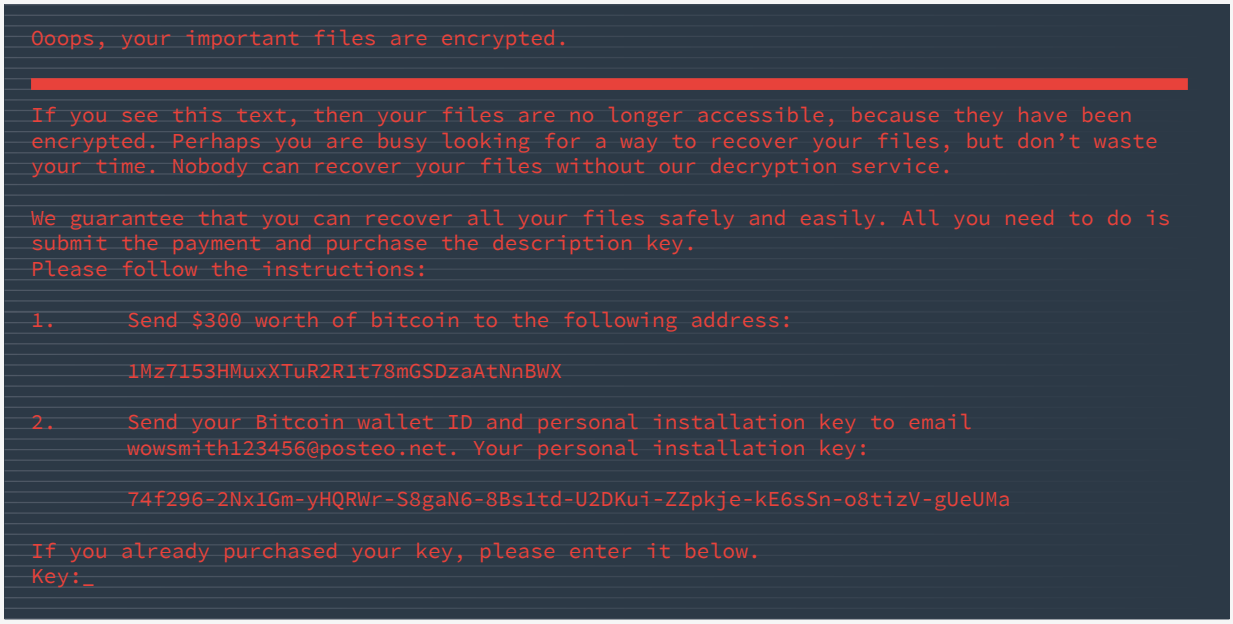
Ostensibly a ransomware attack, commentators have noted the difficulty in successfully monetizing ransomware attacks or collecting crypto-currency ransoms without exposure to law enforcement agencies; instead, it has been suggested that the event was "a deliberate, malicious, destructive attack or perhaps a test disguised as ransomware."[2] More frighteningly, the original Petya attack, after which the event was named, resulted in power outages across the Ukraine – and the impairment of the radiation monitoring system at the Chernobyl nuclear site.

Whatever the motivation, economic damage was significant, with cyber security analytics services provider, Cyence, estimating total global losses in excess of US$850 million.[3]

US$850m

the total global loss estimate of the NotPetya ransomware attack in June 2017.

FIGURE 3 **The NotPetya Ransom Note**
Source: Krebs on Security[4]



BEYOND TECHNOLOGY

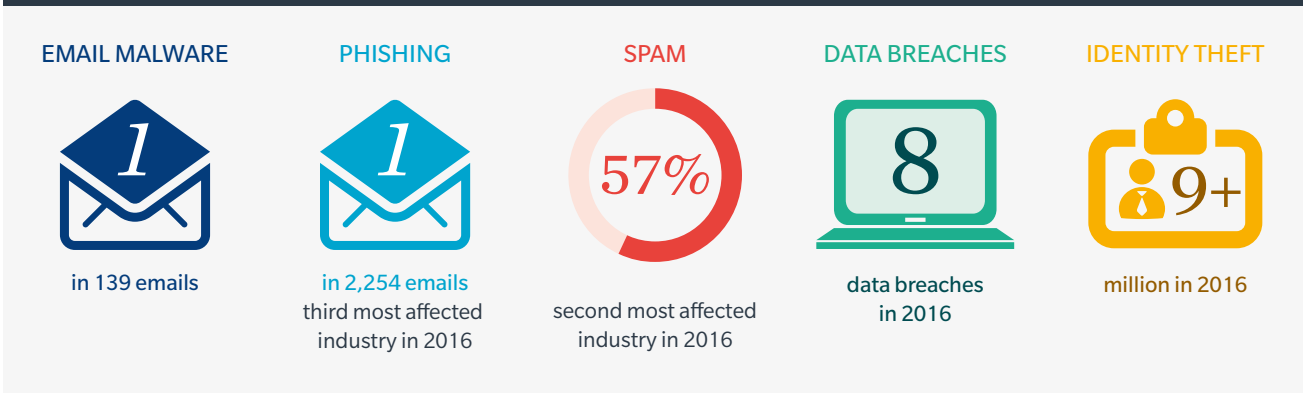
It is worth noting at this point that a key cyber risk factor – and thereby a crucial first line of cyber defense – is company personnel. Human error is a contributing factor in a large number of cyber incidents investigated, whether through lost or stolen devices, data sent in error, deliberate or malicious acts by employees, or through a lack of training and/or a poor understanding of the IT systems and software they are using.

The reality of cyber risk is that it is not simply a technology risk in which technical experts will either breach or attain security – rather risk management encompasses information technology, operational technology, employee training, and management – and potentially crisis response.

KEY RISKS TO THE MINING SECTOR

In the same way that a metals or mining company may face a focused attack or become caught up in an indiscriminate event, so the risks faced by companies are both common to all sectors and specific to operations. Key risks to the sector include:

FIGURE 4 **Mining Cyber Facts**
Source: Symantec[5]



LOSS OF FINANCIAL DATA INTEGRITY

The integrity of financial management and reporting is the cornerstone of investor confidence. For example, a cyber event could lead to the delayed publication of results for a company listed on a stock exchange. Such an attack could create delays while records are reconstituted, which exposes a critical aspect of security to public critique, and complicates an already demanding and critical component of the corporate calendar.

LOSS OF COMMERCIAL DATA AND PRIVACY

The reporting of recent mining sector data breaches has typically focused on the release of sensitive human resources information. While such breaches are clearly detrimental, the loss of commercial privacy – for example, in the context of mergers and acquisitions (M&A) – can have more serious consequences.

LOSS OF EXPLORATION DATA, MINING RIGHTS AND TITLE, AND RESOURCE DEFINITION

Likewise, exploration data includes valuable geological data that has taken considerable time and investment to acquire, and is a core component of a mining company's value. Electronic resource definition and mine models are, in turn, fundamental to day-to-day mining operations. Loss of this data – or loss of access to it – therefore has the potential to cause significant financial loss, including cost of reinstatement.

LOSS OF COMMUNICATIONS

By overwhelming, destroying, or denying access to communication systems, cyber-attackers can deliberately interrupt production and fundamental commercial activities, such as the ability to order supplies and to create or pay invoices.

MAJOR DISRUPTION TO SUPPLIES

Mining operations have ubiquitous and critical dependencies on electrical and water supplies which are vulnerable to interference. Loss of energy can rapidly manifest as significant physical harm – the settling of solids in thickeners, tanks, and pipelines, or the inability to decant excess water from tailings and water dams, for example.

Cyber-attacks on utilities have included attacks on distribution at the highest level, such as the 1999 Trojan horse attack on a Russian energy company that locked out control of a central switchboard that routed gas flow,[6] as well as more focused attacks on specific energy installations.

Moreover, miners are highly dependent on standby systems for critical processes, such as furnace cooling or mine ventilation, therefore a potential cyber-attack represents significant hazard.

MAJOR SUPPLY CHAIN DISRUPTION

The mining supply chain is potentially vulnerable at many points, from inventory control systems through to the disruption of production and delivery of critical inputs. The dependency of gold operations, for example, on continuous cyanide shipments exposes them to disruptive risk at production (for example, through quality control interference or production disruption), shipment (for example, through navigational interference), and at customs clearance (for example, through record tampering).

SAFETY CRITICAL CONTROLS

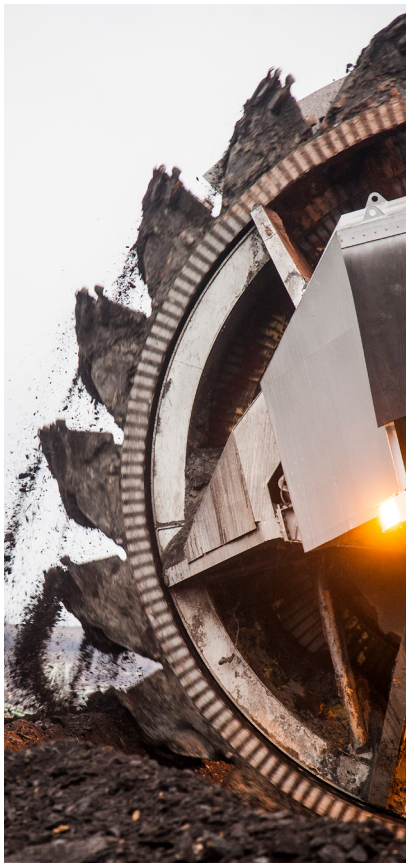
Electronic control systems are a fundamental feature of safety critical systems, ranging from shaft winders to the remote control systems and telemetry used to manage and monitor haul truck operations. Moreover, ventilation, refrigeration, and fire detection and suppression systems are all typically related to supervisory control and data acquisition (SCADA – see page 6) systems, as are many critical aspects of processing operations, such as smelting and refining electrode controls and furnace cooling systems.

LOSS OF ACCESS CONTROLS

In addition, disruptions to electronic access control systems can result in mining operations being unable to access workings or remove workers to safety. Access control is now predominately computerized; making access control breaches at best a threat to production, or, in a worst-case scenario, compromising the safety of thousands of mineworkers.

CRITICAL CONDITION MONITORING SYSTEMS

Stability monitoring systems within both open pit and underground mining operations, as well as tailings impoundments, often incorporate electronic monitoring and warnings systems that are critical to safety. Other condition monitoring systems – for example, air-gap sensors in gearless mill drives – are essential to the integrity of production processes.



DISRUPTION TO SAFE AND INTELLIGENT MINING

Advances in sensor technology and digital processing are improving mine performance and safety. Sensors on equipment, personnel, and rocks generate valuable streams of information; hundreds of parameters are recorded and interpreted every second.

If this information is compromised, miners using the most advanced and emerging technologies are most vulnerable. Aside from the obvious and immediate challenge posed to remote operatorship, tech-led miners may also suffer a prolonged loss of efficiency and a heightened risk of near-term unplanned outages.

UNDERSTANDING SCADA

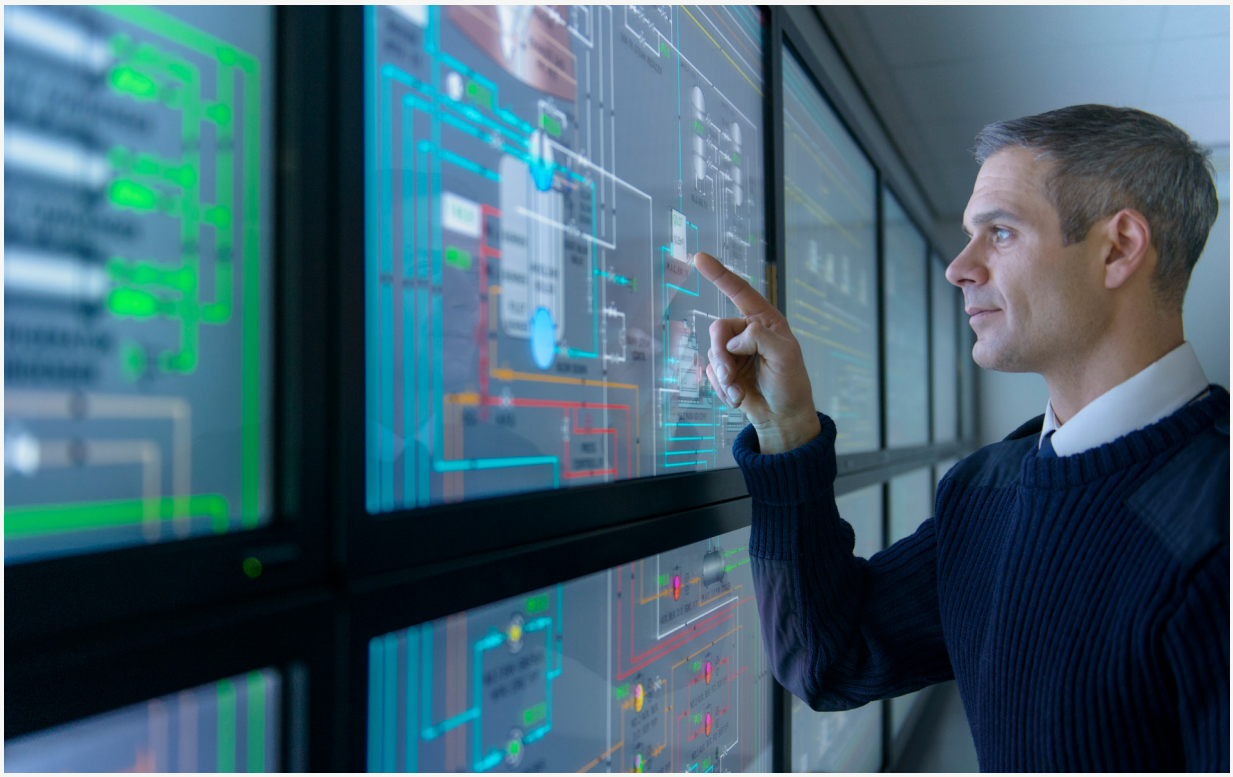
The remote connectivity of modern mining operations is significant. Major plant systems, such as modern gearless mill drives or draglines, are remotely monitored by both original equipment manufacturers (OEMs) and control rooms, while rail, port, blending, and sales operations, may be both interconnected and internet-connected. This remote access and control is provided by industrial control systems (ICS), systems such as SCADA, and by other remote telemetry devices that link to other physical devices through internet access or modems.

The mining sector has been quick to take advantage of these new interconnected systems to capture the benefits of productivity and availability gains. As such, many systems now employ cloud technology, human machine interfaces (HMI), or Wi-Fi capabilities.

The integration of plant from varying suppliers and the rolling implementation of new technologies to plant and processes can introduce vulnerabilities – poor credential management, lack of authentication/authorization features, and the potential for the introduction of malware.[7] The increasing convergence of information and operating technology platforms coupled with misaligned security protocols can therefore afford free movement between systems and platforms once system entry has been achieved.

Several external attacks on similar "open" systems have been experienced within the global utilities sector. In late 2015, there was a coordinated and multi-faceted attack on the SCADA systems used by a Ukrainian power distribution company. The attack began with a spear-phishing campaign, knocking out 30 electricity substations and impacting 80,000 customers. It has since become clear that parallel attacks were attempted at three other distribution companies, which could have affected upwards of 225,000 customers had they been successful.[8]

It was a sophisticated, multi-stage and multi-site attack, employing techniques such as spear-phishing, malware, and the use of remote admin tools to compromise field devices at substations and flooding the customer call center with fake calls. While the incident highlighted a breadth of vulnerabilities, including security lapses in the company's corporate IT and SCADA systems and weaknesses in employee cybersecurity training, it also illustrated the creativity, determination, and preparedness of cyber-attackers when motivated to attack.



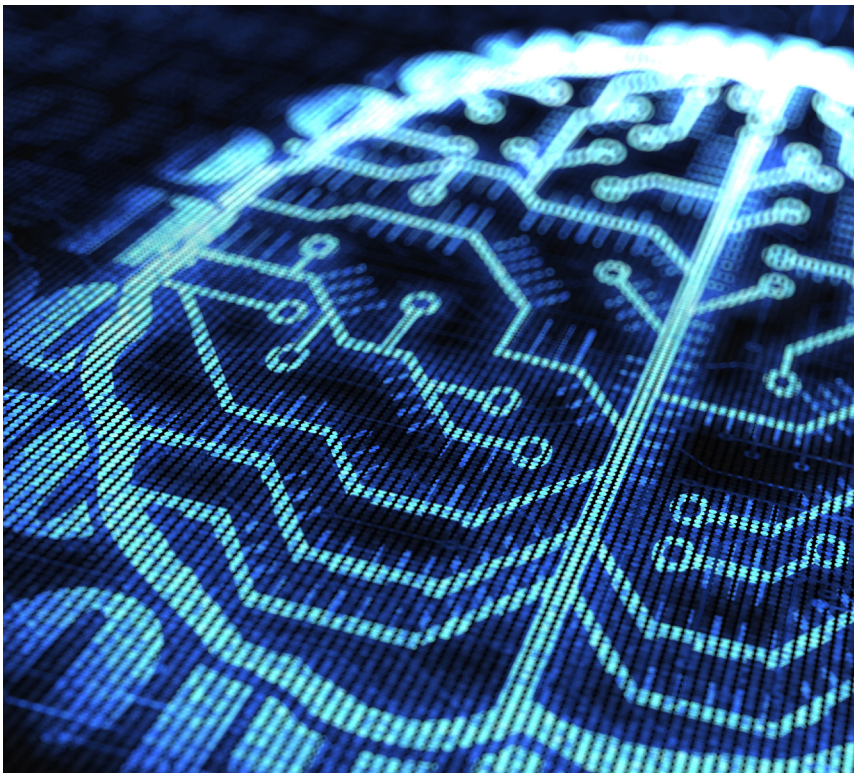
INSURANCE MARKET RESPONSE

The insurance market has developed rapidly in response to the evolving threat of cyber. Annual gross written cyber insurance premiums have grown by 34% per annum over the past seven years, from US$500 million in 2009 to US$3.9 billion in 2016.[9] With approximately US$500 million of cyber capacity now available, together with a greater awareness and understanding of cyber risk, it is expected that the global cyber insurance market will continue to grow at pace and is projected to reach US$9 billion by 2020.[10]

In essence, there are two broad types of cyber insurance cover. Early focus was on third-party liability cover available in specific cyber policies and largely focused on data breach. More recently, attention has turned to first-party cover, and cover for first-party losses in respect of property damage, business interruption (BI) and non-damage business interruption, and fraud.

Today, a growing record of loss adjustment and claims payment spanning data breach, extortion, denial of service, phishing attacks, internal IT failure, and BI enables insurers to model their own exposures, influencing appetite, pricing, and underwriting requirements for cyber cover.

Yet while there is a growing suite of more sophisticated first-and third-party cover (see Figure 5), there remains little standardization in respect of standard insurer-issued products; a problem compounded by the fact that 49% of respondents in a recent Marsh survey[11] admitted having "insufficient knowledge" about their cyber risk exposures to be able to assess the products available to them.



34%
annual growth in gross written cyber insurance premiums (last seven years).

US$3.9bn
written in 2016.

US$500m
cyber capacity available.

+45%
of companies have "insufficient knowledge" of their cyber exposures.

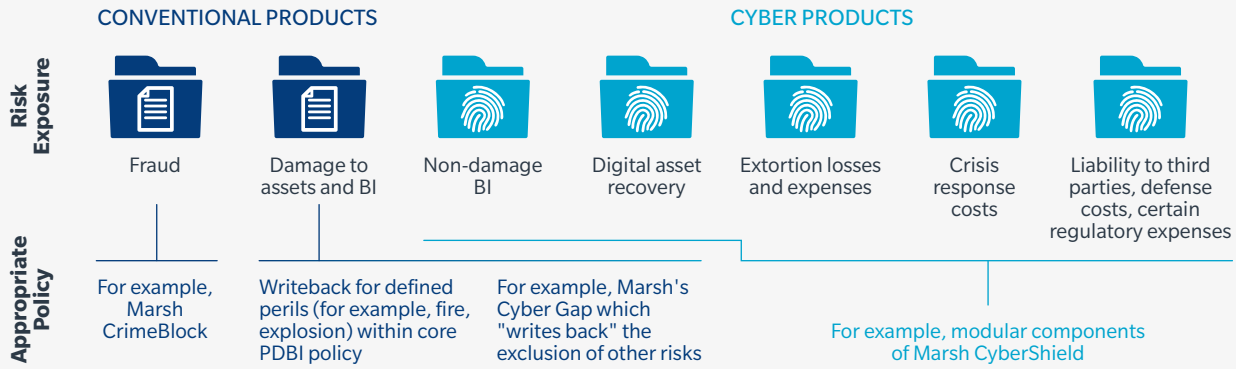
FIGURE 5 **Different Loss Categories for Which Protection is Available in the Cyber Insurance Market**
Source: MMC Cyber Handbook 2018

CATEGORY	DESCRIPTION
Intellectual property (IP) theft	• Loss of value of an IP asset, expressed in terms of loss of revenue as a result of reduced market share.
BI	• Lost profits or extra expenses incurred due to the unavailability of it systems or data as a result of cyber-attacks or other non-malicious IT failures.
Data and software loss	• The cost to reconstitute data or software that has been deleted or corrupted.
Cyber extortion	• The cost of expert handling for an extortion incident, combined with the amount of the ransom payment.
Cyber-crime/cyber fraud	• The direct financial loss suffered by an organization arising from the use of computers to commit fraud or steal money, securities, or other property.
Breach of privacy event	• The cost to investigate and respond to a privacy breach event, including IT forensics, and notifying affected data subjects. • Third-party liability claims arising for the same incidents. Fines from regulators and industry associations.
Network failure liabilities	• Third-party liabilities arising from certain security events occurring within the organization's IT network or passing through it in order to attack a third party.
Impact of reputation	• Loss of revenues arising from an increase in customer churn or reduced transaction volumes, which can be directly attributed to the publication of a defined security breach event.
Physical asset damage	• First-party loss due to the destruction of physical property resulting from cyber-attacks.
Death and bodily injury	• Third-party liability for death and bodily injuries resulting from cyber-attacks.
Incident investigation and response costs	• Direct losses incurred in investigating and "closing" the incident and minimizing post-incident losses. • Applies to all the other categories/events.

DESIGNING A SUITABLE CYBER PROGRAM

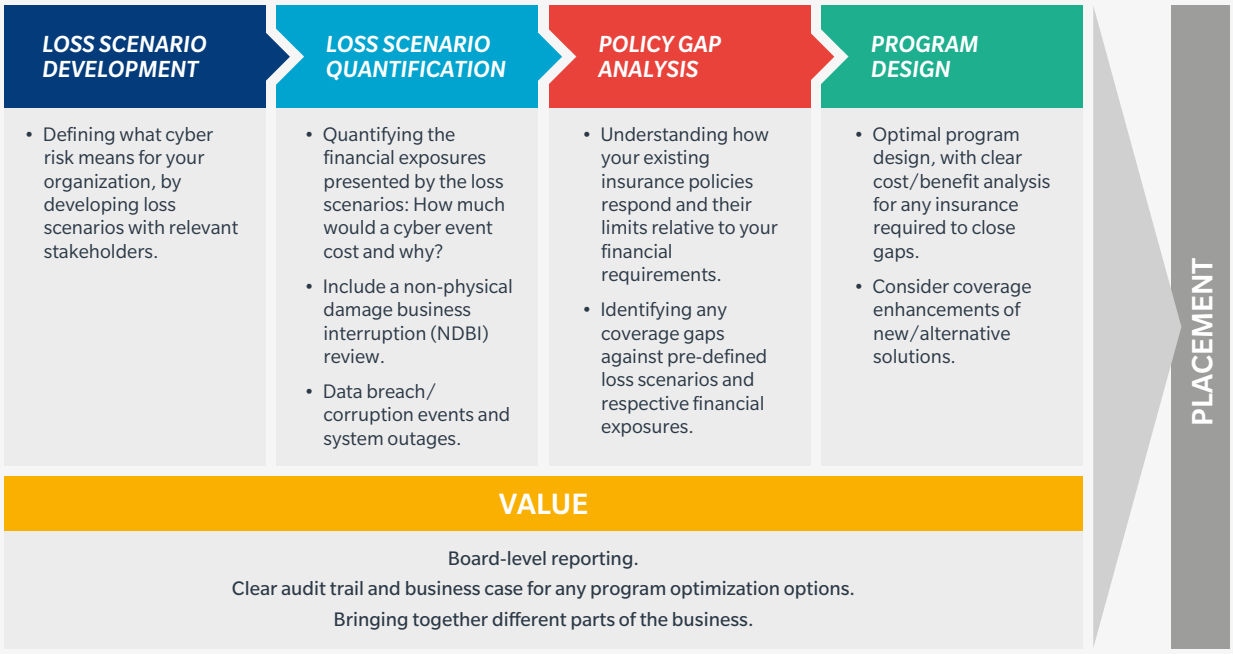
Designing a cyber program begins with establishing a clear understanding of cyber exposures and mapping those against existing non-cyber insurance products. Carefully worded crime and property damage and BI policies are the starting point for comprehensive cyber coverage.

FIGURE 6 **Available Breadth of Cyber Coverage**
Source: Marsh



A modular approach based on loss scenario development and qualification, and a comprehensive policy gap analysis as per the Marsh Cyber Assurance* Consultancy Framework (see Figure 7), can then be developed to address specific aspects of risk exposure, weaving together conventional lines of cover and dedicated cyber products to create a suitable program of protection.

FIGURE 7 **The Marsh Cyber Assurance Consultancy Framework**
Source: Marsh



*Marsh Cyber Assurance is offered in the UK, other Marsh markets offer similar products.

CONCLUSION

Despite the mystique that can surround cyber risk, conventional risk management frameworks provide all of the tools for a strong risk governance framework. Identifying, evaluating, and treating cyber risk will draw on the same principles of risk management used to control other threats to the organization, and a successful risk mitigation program will, in turn, feature a familiar suite of controls.

Pre-loss controls – embedded within operations and combining physical controls, process controls, and employee education – will minimize the probability of an event. Post-loss risk mitigation measures will also reduce impact. A practiced management and operational business continuity plan and crisis response plan will support effective crisis control, while risk transfer – through insurance – provides increasingly economic risk capital and a financial back-stop to cyber risk.

Therefore, despite any remaining novelty around the cyber risk topic, the pathway to resilience is accessible and insurance market support has evolved to provide a broad complement of protection.

SPOTLIGHT

ILLUSTRATIVE PROGRAM RESPONSE

MARSH'S CYBER GAP INSURANCE

POLICY STRUCTURE

Cyber Gap addresses the gap in cover created by cyber exclusions contained in a property damage business interruption (PDBI) policy:

- A wraparound core property damage and BI and/or terrorism policy.
- If the core policy declines a loss due to a cyber exclusion, the Cyber Gap policy is triggered.
- The core policy deductible applies.
- Coverage for dependencies (including utilities) is provided to the extent of core policy coverage.

LOSS SCENARIOS

- A hacker gains access to the industrial control system of a refrigeration plant providing cooling to an underground mine, taking control of and over-speeding the compressor, resulting in catastrophic failure of the machine. The machinery breakdown and BI is recoverable against the Cyber Gap policy.
- The Shamoon virus hits, causing damage and prohibiting the supply of propane to one of your supplier's affiliates. Your sub-limit of named or unnamed suppliers responds through your Cyber Gap policy.
- A contractor connects a laptop to a network and unwittingly transfers a virus. The virus results in a complete loss of plant control room display, leaving plant operators unable to control operating conditions and forcing attempts at a manual shut-down of operations. Resulting breakdown losses and mitigating expenses are recoverable against the Cyber Gap policy.

MARSH CYBERSHIELD

POLICY STRUCTURE

Marsh CyberShield allows for a modular approach to policy construction, including:

- Non-damage business interruption; coverage for production losses caused by a cyber event but without damage to plant.
- Cover for loss of income and increased costs of working resulting from network interruption due to a security failure, system failure, or to operational error (including failure of your third-party outsourced partner(s)).
- Cover for the costs of recovering, reconstructing, reloading, or replacing digital assets which have been impaired due to a security failure, system failure, or operational error (including failure of your third-party outsourced partner(s)).
- Cover for the payment of cyber extortion losses and expenses.
- Associated crisis response costs, including IT forensic costs, legal expenses, customer call center costs, notification expenses, identify theft remediation services, and public relations costs.
- Cover for your liability to third parties, defense costs, and regulatory fines, in respect of:
  - A data breach.
  - Breach of data protection legislation.
  - Breach of confidentiality agreements.
  - Network hijacking, including virus transmission.
- No requirement for monetary retention for BI claims.
- Full retroactive cover; incidents occurring before purchase, but unknown or undiscovered until after purchase, are not excluded on a retroactive date basis.

REFERENCES

1. Mueller, Robert. "RSA Cyber Security Conference", available at https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyberworld-outsmarting-terrorists-hackers-and-spies, accessed February 1, 2018.
2. Krebs on Security. "Petya' Ransomware Outbreak Goes Global', available at https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/, accessed February 1, 2018.
3. Reuters. "Global cyber attack could spur $53 billion in losses - Lloyd's of London", available at https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH, accessed February 1, 2018.
4. "Petya' Ransomware Outbreak Goes Global".
5. Symantec. *Internet Security Threat Report 2017*, available at https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, accessed February 1, 2018.
6. Repository of Industrial Security Incidents Database. "Hacker Takes Over Russian Gas System", available at http://www.risidata.com/Database/Detail/hacker-takes-over-russian-gas-system, accessed February 1, 2018.
7. TRENDMicro. "The State of SCADA HMI Vulnerabilities", available at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities, accessed February 1, 2018.
8. World Energy Council. *World Energy Perspectives: The Road to Resilience October 2016,* available at https://www.worldenergy.org/publications/2016/the-road-to-resilience-managing-cyber-risks/, accessed February 1, 2018.
9. Marsh & McLennan Companies, *MMC Cyber Handbook 2018: Perspectives on the Next Wave of Cyber*, available at https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf, accessed February 1, 2018.
10. Ibid.
11. Ibid.

WHY MARSH?

From the creation of the first cyber policy forms to modern privacy coverage, Marsh helps clients assess their cyber risks and build the right insurance program to meet their unique needs. Our global team of cyber and risk management colleagues provides an unbeatable combination of hands-on practical know-how and claims expertise, winning Advisen's "Best Cyber Risk Broking Team" for three consecutive years (2014-2016).

About Marsh

Marsh is a global leader in insurance broking and innovative risk management solutions. In more than 130 countries, our experts help clients to anticipate, quantify, and more fully understand the range of risks they face. In today's increasingly uncertain global business environment, Marsh helps clients to thrive and survive.

We work with clients of all sizes to define, design, and deliver innovative solutions to better quantify and manage risk. To every client interaction we bring a powerful combination of deep intellectual capital, industry-specific expertise, global experience, and collaboration. We offer risk management, risk consulting, insurance broking, alternative risk financing, and insurance programme management services.

Since 1871 clients have relied on Marsh for trusted advice, to represent their interests in the marketplace, make sense of an increasingly complex world, and help turn risks into new opportunities for growth. Our more than 30,000 colleagues work on behalf of our clients, who are enterprises of all sizes in every industry, and include businesses, government entities, multinational organisations, and individuals around the world.

We are a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With 65,000 colleagues worldwide and annual revenue exceeding $14 billion, Marsh & McLennan Companies also include global leaders Guy Carpenter, Mercer, and Oliver Wyman.

Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to BRINK.

MARSH

To discuss how Marsh CyberShield and the Marsh Cyber Assurance suite of cyber risk solutions can provide cover and peace of mind for your business, please speak to your Marsh client executive, or contact:

MARSH MINING PRACTICE

MATTHEW GOODA
Global Mining Practice Leader
matthew.gooda@marsh.com
+44 20 7357 3017

AUSTRALIA

JAMIE COUGHLAN
Australian Mining Practice Leader
jamie.coughlan@marsh.com
+61 7 311 54530

CANADA

ANDREW KWOK
Canadian Mining Practice Leader
andrew.c.kwok@marsh.com
+1 604 443 3588

SOUTH AFRICA

DEBBIE GERAGHTY
African Mining Practice Leader
debbie.geraghty@marsh.com
+2711 060 7759

UNITED STATES

RICHARD KIMBALL
US Mining Practice Leader
richard.kimball@marsh.com
+ 1 303 308 4563

BRAZIL

WELLINGTON ZANARDI
Brazilian Mining Practice Leader
wellington.zanardi@marsh.com
+55 11 3741 2483

CHILE

LUIS FERRADA
Chilean Mining Practice Leader
luis.ferrada@marsh.com
+56 2 2450 5832

MEXICO

CARLOS ORDÓÑEZ
Mexican Mining Practice Leader
carlos.ordonez@marsh.com
+52 55 5999 4446

PERU

CÉSAR KAHATT
Peruvian Mining Practice Leader
cesar.kahatt@marsh.com
+51 1 604 1371

EUROPE

DAVID BENNING
European Mining Practice Leader
david.benning@marsh.com
+44 20 7357 5870

RUSSIA

ANDREI DENISSOV
C.I.S. Mining Practice Leader
andrei.denissov@marsh.com
+7495 787 70 80

INDIA

ANUJ SINGH
Indian Mining Practice Leader
anuj.p.singh@marsh.com
+1 244 049 205