Willis Towers Watson

From technology to people:

The new frontier in mining cyber risk

No immunities, no boundaries – the risk is systemic...

Cyber security represents a fundamental challenge for organisations and is seen as a top priority for boards. Malicious hacking, ransomware attacks, data leaks and electronic fraud are occurring on a global basis, where the motives vary from financial, political or merely to cause disruption. The recent global ransomware incidents WannaCry and NotPetya have shown us that:

- **No one is immune.** Attacks do not need to be targeted at a specific company or industry sector.
- **Cyber-attacks lack a geographical boundary.** Rogue actors are easily able to bridge the geographical boundaries of an organisation's operation that do not exist in the globally connected world.
- The potential **systemic risk** which can arise from a cyber-attack **is far from theoretical.**

Mining industry particularly vulnerable

Within the mining sector, the convergence of IT and operational technology (OT) through industrial automation, the uptake of smart devices for real-time operations management and remote operations, and the adoption of cloud services are driving significant change to a mining company's operational model. The modern mining company is a transnational corporation, running highly coordinated production operations across multiple sites in multiple countries with varied geopolitical climates, all the while responding to the supply and demand needs of a market-driven economy.

Transformation of working practices

Technology has transformed working practices leading to increasing productivity and driving operational efficiency and innovation. However, this increased adoption and reliance on technology does not come without increased risk and as devices become more connected and processes more digitised, mining companies will need to contend with an increased number of network born security threats. Never has industry been more susceptible to operational derailment and ultimate financial loss due to a cyber-attack.

Connected mining sites and their supply chain require an ongoing programme of investment and monitoring to ensure security and availability are maintained across the entire IT & OT estate to prevent business disruption.

It's not just a technology issue!

In our recent 2017 Cyber Risk Employer Survey (include link) 76% of companies reported that they have improved their technology systems and infrastructure over the last three years. While this shows that companies around the world are focusing their time, resources and budget on technology solutions, most companies still perceive themselves vulnerable to cyber incidents.

While critical to protecting the enterprise, technology is only one piece of the solution. This is again evident from our survey, which shows almost 75% of organisations report that in the next three years, they intend to allocate more capital to human capital solutions (such as comprehensive training programmes for employees) and business processes.

Never has industry been more susceptible to operational derailment and ultimate financial loss due to a cyber-attack.

Human Resources and CISO personnel now playing key roles

Although IT departments – and to some degree, risk managers – are seen as responsible for cyber risk management strategies, other functions such as Human Resources and Chief Information Security Officers (CISOs) are increasingly playing an integral role in protecting the enterprise and creating a cyber-savvy workforce.

The majority of cyber incidents are ultimately sparked by employee behavior (whether through negligence, accidents or intentional acts). Our cyber insurance claims data shows two-thirds of incidents are the direct result of employee behavior – for example, negligence leading to lost devices and malicious and disgruntled insiders seeking to profit from corporate espionage. When analyzing the other 33% of incidents, a large portion can ultimately be traced back to additional human errors that can be linked to issues such as talent shortage, skill deficits and employee engagement.

The value of information is rising

The theft of individuals' personal information and personal financial information has long been a motive behind a number of highly publicized cyber incidents. While this continues to be an area of focus, cyber criminals increasingly understand the value of a much wider range of sensitive data, whether in terms of an opportunity for direct monetary gain or in manipulating business dynamics.

Examples such as theft of intellectual property around production methods or theft of pricing data for metals and minerals by competitors to hijack sales, could all be potential motives. In a competitive market, the importance and value of this information cannot be overlooked. Having a robust information security programme should not be viewed as a cost but rather an essential investment and an opportunity to gain competitive advantage, generating increased confidence with customers and investors seeking to protect the value of their investment.

Regulation continues to tighten

Regulation relating to cyber and information security has historically been focused around data privacy and data protection issues; however, regulatory scope is expanding to encompass infrastructure and providers/operators of essential services. This is a trend which will continue, particularly with the increasingly connected nature of systems, data and services providers. As with any regulation, this will drive the behaviour of organisations to achieve compliance, as the potential financial and reputational consequences of not doing so can be significant.

Managing the consequences of an incident

The cascade of events and disruption following a cyber-incident can be far reaching; for example, the financial impact on some of the companies impacted by the NotPetya ransomware outbreak is estimated to be in the hundreds of millions of dollars. The insurance market in this area has continued to evolve, particularly for those sectors where both IT & OT exposures exist.

Risk Transfer solutions

From a coverage perspective the insurance market draws a distinction between:

- Cyber-attacks leading to **physical outcomes** (e.g. property damage, bodily injury etc.). In this context, the insurance approach can vary from coverage being specifically excluded, specifically included or silent (i.e. neither specifically included or excluded).
- Cyber-attacks leading to **non-physical outcomes** (e.g. loss of data, network outages, extortion demands). The insurance market has developed broad stand-alone product offerings for these exposures some of which can include added access to added value services around incident response to support recovery post event.

Our 2017 Cyber Risk Employer Survey shows that nearly nine in ten companies have reviewed or will review their cyber insurance arrangements within the next two years, with a view to identifying gaps in existing insurance coverage. In addition 71% of respondents advised that they expect to enhance their insurance coverage within the next two years. The insurance market continues to develop its understanding of the cyber risk environment through the collection (and modelling) of more consistent data and this is driving a willingness to develop new products and services to keep pace with this evolving exposure.

What should organisations do?

To manage cyber risk effectively across the enterprise and ensure resiliency, organisations need a fully integrated, comprehensive plan that emphasizes people, capital and technology protections. Understanding the risk exposure across both IT and OT and investing in the appropriate security is vital to remain ahead of the curve and present financial, reputational and intellectual property risk. In particular mining companies should remember;

- **IT solutions can't be adopted and implemented in a vacuum.** People and technology need to have a symbiotic relationship to ensure Cyber security is connected to the business and not simply a superficial wall surrounding an organisation. Cyber risk is complicated; as such, the constantly evolving and dynamic environment demands agile solutions to combat new threats that many organisations may not be tracking.
- **People risks are the next frontier in cyber risk management.** Understanding that technology solutions are only as effective as the people operating and managing those solutions is critical. Organisations need to engage with their IT department and uncover skills deficits and talent shortages in critical roles to ensure that talent strategies align with overall cyber-security objectives. By taking these steps, you can ultimately help improve your employees' "Cyber IQ", create a cyber-savvy workforce and ensure cyber resiliency across all levels of your organisation.
- **Assume it's going to happen.** The notion that *'it won't happen to us'* continues to be disproved therefore preparation is key. When a cyber incident occurs, having a well-developed and well-rehearsed cyber incident response plan will be critical to ensuring a quick recovery, thereby mitigating the longer term financial, regulatory and reputational damage.
- **Transfer the risks you can't remove.** A robust cyber risk management programme will reduce the probability of an event occurring, but you can never fully eliminate the risk. Cyber insurance risk transfer solutions exist to mitigate the financial impact when things go wrong. As a starting point, check your existing insurance coverage; understand what cover you've got and what options are available.

Glynn Thoms *is Executive Director Cyber & TMT at Willis Towers Watson London*

Bangkok

Multi-Risk Consultants (Thailand) Ltd.
21st Floor, Vongvanij B Building
100/64-66 Rama 9 Road,
Bangkok 01320, Thailand

T: +66 2 645 0040

Beijing

18th Floor, West Tower
Twin Towers
B-12 Jian Guo Men Wai Avenue
East Chang'an Street
Chaoyang District
Beijing, PRC 100022

T: +86 21 3887 9988

Brisbane

Level 1, 10 Eagle Street
Brisbane, Queensland 4000
Australia

T: +61 7 3167 8500

Calgary

350 7th Avenue S.W.
West Office Tower, Suite 2200
Portion of Floor 22
Calgary, Alberta T2P 3N9
Canada

T: +1 403 263 6117

Johannesburg

Illovo Edge, 1 Harries Road
Illovo, Johannesburg 2196
South Africa

T: +27 11 535 5400

Knoxville

265 Brookview Centre Way
Brookview Promenade
Suite 505
Knoxville, Tennessee 37919
United States

T: +1 865 588 8101

Lima

Avenida De La Floresta 497
San Borja 602, 603, 604
Lima
Peru

T: +51 1 700 0202

London

51 Lime Street
London, EC3M 7DQ
United Kingdom

T: +44 (0)20 3124 6000

Melbourne

Level 4, 555 Bourke Street
Melbourne, Victoria 3000
Australia

T: +61 3 8681 9800

Miami

1450 Brickell Avenue
Suite 1600 Floor 16
Miami, Florida 33131
United States

T: +1 305 421 6227

Perth

Willis CKA
Level 4
88 William Street
Perth, Western Australia 6000
Australia

T: +61 8 9214 7400

Singapore

6 Battery Road
Floors 05-01, 06-01, 06-02
Singapore 049909

T: +65 6 591 8000

Toronto

100 King Street West
1 First Canadian Place
Suite 4700, Floor 47
Toronto, Ontario M5X 1E5
Canada

T: +1 416 368 9641

Follow us on LinkedIn.com (search for 'Willis Towers Watson Natural Resources Industry Group')

Download our 2016 Natural Resources Risk Index:
https://willistowerswatson.com/en/insights/2016/06/natural-resources-risk-index-2016

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

20502/09/17

willistowerswatson.com

Willis Towers Watson