



Gone phishing

Dan Gleeson receives two perspectives on cybersecurity: one from the mining supplier network and one from the mining community itself

“There is a fine line between securing your operations and implementing innovations or production enhancements.”

These are the words of Ian Lee, Manager, IT Security, Compliance & Enterprise Architecture at Hudbay Minerals, who neatly spells out the dilemma mining companies face in today's digitally connected world.

It is not a matter of choosing one or the other – cybersecurity or productivity-enhancing technology – it is all about discussing what impact adopting innovative solutions will have on the digital ecosystem at mine sites or company headquarters.

Apala Ray, ABB's Global Cybersecurity Manager, Process Automation, Process Industries, has been involved in a few of these conversations and knows the potential pitfalls mining companies can leave themselves open to.

She is also abundantly aware of the benefits that come with adopting new digital and automation solutions. They offer “mining operators unprecedented visualisation across their operations, allowing them to make smart, informed decisions that improve production efficiency”, she told *IM*.

Yet, this increased interconnectedness between operational technology (OT) and information technology (IT) systems makes industrial plants more vulnerable to sophisticated cyberattacks, Ray cautions, hinting at Lee's opening point.

This means there is a decision-making process to go through even before implementing these solutions.

The cyber threats can take the form of generic

‘white noise’ attacks that impact both IT and OT systems, as well as attacks using custom malware specifically crafted to infiltrate the target environment, according to Ray.

This means cybersecurity must be addressed at each phase of an asset's lifecycle – from design and development, to operations and maintenance – identifying what needs to be protected, when attacks and security breaches occur and effective back-up and recovery plans.

Why us?

Despite this impending threat, cybersecurity is not top of mind for miners implementing new OT, according to a 2019 State of Play report on cybersecurity in mining.

Through interviews, survey and analysis of Australia's largest mining and service companies, including BHP, Rio Tinto, South32, and Anglo American, the ‘State of Play: Cyber Security Report’, from researchers at State of Play, uncovered that 98% of top-level executives thought a catastrophic event was required to drive an industry response to cybersecurity in mining.

The reality is that this ‘catastrophic event’ has not yet occurred in the mining space, although it is getting nearer.

In March 2019, Norsk Hydro, a global aluminium producer, found itself the subject of an attack. This came in the form of a compromised email sent via an existing customer's email address to an unsuspecting employee. The employee opened the attachment and unknowingly released a type of

ABB's Apala Ray says more and more cybersecurity solutions are emerging to protect clients, but she places the onus on mining companies to develop a “coherent cybersecurity strategy”

ransomware that gave cyber criminals access to the Norsk Hydro network.

Earlier that year, hackers blocked access to Nyrstar's IT systems, databases and email to try and disrupt operations.

While both incidents are noteworthy, neither packed the same punch as the ‘NonPetya’ ransomware incident in 2017. While this ‘white noise’ cyberattack did not specifically target the industrial sector, it hit Maersk, the world's largest shipping firm. This ended up costing the company \$300 million, taking almost 10 days to rebuild the affected network of 4,000 servers and 45,000 PCs.

These warnings aside, there continues to be a worrying perception that most mining companies are too small or insignificant for hackers to target. The obvious rationale for an attack on a junior mining company, for instance, is hard to understand.

Lee has heard this argument but says such complacency is unwarranted.

“Hudbay in the grand scheme of things is a relatively small company, but every hacker will practice somewhere,” he told *IM*. “These hackers are not going to start taking on the big guys; they will start with the small guys and see what they can accomplish at that level before moving onto bigger targets.”

Armed with this knowledge, Lee and his team devised a sophisticated cybersecurity training program back in 2018 to help protect employees and the company from such attacks.

With 94% of malware delivered via email and phishing attacks accounting for more than 80% of

reported security incidents, according to csoonline.com, the training focused mainly on potential email phishing attacks.

Hudbay teamed up with **Infosec IQ** to rollout this testing and training.

Having found a baseline of what Infosec referred to as “phish-prone users” back in 2018 through several exercises looking to replicate typical phishing behaviour, Hudbay started flagging internal examples of malicious emails that had come through to the company from external sources.

“We then highlighted some of the tell-tale signs to show how they were fake,” Lee explained. “This could be a misspelling of Hudbay Minerals, wrong grammar, etc. These were the standard things people needed to be aware of that they used to gloss over prior to them being highlighted.”

Going into 2019, Hudbay, backed by Infosec’s program, then started to deploy continual phish testing to compare users with the baseline they had confirmed the previous year.

“This could be one, two, three emails a month that were simulated phishing emails,” Lee said. “As soon as people clicked on something they shouldn’t have, they received immediate feedback to make them aware of things they should watch out for. At the same time, the system noted the behaviour for us to review on a regular basis.”

In tandem with this, monthly training courses were rolled out covering phishing, flash drives and safe web browsing.

The program led to a dramatic decrease in phish-prone users within Hudbay, with the metric going from 44% in the March quarter of 2018 (initial testing) to just 5.5% in the September quarter of 2020.

Lee says the training has been a worthwhile exercise the company plans to continue with.

That is not to say it has been easy getting all employees on-board with increasing their cybersecurity awareness.

“There definitely are people that understand the need and usefulness more than others,” he said. “It is sometimes challenging to convince personnel it is worth their time to engage with this training.”

Physical on-site safety has buy-in across the board at mine sites, but the less ‘tangible’ threat that comes with cybersecurity is harder to get across to personnel.

“If we lost \$1,000 in an accounts payable scam that is one thing, but if we have a mill that fails, for example, that affects the physical process,” Lee said. “This type of example tends to get more traction and attention across the company.”

Lee and Hudbay are committed to increasing engagement with this cybersecurity training.

The company currently has a 60-70% participation rate in the training process, which will increase when Hudbay makes it mandatory in the near term.

Engagement and awareness may also increase when the phish testing becomes much more targeted, directing relevant emails quoting actual employees



and what appear to be genuine instructions during these tests, Lee explained.

This reflects the increased sophistication of phishing emails the company is already getting.

“These testing emails will be more specific and relevant to the users, targeting their specific group,” Lee said. “The emails we are receiving are already becoming that much more targeted, with the phishers directing what appear to be normal requests to the right people.”

Layered protection

Hudbay chose its ongoing cybersecurity training program to augment existing technical controls where further investment in such controls may have diminishing returns, according to Lee.

Based on his 15-plus years of experience in IT, Lee indicated staff can often rely on the technical controls of cybersecurity solutions to safeguard them should such third-party protection be employed. This would not be a problem in an environment where malware risks do not evolve, but the speed and complexity of changes coming from this community means such protection needs to constantly be updated.

“It really is a game of whack-a-mole; you are never going to catch them all,” Lee said. “We could put in all of these technical controls – enhanced malware protection, phishing and web filters, for example – but you are always going to be playing catch up.”

ABB’s Ray says more and more cybersecurity solutions are emerging to protect clients, but she places the onus on mining companies to develop a “coherent cybersecurity strategy”. Layered onto this strategy can be measures to protect assets, processes and people from imminent danger.

She thinks partnering with a recognised technology leader can provide protection against imminent cyber danger.

This is where ABB, as a maintenance service provider, an integration service provider and a product supplier, has an advantage over some of its peers, Ray argues.

ABB’s cybersecurity portfolio is built around three layers: foundation, service and operation.

“In the mining sector, the first foundation layer is of particular importance,” Ray said. “US Homeland Security reports that 98% of cyberattacks can be

Hudbay’s Ian Lee says every system the company installs, or every change made to operational technology must go through an internal IT and ICS policy

mitigated if industrial operators have basic digital hygiene and process controls in place, including the latest anti-virus software and a regular back-up system.

“To protect industrial facilities from undetected ‘zero-day attacks’ from advanced persistent threats such as ransomware, ABB also advises that network segregation and recovery processes are put in place; the latter allowing mining companies to maintain production following a cyberattack.”

The ABB Ability™ CyberSecurity Fingerprint solution provides customers with an initial in-depth site survey to assess their existing cybersecurity control system. Combining data from an ABB Ability Cyber Security Benchmark control system asset risk review with insights from plant personnel, ABB can then advise the client on risk mitigation and how to improve its overall cybersecurity profile.

Ongoing security patches and antivirus software need to be constantly reviewed as part of this.

“Keeping these basic function controls updated is part of the second layer of ABB’s cybersecurity portfolio,” Ray said.

The third layer of protection involves operational security monitoring in collaboration with strategic partners, using advanced analytics to predict and identify evolving security threats, and adapting solutions from the IT sector – IBM QRadar and Splunk, for example – for use in the OT space, Ray says.

ABB has an existing relationship with IBM. The two signed an agreement back in October to develop a new OT Security Event Monitoring Service that combines ABB’s process control system domain expertise with IBM’s security event monitoring portfolio to improve security for industrial operators like mining companies. This new service better connects OT data with the broader IT security ecosystem, providing the domain knowledge needed to swiftly react to security incidents related to process control, according to the companies.

While ABB is evidently well schooled on cybersecurity risks, Lee has seen mixed responses

from the wider mining vendor community.

“The newer vendors to this space that are not as established in the mining PLC, automation and industrial control system type of stuff tend to have these controls in-built from the off,” he said. “This could be integrated login and user identity access management; everything you would expect on the corporate side, they are also doing on the control side.

“Some of the legacy vendors are either trying to bolt on these newer requirements or are looking for ways around it.”

According to Ray, all companies in the mining vendor ecosystem have responsibilities to protect end users.

“The asset owner, the maintenance service provider, the integration service provider, and finally the product supplier all have clearly defined responsibilities, and must work together,” she said. “Industry standards such as IEC 62443 help mining operators and technology providers such as ABB to identify risk: ‘do we need high-end solutions, or can

we afford to employ lesser measures based on the risk exposure?’”

“As asset owners, customers are in charge of cybersecurity strategy and associated risk throughout the life cycle. The maintenance service provider reviews the technical, process and organisational measures across the holistic protection scheme to assess if security measures are fit for purpose.

“The integration service provider develops and validates this holistic protection scheme and maps the residual cybersecurity risk. The product supplier takes into account the requirements of the target market, shares technical documents with integration and commissioning providers, undertakes vulnerability assessments, and ultimately deploys cybersecurity technologies to industrial clients.”


Lee says cybersecurity protocols are improving across the board, but mining companies need to confirm they are asking the right questions to ensure they are getting a secure system. This is becoming more important with every new OT and IT system that is installed to boost productivity, streamline

operations, or reduce costs at mine sites or mining company offices.

“Everything is internet connected these days and every vendor wants their equipment to report into their portal to let them know when they need to replace a bearing, drive, pulley, for instance,” Lee says.

This leaves the operation susceptible should an attacker want to gain access to site architecture; a fact Lee is abundantly aware of.

“While I believe our security controls are above industry norms, we are constantly debating what holes may open up should we implement new solutions to increase production, productivity, etc,” he said. “Every system we put in or every change we make has to go through our IT and ICS policy. There are various layers in between that, which need to be considered.”

More miners will in the future be following the example Hudbay has set, and the vendor community needs to acknowledge this when releasing the next new, shiny solution. 

The Operational Technology Cyber Security Alliance (OTCSA) has, at its core, an aim to bridge any dangerous gaps in security for operational technology (OT) and information technology (IT) systems, critical infrastructure and industrial control systems to support and improve the daily lives of citizens and workers in a rapidly evolving world.

Its mission is five-fold. Namely to:

- Strengthen cyber-physical risk posture of OT environments and interfaces for OT/IT interconnectivity;
- Guide OT operators on how to protect their OT infrastructure based on a risk management process and reference architectures/designs that are demonstrably compliant with regulations and international standards such as IEC 62443;
- Guide OT suppliers on secure OT system architectures, relevant interfaces and security functionalities;
- Support the procurement, development, installation, operation, maintenance, and implementation of a safer, more secure critical infrastructure; and
- Shorten the time to adoption of safer, more secure critical infrastructures.

In September last year, IntelliSense.io became a new member of OTCSA to further its aim of providing miners with a safer future with secure optimisation technology that can leverage both OT and cloud environments.

IntelliSense.io has been securely deploying artificial intelligence-based based process optimisation applications on OT networks for its customers globally and, it says, has a future-proof platform.

Dr Sandro Barros, CTO, IntelliSense.io, said the convergence of OT and IT networks is exposing industrial control, protection and automation systems to external threats, as seen in the recent past with malwares like Triton that attacked an oil and gas plant, and in Ukraine, that had its power grid taken down by a cyberattack.

“IntelliSense.io has extensive experience on the deployment of AI applications within OT/IT networks and is eager to add its expertise to



IntelliSense.io has been securely deploying artificial intelligence-based based process optimisation applications on operational technology networks for its customers globally and, it says, has a future-proof platform

developing best practices for secure and reliable solutions for the mining industry,” Barros added.

Elad Ben-Meir, Executive Board Member of the OTCSA and CEO of SCADAfence, welcomed IntelliSense.io as its newest member, explaining there was a need for further collaboration in the cybersecurity environment.

“As we witness more and more attacks on critical infrastructure, and predictions by Gartner that 75% of CEOs will be personally liable for cyber-physical security incidents by 2024, there is no doubt that the collaboration like we have in OTCSA is the key to success,” Ben-Meir said.

The robust security guidelines of the OTCSA, which IntelliSense.io will contribute to, cover the entire mining life cycle – procurement, development, deployment, installation, operation, maintenance and decommission – and address aspects related to people, process, and technology.