Commodity Trading Insights

Cyber Security and Commodity Trading

1. The evolving threat ecosystem

Commodity traders come in all shapes and sizes. They are engaged in transformation activities, over all types of commodities, from extraction and processing to logistics and storage. Some hedge their risks in their business activities, and most do not actively speculate directly in commodity price movements. Risk management is a key component of operations and a key part of the business model.

As information security professionals we perceive that in comparison to similar financial services businesses commodity traders face an increased threat to their specialist systems and processes from the latest, highly motivated and sophisticated attackers. The methods they use cause disruption, financial loss and reputation damage if successfully executed.

We are now seeing specific growth in the risks posed to technology-dependent trading operations, especially where the financial (and kudos) return for the attacker may also be much higher.

In this context, we have set out the security risks that have developed from these emerging trends.

2. Growth and acquisitions create new risks

Trading companies have, for the most part, a growing **global IT presence**, due to their organic and inorganic growth strategies. In addition, they operate in some of the world's fastest developing economies, which are also still developing a national ICT infrastructure. This global IT "footprint" leads to a large **attack surface** that has to be defended (each local office and computer network potentially represents an entry point for an attack).

3. Perception increases the threat

There is also a perception amongst some politicians, journalists, financial commentators, and environmentalists that commodity traders are not only engaged in extracting and processing key minerals and commodities from sources in developing countries, but also trading in those same commodities to increase profits at the expense of others. This perception in the minds of many people has led to the risk that such organisations could be subjected to attack over the Internet to disrupt their businesses.

The relationships between commodity trading companies and governments in the developing world, where many operate parts of their business, are also under constant scrutiny, subject to speculation and even regulatory investigation. Legal disputes discussed in the public realm and bribery allegations all heighten the perception that traders are acting solely in self-interest at the expense of other stakeholders.

Where the commodity traded is also part the human food-chain or a key energy resource, more suspicions arise in the minds of some about the role traders play in the world economy.

4. The Internet levels the playing field

One of reasons for this threat being different is that the Internet has allowed those who wish to do so to challenge any business, or business model they do not understand or are suspicious of, in a very direct way, and the Internet also allows the like-minded to work collectively. It is this dimension that has spawned hactivist groups, such as **"Anonymous",** to champion any social causes its members feel

pwc

should be addressed and level the "playing field" against the corporate world.

In addition, some of these same **environmentalists and anti-globalisation groups can also constitute a potential threat** to a commodity trader from a "physical" point of view, but it's far more likely and significant in the context of the cybersecurity risk that these groups could organise and collectively attack any target they feel deserves their wrath.

Whilst many commodity traders focus their risk management activities on core business, looking to diversify their asset risk, insure themselves and hedge large transactions, they do not appear to focus enough time and resources on these emerging external threats. In addition, the threat is not just to them, but also to the very markets in which they trade as these, too, can be the subject of an attack which might prevent traders from executing any trades (trading or hedging), even in their own positions, in commodity markets.

Depending on the precise business activities involved, commodity trading is very dependent on secure, operational computer systems; the speed of connections to financial exchanges to trade is important to some players, and their business models are driven by evolving technologies, data exchanges and new trading algorithms that help them to be more efficient and reactive.

These companies will have to improve their defences against the many new and evolving cyber threats.

5. The broader threat

The deployment of technology in all the business processes, combined with the current economic malaise, is driving innovation in the field of cybercrime.

For example, as information security experts we believe that globally, companies are not adequately prepared to face the new techniques that are being used as external threats, such as denial-of-service (DoS) attacks and the advanced persistent threat (APT). The sophistication of the threat is increasing.

The digital revolution is impacting information security way beyond the traditional models deployed. The responsibility for information security should not fall just on IT. It's a business-wide issue. Many trading companies may not have put in place adequate controls to protect against the magnitude of the threat.

They could really benefit from hiring an information security expert or consultants to challenge the current systems in place, identify threats and protect users from compromises.

6. Cyber Security Intelligence Switzerland

PwC recently conducted cyber security threat intelligence research on Swiss Internet service providers whose users had been compromised within the last 90 days. PwC found 14,000 domains through which user credentials had been stolen by botnets run by criminals.

7. Next steps

No one should down play the current threat to the sector. Organisations need to complete a thorough risk assessment of their operations and take appropriate measures. One way in which organisations can take stock of their current situation is to carry out a cyber threat risk assessment and take an in-depth look at the threats by using the intelligence gathered about those that would wish to attack the organisation. They can then invest in the most effective counter-measures.

Contacts

Robert Metcalf
robert.metcalf@ch.pwc.com
+41 58 792 92 42

Kevin Kirst
kevin.kirst@ch.pwc.com
+41 58 792 2877