



Metts



Ritter

## Pipeline Security: Investment or Expense?

By Luke Ritter and Timothy Metts

Experts have suggested that pipeline operators have two basic options for developing a security management strategy: Do the minimum required for compliance with a clear understanding of the residual risks, or develop and implement a proactive, managed risk approach that treats security as a core business function. Can effective security management produce a significant return on investment? Are companies that view risk management as an expense, rather than an investment, missing an opportunity to exploit a value opportunity? Does the industry recognize the threat to pipelines as a persistent and pervasive risk? Two industry veterans, one with deep knowledge in the security sector and the other with 10 years of risk management experience, provide their thoughts on these issues. Luke Ritter and Timothy Metts provide their joint argument for proactive security management.

**Q.** *How can a pipeline company determine its “risk appetite,” which the insurance industry defines as the level of risk that an organization is willing to accept.*

Tolerance for exposure can vary greatly, even within the same industry segment. As a precursor to managing security risk, it is essential for a company to determine its risk appetite. This can be done using an analysis that accounts for a combination of threats, vulnerabilities and contingent events as they compare to a firm’s security posture. It’s interesting to note that often a company’s risk appetite does not match its actual level of exposure. True exposure can dwarf appetite and the capital available for mitigation. Risk averse businesses are often paralyzed by an inability to quantify the exposure when they should be aggressively investing in security. This highlights the importance of a structured process with which quantitatively defined, risk-cognizant key objectives and metrics can be developed.

**Q.** *What is the impact of not having a secure and resilient enterprise? Can you offer some examples?*

In Michigan, nearly 1 million gallons of crude oil recently leaked into a creek, which flowed into the Kalamazoo River, due to corrosion. The pipeline operator has estimated \$300 million to \$400 million dollars in pending insurance claims. The spill contaminated 37 miles of the river before it could be contained and mitigated.

In another recent incident, 28 people were killed and 52 injured, when a crude oil pipeline exploded in Mexico. Thirty homes were destroyed, Army troops were deployed, 500 people were evacuated to temporary shelters, and a bridge was rendered unusable. Deliberate tampering for theft has been traced as the root cause of this catastrophic event.

These are just two examples of at least a half dozen catastrophic pipeline events that have occurred in the last year. Threats may be natural, manmade or due to mechanical failures. The cause, however, is not nearly as important as the consequence. Over time, a company’s customers, institutional investors, insurers and regulators tune in to positive and negative business influences — security is an important metric. It is hard to argue that a more secure and resilient pipeline is not a more valuable one. However, without understanding the risk exposure, companies lack the understanding to make investments to enhance and upgrade their security practices. Companies that take a proactive approach are well positioned to develop risk mitigation strategies that maximize available capital and produce tangible benefits. Ultimately, these benefits will create a competitive advantage relative to companies that have not rigorously quantified and analyzed their risk exposure.

**Q.** *Can pipeline companies afford to invest in security as a core business function?*

The reality is that companies can’t afford not to invest in security as a core function. Making informed decisions to allocate scarce capital should include security and risk management considerations. In some cases, CEOs may be betting their company’s long-term viability on the chance that a catastrophic event won’t impact their enterprise. Forward-leaning corporations are striving to avoid what has been termed “willful disregard for the obvious” — which now includes, by default, a comprehensive and effective approach to risk management.

To survive in a rapidly changing business environment that includes persistent and pervasive security risk, it is essential that successful enterprises invest proactively in security management. Corporate decision-makers must be prepared to manage risk before it manages them — or be willing to accept the consequences. The process starts with understanding exposure and concludes with evaluating the trade-off of various investment decisions. Ultimately, proactive companies will address two fundamental questions, “What is the potential range of outcomes?” and, “What can I do to mitigate the exposure?”

Luke Ritter leads the Risk Management practice at Ridge Global and is co-author of *Securing Global Transportation Networks: A Total Security Management Approach* (McGraw Hill, 2006).

Timothy Metts is a commodity and enterprise risk management expert for Pace Global. He sits on the Risk Committees of many of the company’s largest clients, including electric utilities and gas distribution companies.