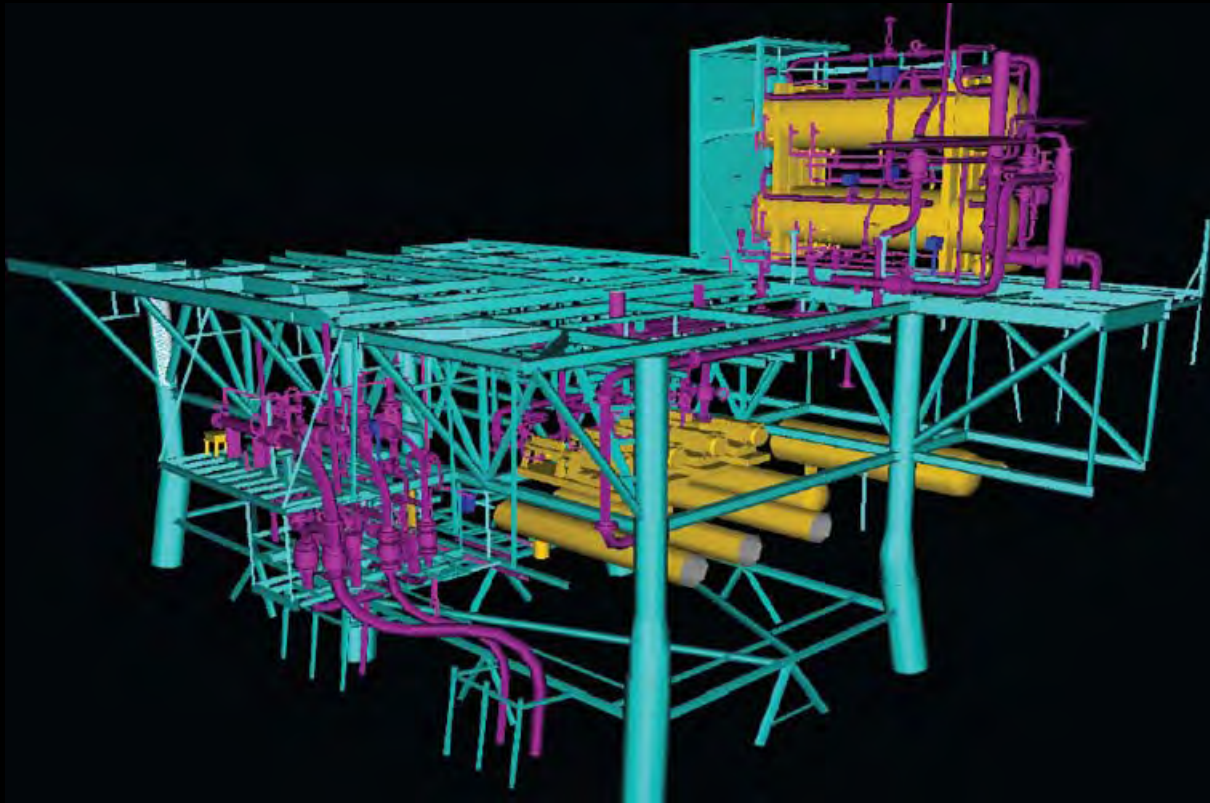


zeus

# TECHNOLOGY

magazine

A Focus on the Full Spectrum of IT Solutions for Oil & Gas



**E-mail Policy**

**Laser Scanning**

**Social Networking**

**Green Data Centers**



# MessageGate Uncovers Urgent Need for Stronger E-mail Controls

In light of the recent update to US Federal Energy Regulatory Commission (FERC) regulations, a new market study by MessageGate Inc. reveals that many regulated energy and gas companies still lack the required e-mail policy controls, training and education needed to maintain compliance. With a single e-mail violation under FERC leading to fines up to \$1 million per day, organizations are at tremendous risk of incurring costly penalties.

However, a preventative e-mail policy control can help organizations to centrally manage e-mail exchanges, especially between shared functions such as HR and IT to avoid triggering FERC violations and costly mishaps.

FERC Order 717, the most recent FERC regulation, requires organizations to manage and prevent communications between marketing function employees and marketing affiliates. Recent research collected during customer e-mail compliance audits through the MessageGate Activity Profile (MAP) service indicated that organizations in the energy industry have successfully formed ethical walls between different employee groups, yet lack the policy-specific e-mail controls to centrally manage e-mail exchanges, especially between shared functions such as HR and IT. Organizations without effective internal e-mail safeguards in place run a greater risk of incurring costly penalties in violation of FERC.

“Meeting compliance mandates, such as FERC,

head-on is critical to the trustworthiness and ultimately the success of companies in highly regulated industries,” said Brian Babineau, senior analyst Enterprise Strategy Group (ESG). “With Order 717 adding responsibility

onto already overburdened senior management, organizations must find ways to automate policy enforcement and report on the effectiveness of controls. MessageGate provides an active form of secondary insurance against a potential FERC violation or corporate data breach by enforcing corporate communication policies consistently, which allows energy and gas providers to focus on their core business and customers.”

The following tactics can help organizations comply with the recent FERC update Order 717 and avoid costly penalties:

1. Maintain equal market opportunities for all resellers. While ethical walls only control communications between marketing function employees and marketing affiliates, FERC requires that shared employees

must also observe ethical walls to preserve ongoing communications. Manage intentional and unintentional employee misuse by allowing only compliant messages that adhere to FERC’s “no conduit” rule, by monitoring and immediately acting upon inbound and outbound content, as well as messages sent within an organization, including attachments – all in real time.

2. Foster a culture of compliance and execution. The responsibility of maintaining a culture of compliance falls increasingly on the heads of senior

---

“Organizations of all sizes are pressed to take a proactive approach to e-mail risk management, implementing e-mail controls and policy enforcement that can be enforced in real time.”

- Norbert Orth, president and CEO, MessageGate.



management at regulated entities. Initiating a proactive e-mail security and archiving solution that implements technology and written policies for compliance protects employees at all levels. The automatic identification and prevention of policy violations can also enable management to educate employees and help change their individual behavior, reinforce proper practices and instill a culture of compliance.

3. Create and manage flexible e-mail user groups to prevent unintentional e-mail misuse. Under Order 717, gas and electric companies must control communication between transmission function employees and energy and market affiliates. Insufficient e-mail controls and casual e-mail misuse at the employee level can lead to potential data leaks and leave the door open to e-discovery problems. Consider a flexible policy engine that can be used proactively to create and apply e-mail controls and policies specific to FERC and maintain the separation required between user groups.

4. Measure compliance in real time. Energy and gas companies that lack a clear understanding of what is happening within their e-mail systems at any point in time decrease their ability to prevent violations and are at risk of violating FERC regulations. Through a proactive e-mail security and archive management solution, organizations can stop the risk of incidents within e-mail traffic in real time and provide IT with the ability to review and monitor e-mails within the live e-mail stream through a network

implementation.

5. Provide real-time blocking and re-routing of outbound e-mails. For companies to meet FERC requirements, a proactive e-mail risk management approach is required in order to block and prevent restricted information contained within e-mail from ever reaching restricted individuals based on group designations, or the parameters of content in the message or attachment. Providing real-time blocking and re-routing of outbound e-mail can make the difference between being in compliance and costly legal fines.

“As regulation in the energy and gas industry continues to tighten, organizations of all sizes are pressed to take a proactive approach to e-mail risk management, implementing e-mail controls and policy enforcement that can be enforced in real time,” said Norbert Orth, president and CEO, MessageGate. “With a history of helping companies navigate through increasingly complex regulations, such as FERC, MessageGate provides the critical foundation required for any organization’s proactive approach to building a culture of compliance.”

MessageGate facilitates enterprise e-mail risk management through e-mail controls and risk management software that incorporates active security and archive policies. MessageGate promotes proper e-mail use through activity profiles, archive categorization and policy enforcement.

[www.messagegate.com](http://www.messagegate.com)

## Data Hung Out to Dry: 9,000 USBs Left at Dry Cleaners

Data loss is at an all time high due to USB or memory sticks most people use to download and transport large amounts of sensitive data. A recent survey released by Texas-based data security experts Credant Technologies reported that in the last year, 9,000 USB sticks have been forgotten in people’s pockets as they take their clothes to be washed at the local dry cleaners. Dry cleaners in the suburbs, on the commuter belt or based in city centers find the most USB or memory sticks, the survey found. One dry cleaner in the heart of the City of London said he is getting an average of one USB stick every two weeks; another said he had found at least 80 in the past year.

The survey was carried out to gauge the frequency and ease with which mobile devices such as USB and memory sticks are lost or forgotten in strange places such as dry cleaners. The survey figures were based on phone interviews conducted among 500 dry cleaners across the UK, who on average had found two USB sticks during the course of a year. These figures were then multiplied by the total number of dry cleaners, which is 4,500, according to the Textile Services Association.

Credent uses the results as a warning to people across the globe to be vigilant when downloading information to carry around with them because it does get lost frequently.

A similar survey was conducted by Credant Technologies last September among taxi drivers in London and New York, which showed that more than 12,500 portable devices such as laptops, iPods and memory sticks are forgotten in the back of taxis every six months.

Michael Callahan, Sr. VP and chief marketing officer at Credant Technologies, said: “Although we conducted this survey in the UK, the idea was to show people everywhere how easy it is to lose data – even in their local dry cleaners – and that none of us is infallible. We’re convinced if we were to do the same survey in the US we’d get very similar results. If the data are sensitive or valuable, then people should protect this information with encryption so no one can access the data at any point, as it could easily end up in the wrong hands.”

USB devices now have the capacity to store as much as 10,000 Word documents, 11,000 pictures, 500,000 contact details or an amazing 1.1 million e-mails, making them an obvious target for identity theft criminals and hackers, who can steal this information and assume the identity of the user both in their personal or business life. Credent recommends encrypting all USB sticks every time data is stored on them.

[www.credant.com](http://www.credant.com)