Vaporstream

Secure Crisis Communications: Changing the Game in Energy and Utilities

Vaporstream

TABLE OF CONTENTS

Introduction

Swift and candid communications during times of crisis are key to executing successful response plans that mitigate risk. In a world of unprecedented natural disasters, increased cyberterrorism and evolving regulations – all of which are complicated by aging infrastructure – rapid and efficient incident and emergency notifications are more critical than ever. Every reaction to a crisis, however, is judged by public opinion and the financial markets, both of which can drastically impact investments.

Antiquated communication plans and methods that include such channels as fax, walkie-talkies, pagers, phone trees and email no longer suffice for today's challenging landscape. While newer methods such as social media have proven helpful to connect consumers during major events, they're unreliable and prone to misinformation, confusion and data leaks of sensitive information. Some companies have also turned to SMS text messaging due to its efficiency, however, SMS shares the same downfalls as social media.

As natural and man-made events have continued to evolve in magnitude and complexity, communications that offer no protections against third-party surveillance or unintended propagation are now also problematic and potentially devastating. When communicating sensitive details about a crisis, especially while discovery and containment are still in process, it is vital to a successful response plan that communications are kept secure and controlled.

> *In the midst of these new challenges and risks facing the energy and utilities industry, how can companies ensure successful, accurate and candid communications to execute rapid and efficient emergency response plans?*

The reality is that energy and utility companies need a **real-time, compliant and secure** means of communicating with their entire organization – including field operations, cybersecurity teams, legal, compliance and public relations – from a central communications hub. This is especially true during times of crisis, when the chain of communication does not stop at the walls of the organization. Companies need to immediately notify third-parties such as regulators and key warning points including emergency management offices and first responders. They must also be able to trust in communications cross-border with international offices and travelers. Trust that communications are secure, mitigates the risk of misinformation and enables the organization to control the conversation as the narrative of the incident at hand is formulated. If the public needs to be informed, mass communications can go out swiftly, and without error, to ensure proper notification and readiness.

Introduction

The Vaporstream Secure Messaging Platform for Energy is the real-time, compliant and secure enterprise solution used for confidential crisis communications, mass incident notifications and emergency response in the energy and utilities industry today. Whether a security breach, terrorist attack, infrastructure failure, natural disaster or loss of power grid, Vaporstream enables secure collaboration, automating secure, mass incident notifications and the necessary routine communications required during a crisis to ensure rapid response and reduced human errors.

Critical during small anomalies, scheduled test scenarios and other disruptions of operations, communications must be protected against third-party surveillance and potential information leaks caused by unintended data propagation. Unexpected exposure of sensitive information can unnecessarily jeopardize your business or lead to panic, all based on half-truths or misinformation taken out of context. Having a secure and compliant means with which to communicate is not only vital to having candid conversations about the situation at hand, but to controlling the narrative of the event, containing damages, meeting regulatory and legal requirements and your ability to quickly prioritize and allocate the appropriate resources during times of crisis. Vaporstream provides the energy and utilities industry with the crisis communication tool of choice to efficiently and securely collaborate while controlling the conversation – ensuring one source of truth during any crisis, something antiquated, and even popular, however, non- secure mass communication systems simply cannot do.

I. Managing the Risk of a Challenging Landscape

Mother Nature

The increasing number of high-profile natural disasters – many of unprecedented magnitude – such as earthquakes, wildfires and hurricanes are putting energy and utility companies in the spotlight. Consider the recent California wildfires: state utility companies were contending with being put under investigation for causing the fires, forcing them to choose between working around the clock to keep the power on to support makeshift shelters and reduce the number of missing persons, or turn off the power preemptively as a safety precaution and risk public ire. One utility company in particular saw its market share plummet by more than $7 billion once fire investigators announced the investigation.[i]

One utility company saw its market share plummet by more than $7 billion once fire investigators announced the investigation.[i]

In our ever-changing world, it is hard to prepare for everything. In 2017, energy and utility companies in Texas and Florida were better prepared for Hurricanes Harvey and Irma than previous storms, but they still fell victim to the shortcomings of social media communications. In Florida, emergency responders became so overwhelmed by social media communications that the US Coast Guard tweeted a request to call them instead. The inability to effectively manage communications tragically resulted in eight deaths after a transformer failed that powered the air conditioning at a shelter.

Cyberterrorism

As the industry adapts to smart cities and updates old infrastructures and systems, so too does it become more vulnerable to cyberattacks. Energy and utility companies have been subject to very sophisticated attacks, compromising corporate assets, public infrastructure and safety – putting critical infrastructure including railways, airports, plants and entire smart cities at risk. Symantec, a cybersecurity and software services company, recently reported that a campaign, known as Dragonfly 2.0, which uses a variety of infection vectors to gain access to a victims' networks, has been underway since at least December 2015, with a distinct increase in activity in 2017.[ii] In addition, Cisco Systems, a networking hardware company, reported numerous email-based attacks targeting the energy industry this past summer. It warned that these emails use a toolkit called Phishery which steals victims' credentials via a template injection attack.[iii]

Compliance Regulations

The energy and utilities industry not only has to answer to a variety of different regulatory authorities (FERC, EPA, NERC, NRC, DOE)[iv], it also has to be ready to adapt to evolving cybersecurity, renewable energy and infrastructure requirements. Over the past year, Federal Energy Regulatory Commission (FERC) has increased its focus on North American Electric Reliability Corporation (NERC), participating in a growing number of NERC audits and actively initiating FERC audits of compliance by entities subject to NERC cybersecurity (CIP) regulations. Regulation of cybersecurity operations and activities are expected to continue to evolve, with a mix of mandatory regulatory requirements and pressure to step up voluntary efforts. Meanwhile, NERC is in the midst of examining regulations around third-party vendors/supply chains and cross-border collaboration.[v]

Increased scrutiny from state and federal regulators (FERC, Pipeline and Hazardous Materials Safety Administration (PHMSA), and state public utility commissions (PUCs) are driving states to improve infrastructure safety and replace old, dangerous infrastructure in order to ensure public safety. Consider a gas pipeline explosion in Colorado last year: The Colorado Oil and Gas Conservation Commission ordered tests that showed failures on 0.35 percent of approximately 120,000 lines in close proximity to populated areas, with 13,000 lines showing uncertain results. The Colorado commission is now rewriting statewide flow line regulations.[vi]

Aging Infrastructure

Complicating the evolving challenges presented by natural disasters, cyberterrorism and compliance regulations is the immediate need – and sometimes scramble – to update aging infrastructure in order to keep pace with this new landscape. Developing smarter energy infrastructure (also known as grid modernization) is essential to enhance reliability, resiliency and security. It is necessary to mitigate risk; improve outage management and restoration; seamlessly integrate and manage DERs (distributed energy resources); and empower customers with more energy options and solutions.[vii]

In 2016, American electric companies invested $112.5 billion, a fifth-straight year of record-high capital expendatures, to build smarter energy infrastructure. [ix]

Unfortunately, developing a smarter energy infrastructure is a multibillion, multiyear endeavor. In 2016, American electric companies invested $112.5 billion, a fifth-straight year of record-high capital expenditures, to build smarter energy infrastructure.[viii] But smarter energy infrastructure is non-negotiable when combatting natural disasters. Since Hurricane Wilma in 2005, Florida Power & Light Company has invested over $3 billion to build a smarter and more resilient energy grid, upgrading transmission lines, power poles, installing nearly 5 million smart meters and more than 83,000 intelligent devices.[ix] FPL also plans to add 12 hardened service centers that can withstand Category 5 hurricanes by the end of the year.[x]

Corporate Reputation

In a world where both the news media and social media users are chomping at the bit to voice their opinions, maintaining control of your company's narrative remains harder than ever. The tiniest whisper of an issue, insinuation or rumor about a potential situation can lead to stock fluctuations, consumer mistrust and much more. The tiniest whisper of an issue, insinuation or rumor about a potential situation can lead to stock fluctuations, consumer mistrust and much more.

The tiniest whisper of an issue, insinuation or rumor about a potential situation can lead to stock fluctuations, consumer mistrust and much more.

Take Florida Power & Light Company's (FPL) experience during Hurricane Irma: because of the investments they made in smarter infrastructure, they were able to restore power to 90 percent of their customers within 10 days – as opposed to the 18 days following Wilma. In addition, fewer than half as many FPL substations were affected, and those that were came back online quickly. Automated switching helped to avoid interruptions for nearly 600,000 customers.[xi] Despite their success, just four days after Hurricane Irma, an article titled "Why Didn't FPL Do More to Prepare for Irma?" appeared in the Miami New Times [xii] and sparked a round of similar articles and social media complaints. The article went on to attack FPL's "highly touted storm-ready technology [for not working] after Irma," among other accusations. What should have been a story about FPL's success mitigating harm during Hurricane Irma – including restoring power to fifty percent of customers who were affected within one day – the media and the public turned into a devastating PR nightmare.[xiii]

II. Enterprise-Grade Secure Text Messaging: The Solution for Secure Crisis Communications

Internal and External Communications

A real-time, secure and compliant communication plan for times of crisis is the key to successful incident notification and emergency response. With a secure communications plan, global companies can immediately mass notify the appropriate internal staff and critical third parties, such as warning points, emergency management offices, first responders and regulators, when an incident or crisis occurs. This ensures that only the Executive Management team and the Strategic and Tactical teams are provided with the necessary information about the crisis until others need to be included. Routine communications can also be automated to ensure that constant communication occurs between field operators and headquarters, including real-time status updates, providing field staff greater knowledge about the event and more time to focus on the crisis at hand. Conversely, it also provides headquarters with the timely, candid information needed to prioritize and make important decisions quickly.

Automated communications provide headquarters with the timely, candid information needed to prioritize and make important decisions quickly.

With the **Vaporstream Secure Messaging Platform for Energy**, companies can securely collaborate when a crisis occurs. Organizations can pre-configure automated templates based on different event types, or routine communications, in order to speed up response times in answering the call to respond. Automated, secure notifications, assignments, check-ins and status updates mitigate room for human error while increasing situational awareness in the field for better decision making throughout the event. This allows your strategic and tactical teams to focus on the crisis at hand, while at the same time, automated templates can be adjusted in real-time if something unexpected occurs or if an incident turns out to be more serious or complicated than first anticipated.

As initial notification is critical to response times, Vaporstream provides persistent notifications and can even take over the smartphone to ensure that notifications are never missed; delivery/read receipts are visual and easily monitored and reported against to provide a quick picture of response times. Replies to notifications can also be monitored by one address or turned into secure group chats with a designated crisis team, allowing for candid collaboration during discovery, containment and response efforts. This enables comprehensive, secure and compliant collaboration as a crisis evolves and is eradicated.

Controlling the Narrative About Your Business

Maintaining your corporate reputation comes down to controlling the conversation and the narrative that surrounds your business. Too often an internal stakeholder or third-party business partner inadvertently shares a small piece of information which ultimately finds its way into the hands of reporters who are not informed enough to understand the bigger picture. Glorifying a crisis or reporting misinformation happens too easily. And as mentioned previously, any insinuation, speculation or rumor can negatively affect a corporation's valuation, customer loyalty and trust – something the media does not always prioritize in light of "breaking news".

Recipients cannot forward, share, save or otherwise distribute information sent to them, helping to prevent unintended propagation and leaks to the media or public mass.

Vaporstream gives you absolute control over the use and distribution of any information regarding your business sent via a secure Vaporstream message. This mitigates any inadvertent dissemination of sensitive information. Recipients cannot forward, share, save or otherwise distribute information sent to them, helping to prevent unintended propagation and leaks to the media or public mass. **Vaporstream's Secure Messaging Platform** provides companies with secure and controlled views of their information, allowing them to get in front of a crisis, avoiding the need for public relations to chase the story, but rather own the story. Companies can be confident that their executive, strategic and tactical teams can communicate about any crisis, contract or issue without worrying about surveillance or data leaks – and that they can deliver one truth that sets the narrative for the event.

Staying Compliant

The range of regulatory requirements, combined with the rapid rate at which those requirements are changing, demands a comprehensive and flexible information governance approach. Vaporstream's enterprise text messaging platform is secure, ephemeral AND compliant. As an option, organizations can archive a single instance of messages to a client-designated repository of record (such as a document/records repository, archive, etc.) for legal and compliance purposes. This ensures safe record keeping and secure access. Organizations can then perform audit and compliance reporting, review actions after an event and discuss lessons learned to improve decision-making processes moving forward.

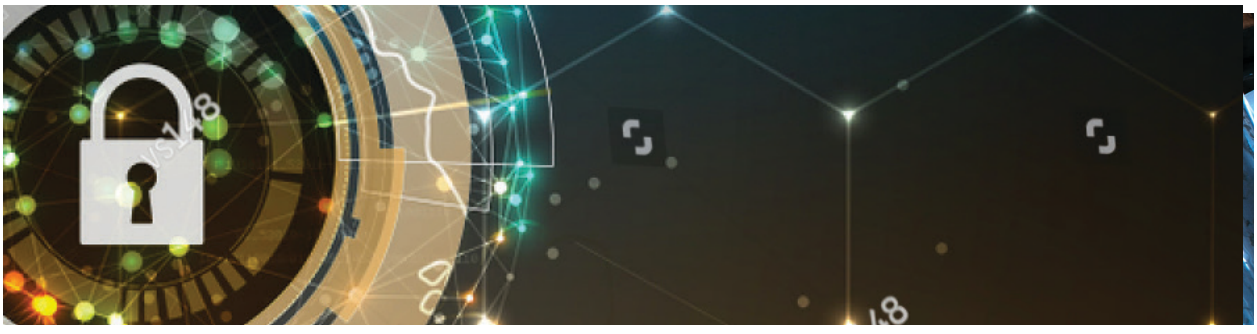
Keeping Bad Actors out of the Know

While cybersecurity is essential to a secure communication plan, unfortunately there is no foolproof way to prevent cyberattacks. As organizations strengthen defense-in-depth strategies, Vaporstream addresses cyber threats by providing a separate, confidential and secure communication channel when an attack occurs. Vaporstream goes beyond simple encryption of text to eliminate data leaks and ensures communications can continue – undetected and uncompromised – outside of your network. While you continue to discuss response and recovery with your teams via Vaporstream, bad actors - who typically monitor network communications in order to stay one step ahead - remain "out of the know". **Vaporstream** can be used in this manner for any IT outage or emergency scenarios.

Your Reputation – Our Secure Advantage

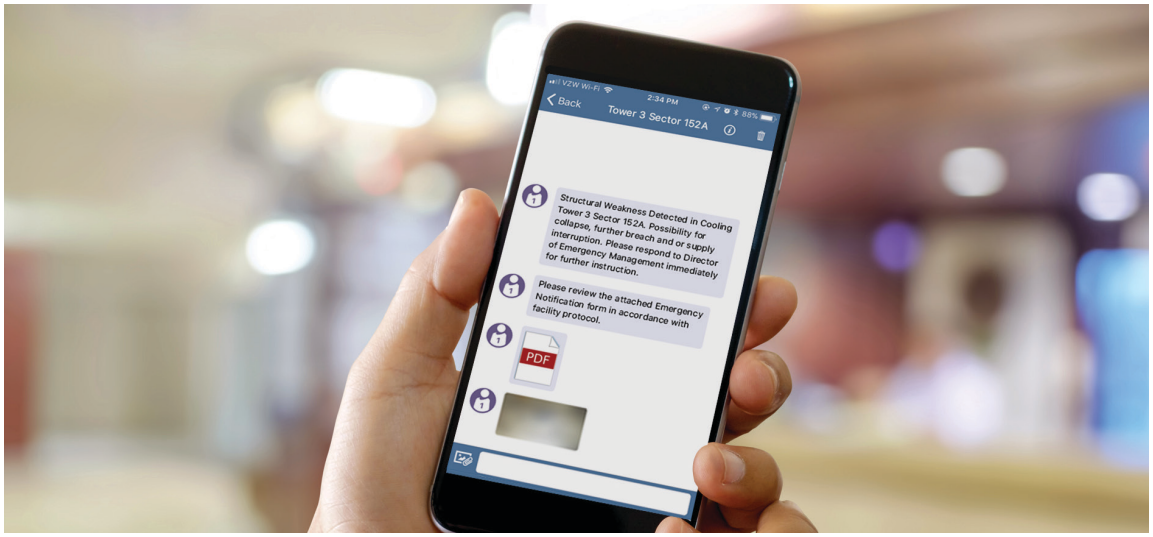
The award-winning, **Vaporstream Secure Messaging Platform for Energy** was built by security, privacy and compliance experts – each with over 30 years of experience in the content management industry. In fact, security and privacy are at the foundation of everything Vaporstream does. Our unique, multi-layered and patented security and access controls undergo rigorous testing - including third-party security certification by white hat hackers NowSecure. For the second year in a row, NowSecure has certified Vaporstream for its confidentiality, protection from breach and adherence to compliance requirements. By providing companies with a secure environment to communicate the most strategic, time-sensitive and confidential details that drive business, organizations can now communicate with confidence. Vaporstream keeps you in control of your content, where it is stored and its use - at all times: whether during a time of crisis, disruption of operations, test scenarios or simply routine, daily communications. Messages are also ephemeral, allowing companies to set timeframes that initiate "vaporization" of texts and metadata from all devices, providing additional protection against data leaks from unsecured, stolen or lost devices. Messages are never stored on Vaporstream servers and therefore Vaporstream employees never have access to your private information.

Vaporstream's unique, multi-layered and patented security and access controls undergo rigorous testing – including third-party security certification by white hat hackers NowSecure.



Vaporstream's Secure Messaging Platform Provides:

- Secure, compliant and rapid communications between the organization and staff, regulators, emergency management offices, first responders during a crisis.
- Real-time, secure collaboration with complete comtrol of your content, storage and use to ensure one source of truth. Advanced controls remove the risk of propogation; data leaks simply cannot occur.
- Encrypted text messaging in transit and at rest, eliminates the chance of data exposure, surveillance and man-in-the-middle attakcs. This allows secue cross-border collaboration with international offices or duging an international incident without fear of surveillance or data leak.
- Broadcast, group and individual messaging enables secure, real-time collaboration and rapid decision-making.
- Automated mass communications with predefined templates, recipients and more enable internal and B2B communications via secure, encrypted text as well as mass communications via standard SMS text to the public mass.
- Recurring notifications with the ability to take over the device to ensure that notifications are never missed, as well as indiviidual recieve/read indicators for easy visualization and reporting on response times.
- The ability to archive a single copy of messages to an organizational-designated "repository of record," for legal and compliance purposes.
- Ephemeral messages vaporize on demand or automatically after a predetermined interval of inactivity, based on your corporate policies to alleviate exposure risk due to lost or stolen devices.
- A secure, alternative communication channel, in the case that your network has been compromised, in order to keep bad actors "out of the know".
- Easy to deply and use for easy adoption; supports iOS, Android, Web desktop and Tablets.

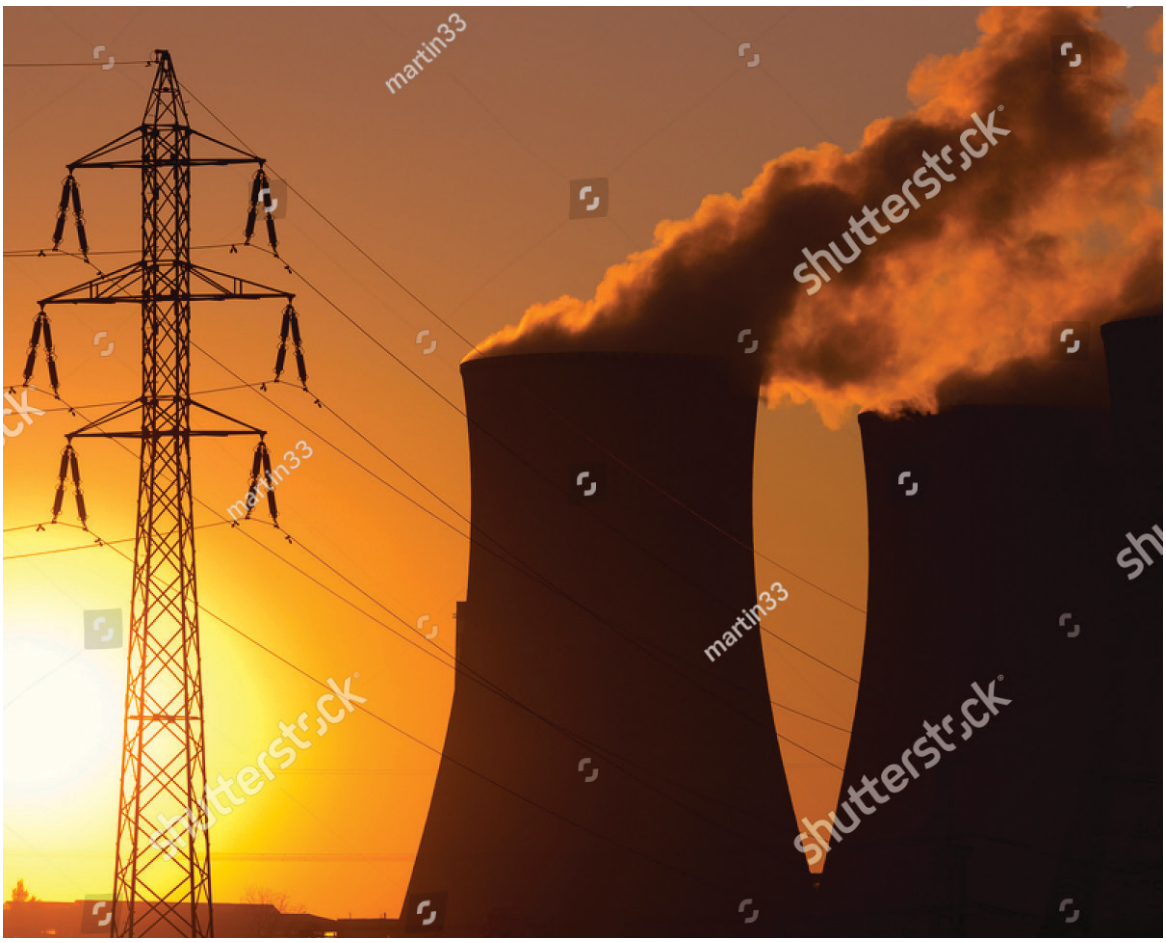


Conclusion

Implementing secure, rapid and efficient crisis communications is more critical than ever in the energy and utilities industry. With a constantly evolving and complex landscape, security and confidentiality are now paramount to transforming how your business communicates to meet these requirements head on. The ability to automate mass notifications internally and externally while increasing response times and decreasing human errors is just the beginning. Controlling sensitive communications during a crisis must also be a critical part of your emergency and crisis communication plan. In today's hyper-social and media-driven world, ensuring secure collaboration among executive management, strategic and tactical teams have become vital to successful response, recovery and eradication.

Communicate with confidence with Vaporstream. Deliver one truth during a crisis-to employees, first responders, regulators and the public-when it matters most.

Communicate with confidence with Vaporstream. Deliver one truth during a crisis - to employees, first responders, regulators and the public - when it matters most.



REFERENCES

i https://www.bloomberg.com/news/articles/2017-11-28/for-a-look-at-pg-e-s-fate-after-fires-watch-this-san-diego-case

ii https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

iii http://blog.talosintelligence.com/2017/07/template-injection.html

iv https://content.next.westlaw.com/Document/Ieb49d7b91cb511e38578f7ccc38dcbee/View/FullText.html

v "Navigating the year ahead, Energy and resources regulatory outlook 2018." Deloitte Center for Regulatory Strategy. https://www2.deloitte.com/us/en/pages/regulatory/articles/energy-regulatory-outlook.html

vi "Navigating the year ahead, Energy and resources regulatory outlook 2018." Deloitte Center for Regulatory Strategy. https://www2.deloitte.com/us/en/pages/regulatory/articles/energy-regulatory-outlook.html

vii "The 10 Things You Should Know About Developing Smarter Energy Infrastructure." Edison Electric Institute. http://www.edisonfoundation.net/iei/publications/Documents/IEI_Grid%20Mod%20101%20Top%2010.pdf

viii "Delivering America's Energy Future." Edison Electric Institute. http://www.eei.org/issuesandpolicy/grid-enhancements/Documents/10_Things_You_Should_Know.pdf

ix "Investing in Resiliency," Eric Silagy. Electric Perspectives January/February 2018. https://mydigimag.rrd.com/publication/?i=466942&ver=html5&p=28#{%22page%22:0,%22issue_id%22:466942}

x https://www.mypalmbeachpost.com/news/local/fpl-center-near-boynton-beach-now-fit-for-category-hurricane/Kq10x5JDWe7ZbAysQSqT0L/

xi "Investing in Resiliency," Eric Silagy. Electric Perspectives January/February 2018. https://mydigimag.rrd.com/publication/?i=466942&ver=html5&p=28#{%22page%22:0,%22issue_id%22:466942}

xii http://www.miaminewtimes.com/news/miami-frustrated-with-fpl-after-hurricane-irma-9666311

xiii https://www.mypalmbeachpost.com/news/local/fpl-center-near-boynton-beach-now-fit-for-category-hurricane/Kq10x5JDWe7ZbAysQSqT0L/

Vaporstream

Vaporstream offers the unique technology and expertise required to address the security, privacy and compliance challenges faced in our fast-paced and mobile world. Recognized for its patented, ephemeral and secure messaging platform, Vaporstream empowers organizations to securely leverage the efficiencies of modern-day mobile messaging demanded by today's mobile workforce —without jeopardizing security or compliance. At Vaporstream, we pride ourselves on delivering services that generate efficiency and value for our customers.

If you would like to learn more about how Vaporstream can help optimize your business communications and partner with you for secure, compliant messaging contact us today.

(800) 367-0780 | info@vaporstream.com | www.vaporstream.com

Vaporstream's Secure Messaging Platform Provides:

Real-time, secure collaboration with complete control of your content, storage and use during discovery, containment, response and recovery; advanced controls remove the risk of propagation. Data leaks simply cannot occur.

Encrypted text messaging in transit and at rest, eliminating the chance of data exposure, surveillance and man-in-the-middle attacks.

Secure, compliant and rapid communications between the organization and staff, warning points, emergency management offices, first responders and the public as required.

The ability to conduct secure, cross-border collaboration with international offices or during an international incident without fear of surveillance or data leak. Creates a direct line to U.S. and U.S. government during global incidents.

Automated communications with predefined templates, recipients and more to reduce errors, speeds response to incidents and provides diverse, geographically dispersed teams better situational awareness during an event;

Secure, mass messaging for internal and B2B communications via secure encrypted text messaging as well as mass communications to the public via standard SMS.

The ability to archive a single copy of messages to a client-designated “repository of record,” for legal and compliance purposes; as an example, collect all needed conversations to meet FERC requirements in one place at your site.

A secure, alternative communication channel, in the case that your network has been compromised, in order to keep bad actors – who may have control of the network and network communications – “out of the know” as response plans are executed;

Recurring notifications and the ability to take over the device to ensure that notifications are never missed.

Broadcast and group secure text messaging

Easy visualization and reporting on who has received / read messages, as well as time to respond.

Ephemeral messaging that alleviates clutter and risk; messages vaporize on demand or automatically after a predetermined interval of inactivity, based on your corporate policies.

Easy to deploy and use for easy adoption; supports iOS, Android, Web desktop and Tablets

And more…

Vaporstream's Secure Messaging Platform Provides:

Real-time, secure collaboration with complete control of your content, storage and use during discovery, containment, response and recovery; advanced controls remove the risk of propagation. Data leaks simply cannot occur.
Encrypted text messaging in transit and at rest, eliminating the chance of data exposure, surveillance and man-in-the-middle attacks.
Secure, compliant and rapid communications between the organization and staff, warning points, emergency management offices, first responders and the public as required.
The ability to conduct secure, cross-border collaboration with international offices or during an international incident without fear of surveillance or data leak. Creates a direct line to U.S. and U.S. government during global incidents.
Automated communications with predefined templates, recipients and more to reduce errors, speeds response to incidents and provides diverse, geographically dispersed teams better situational awareness during an event.
Secure, mass messaging for internal and B2B communications via secure encrypted text messaging as well as mass communications to the public via standard SMS.
The ability to archive a single copy of messages to a client-designated “repository of record,” for legal and compliance purposes; as an example, collect all needed conversations to meet FERC requirements in one place at your site.
A secure, alternative communication channel, in the case that your network has been compromised, in order to keep bad actors – who may have control of the network and network communications – “out of the know” as response plans are executed.
Recurring notifications and the ability to take over the device to ensure that notifications are never missed
Broadcast and group secure text messaging.
Easy visualization and reporting on who has received / read messages, as well as time to respond.
Ephemeral messaging that alleviates clutter and risk; messages vaporize on demand or automatically after a predetermined interval of inactivity, based on your corporate policies.
Easy to deploy and use for easy adoption; supports iOS, Android, Web desktop and Tablets

And more…