BANKING & FINANCIAL
SAFETY & SECURITY

CASE STUDY

Global Business and Financial Information Company

Disperse workforce drives need to communicate while maintaining security and privacy

Executives and staff safety

In a large city, a small team of corporate security professionals keeps an army of global executives safe, ensuring business continuity for a key player in world markets. They spend their days ensuring that the Security Operations Centers (SOCs) in dozens of offices around the globe detect, analyze and respond to incidents swiftly and successfully. Because of them, their corporate executives can conduct business with the confidence that vulnerabilities will be mitigated.

But this is no easy task. Terrorism threatens. Natural disasters arise. Our dependency on electricity and internet creates problems when we lose power or connectivity. The company struggles to balance executive autonomy with security checks and balances. Communication falters when their internal network goes down. As a result, business continuity is jeopardized and the supply chain grinds to a crawl. They needed secure, reliable, seamless communication to manage incidents across a globally dispersed workforce.

So, the Director of Security turned to Mutualink, the interoperability solution that supports secure multimedia collaboration within the enterprise. Daily, and during natural disasters or other emergencies, they count on Mutualink for seamless security communications. The solution lets them share radio and video resources in an ***always on*** environment, using a self-contained local network. Plans are in the works to bring Mutualink's communication solution beyond the Global Security group to Business Continuity and Supply Chain groups for true company-wide interoperability.

The strength of relationships between SOC personnel from remote campuses improved due to the ability to connect in ad hoc online incidents. Radio communications bridged to cell phones increases the quantity, clarity and ease of voice communications.

always on

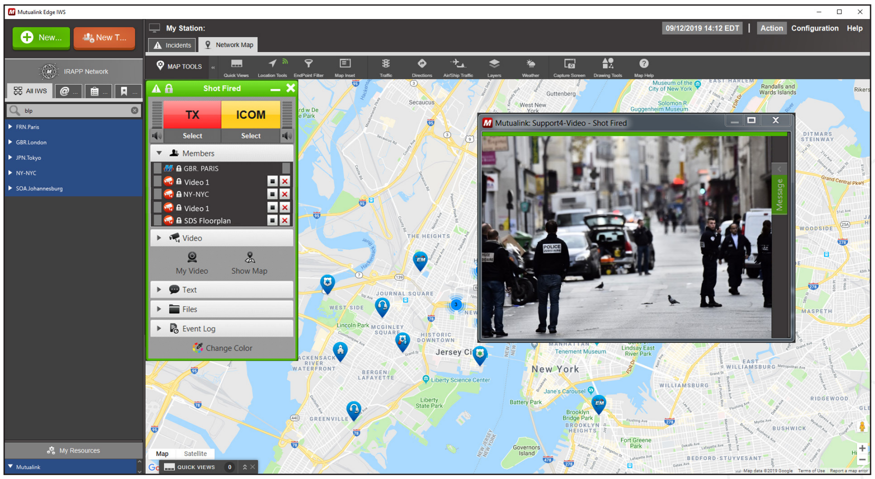
CASE STUDY: Global Business and Financial Information Company

> ***"Once you have a workforce dispersed in offices, mobile locations and events around the globe, security gets complex and the need to maintain communications becomes vital."***
>
> - said the Director of Global Security

In early 2016, the inability to manage incidents when the network was offline was a problem. The security team began to look at ways to communicate seamlessly and share resources regardless of connectivity using a local network solution.

The Director of Security believed that connecting global offices on this network would be crucial for ensuring executive wellbeing and maintaining business continuity, especially in an environment of increased terrorist activities around the world, but notably in Europe. *"We needed a way to stay connected to our offices and executives no matter where they were, so we found a solution with workstations, software, Mobile GoKits and smartphone apps,"* he said.

The Security team used Mutualink to communicate internally with their offices around the world – connecting radios, video, data and text messaging among five global regions.



VOICE

Connects incompatible radio systems, PTT apps, mobile phone and landline phones.

VIDEO

Shares video streams in real time.

DATA

Shares floor plans and other critical situational information.

Mutualink

Today, this global giant achieved their internal communication goals and recognizes the benefit of encouraging their corporate neighbors to also join the network. The Director of Security looks to the use case of the Atlantic City casinos, all of whom are able to connect to one another using Mutualink – a true help should they encounter a bomb threat or similar emergency. Having a way to connect on a one-to-one or one-to-many basis, each participant maintaining control over their own resources, enables neighboring corporations to achieve a new level of security through collaboration.

> ***The ability to build relationships with security teams in SOCs across the city - especially neighboring enterprises – means that the trust is there for when we really need it.***
>
> - Global Enterprise Director of Security

DHS SAFETY Act Certified Qualified Anti-Terrorism Technology

Commercial office buildings increasingly turn to the legal liability protections available under the Department of Homeland Security (DHS) SAFETY Act. The DHS Best Practices for Anti-Terrorism Security (BPATS) list provides policies and procedures to facilitate site security communication with internal and external resources.

U.S. DEPARTMENT OF HOMELAND SECURITY
CERTIFIED
SAFETY ACT
www.safetyact.gov
SCIENCE AND TECHNOLOGY
®

In June of 2018, this corporate headquarters security program earned designation as a SAFETY Act technology. By undertaking training and testing with other corporate neighbors, global financial services colleagues and Mutualink public safety and private security network participants, the company complies with the Testing and Evaluation conditions it will need to satisfy to earn SAFETY Act certification.

Security concerns are heightened by the complexities of mass gathering venues and events, as noted by SAFETY Act BPATS Tier III research. And this company hosts and attends dozens of high-risk events each year. This customer uses Mutualink's Mobile GoKits for always on connectivity to headquarters and regional office SOCs. *"This solution lets us connect by ethernet, commercial mobile broadband or satellite,"* explained the Director of Security. So, whether the event is pre-planned (like a political convention) or ad hoc, communication disruptions are mitigated by the ability to go in-field with full multimedia interoperability.

In the future, the ever-changing technology landscape will require even more merging and bridging of systems to ensure that the corporation, its executive and its workforce is protected. *"Business continuity will always be one of the most important concerns for our global security team, and communications and connections are at the center of success,"* concludes the Director of Security.

ABOUT THE RESEARCH

This case study is based on a June 7, 2019 interview with a Director of Security and his team in a leading global provider of business and financial information.

DHS BEST PRACTICES FOR ANTI-TERRORISM SECURITY

5.1.03
Set in place a capability for security personnel (guards) to immediately communicate with one another through communication devices (e.g., portable radio, pager, cell phone, personal data assistants [PDAs]).

5.1.04
Consider adding communication security (e.g., encryption, multiple frequencies) that prevents unauthorized interception of information being transferred.

5.1.05
Identify the frequencies and channels used by local and state police forces for communications. Coordinate use of appropriate frequencies to ensure communication and deter interference.

5.1.06
There are redundancies in the communications system that prevent single points of failure (e.g., have backup emergency communication equipment like cell phones or emergency radios available for use in the event that all primary channels are unavailable).

5.1.07
Alert site occupants immediately to changes in threat level and related changes to security and safety measures. Inform all personnel regularly on the general security situation.

5.1.08
Issue heightened security awareness alerts, including heightened control measures to vendors and contractors.

5.1.09
Use more than one medium (e.g., text message, e-mail, phone, etc.) to disseminate general security information to tenants.

For more information on any of our products or services please contact us:

mutualink.net

(866) 957-5465

info@mutualink.net