

I. Market Overview/Key Challenges

In early 2007, TJX, the parent company of TJ Maxx and Marshalls retail chains lost some 46 million customer credit and debit card data from its wireless networks. Identity thieves equipped with a laptop and a simple antenna hacked into TJX networks, from innocuous cars parked outside of its retail and corporate locations. IT experts have identified the nation's wireless vulnerability. In 2003, the media reported the possibility of terrorists or criminals to hack into airline networks at the nation's airports. Persistent terrorists could hack into airlines' central computers, create tickets or worse – manipulate passenger or cargo manifest to allow hijackers or dangerous cargo onboard.

In today's digital economy, espionage against the U.S. aerospace and defense corporations continues to increase alarmingly. In addition to major breaches in defense and government networks to steal sensitive information and secrets, spies and hackers are exploiting wireless vulnerabilities in Corporate America for nefarious purposes.

The federal government has long understood the RF threat to national security, which has resulted in stringent regulatory standards to prevent RF emanations of classified or sensitive data. Standards such as Sensitive Compartmentalized Information Facility (SCIF) and TEMPEST were developed to protect data from unauthorized capture and exploitation long before the debut of cellular phones and WiFi. However, Corporate America has yet to embrace comparable security to protect its assets. Today's corporations have yet to fully embrace a multilayered approach to wireless security in lieu of software-based encryption.

What Is A SCIF?

Developed by the federal government, Sensitive Compartmented Information Facility or SCIF (pronounced 'skiff'), is a secured work environment where classified information is handled. SCIFs vary in size from office buildings to deployable ISO container-configurations for forward deployment to hostile locales. Exact construction standards are defined under Director of Central Intelligence Directives.

II. Award Categories & Relevance

The U.S. wireless security and SCIF market is a multi-billion dollar industry. Although federal agencies are the primary consumers of SCIFs, corporations have increased its demand for SCIFs and other secure wireless facilities to counter the ever growing threat. The strategic and economic damage of stolen secrets or data is enormous. Therefore, solutions that enhance wireless security are critical to America's strategic and economic well-being.

III. 2007 North American Wireless Security Technology Growth Excellence of the Year Award

Award Description

The Frost & Sullivan Growth Excellence Award is bestowed each year upon the company which has demonstrated excellence in implementing and sustaining growth through unique growth strategies. Frost & Sullivan, through this exhaustive selection process, seeks to identify a company that has exhibited excellence in all its functional areas, resulting in sustained financial growth.

Research Methodology

A recipient is chosen to receive the Frost & Sullivan Growth Excellence Award based on specific criteria. Through primary and secondary research methods, all companies' market revenues are tracked and those exhibiting significant growth are noted for their strategy implementation. Revenues are then compared year to year to monitor growth patterns. When a company continues to show high growth rates in unit shipments, revenues and profitability, it is a candidate for the Frost & Sullivan Growth Excellence Award.

Measurement Criteria

This Award is given to the company that has bolstered their position in the market during the base year and whose strategy will have a lasting impact on the market. The Award criteria is based on the following:

- Ability to grow in a saturated or maturing market
- Annual market share growth
- Implementing a unique sales strategy to increase market share and revenue growth
- Effective management of existing product portfolio
- Product innovation—satisfying unmet needs, creating new needs, and developing new technologies
- Technological innovation and leadership
- Discovering new venues for an established product
- Strong sales force strategy—number of sales people (direct and indirect), sales force specialization, efficiency in distribution, ability to train and educate, and strong customer service
- Ability to establish brand awareness through promotional activities and advertising
- Strategic mergers, acquisitions, or joint ventures to penetrate new markets
- Reorganization structured around growth strategy

**2007 North American Wireless Security Technology
Growth Excellence of the Year Award
Award Recipient: EM-SEC Technologies LLC**

The Frost & Sullivan Aerospace & Defense Group is proud to present EM-SEC Technologies LLC of Southern Pines, NC, with the 2007 United States Wireless Security Technology Growth Excellence Award. Frost & Sullivan applauds its novel contribution to defending U.S. economic and strategic interests from hostile threats because of its groundbreaking RF emanation solution, the EM-SEC 2060 coating. Corporate wireless networks have come to rely upon encryption to defeat hacking. With persistence, the most formidable wireless encryption could be cracked. Cell phone conversations could be tapped. Only RF emanation or shielding can truly prevent eavesdroppers from accessing wireless signals in the first place.

The 2060 coating has been certified to the highest regulatory and environmental standards because of its low environmental impact. EM-SEC Technologies is fast becoming a global leader in RF containment for federal and corporate users such as defense firms, banks, financial institutions, and hospitals.

IV. Summary of Best Practices

EM-SEC 2060: a cost-effective, wireless security solution

The EM-SEC's 2060 coating offers SCIFs and corporate SCIF-like facilities a cost-effective TEMPEST solution to secure wireless transmissions from hacking. At \$6 per square foot, the 2060 coating can be applied by spray, brush, or roll, on new and old surfaces including drywall, sheetrock, plaster, concrete, block, brick, wood, particle board, plastics, etc. in different locations e.g. corporate offices, boardrooms, server rooms, laboratories, and especially in areas difficult to shield. Furthermore, the 2060 formula is applicable on vehicles and other platforms to expand wireless security in other applications.

The applicability of the 2060 coating on any material enables architects to build or retrofit affordable wireless secure spaces that are beyond the usual bunker. Compared to the cost of inaction, the 2060 solution is both affordable and prudent for corporations big and small.

Walls Do Have Ears, You Know

Wireless and cellular security has been heavily software-reliant. Multilayered approaches to security have not been considered by most corporations because of its unfamiliarity with established standards such as SCIF. EM-SEC Technologies aims to educate U.S. corporations about adopting SCIF and RF emanation standards to protect its wireless networks. The best wireless encryption key cannot defeat a determined foe parked outside of an unshielded building unless a SCIF-like approach is taken to block RF access.

In the financial and banking sectors, breaches in wireless security incur billions in losses annually. The negative publicity stemming from data losses such as credit information can impact adversely the otherwise stellar reputation of implicated entity. EM-SEC Technologies is indeed expanding its 2060 solution to the IT, financial, medical, and pharmaceutical industries, in addition to the federal government and the military. Furthermore, it has received numerous inquiries from American corporations located overseas, where host nation industrial and military espionage is highly active.

EM-SEC also anticipates and responds to a client's security requirements with its value-added approach to wireless security. EM-SEC professionals offer important services such as site evaluation, risk and threat assessment, and turn-key solutions to maximize electronic security and minimize disruptions.

Conclusion

EM-SEC Technologies LLC provides an important tool for government and industry to build a multilayered approach to protect wireless networks from both espionage and crime. It leverages its expertise and experience to provide a simple, cost-effective solution for American corporations. Frost & Sullivan is honored to present EM-SEC Technologies LLC with the 2007 U.S. wireless security technology award, for its EM-SEC 2060 RF emanation coating to defend wireless networks and electromagnetic emissions against identity theft, bank fraud, and more importantly, to protect national defense and homeland security.

About Best Practices

Frost & Sullivan Best Practices Awards recognize companies in a variety of regional and global markets for demonstrating outstanding achievement and superior performance in areas such as leadership, technological innovation, customer service, and strategic product development. Industry analysts compare market participants and measure performance through in-depth interviews, analysis, and extensive secondary research in order to identify best practices in the industry.

About Frost & Sullivan

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services, and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies, and the investment community by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics, and demographics. For more information, visit www.frost.com.