Cisco Systems - The Self-Defending Network

Source: Effies (North America), Effie Awards, 2005

Not so very long ago, viruses were mere nuisances, barely registering on the concerns of senior executives. Today, IT security is a top business priority with billions of dollars at stake. With low awareness and a perceived limited product breadth, Cisco broke through the highly specialized security market by tackling security as human factor rather than a technology issue. With 'The Self-Defending Network' campaign, Cisco not only became the #1 security vendor in all product categories, it strengthened its technology leadership by addressing a pressing and sensitive issue business executives took notice of.

Brand Name: CISCO Systems
Product Type or Description: Network Security Technology
Category for this Entry: Computer Software
Campaign Title: “The Self-Defending Network”
Agency: Ogilvy & Mather
Client: CISCO Systems, Inc.

MARKETING CHALLENGE

A Hack of A Good Business

It has been two decades since the movie War Games in which a teenage boy used a backdoor-unauthenticated dialup modem to hack into a military central computer. Since then, threats have become more complex, more malevolent and faster spreading, turning information security into the stuff of headlines. In 2003, security breaches affected 90% of US businesses and cost $17 billion annually: as a leader in information technology, Cisco wanted to gain a more sizeable piece of the burgeoning market. Unfortunately, Cisco faced many challenges:

- A highly competitive and fragmented market: given the complex nature of threats, the security market was swamped with “best of breed” point solution providers claiming greater expertise than the larger integrated technology vendors like Cisco
- Lack of security credentials: In the US, Cisco was known as the network leader, but not as a security expert. It was widely believed that Cisco only offered limited security features that were a good start, but not comprehensive
- Security was misunderstood: security czars at large firms spent millions to secure their firms but were at a loss when asked specific justification for the types of products they chose. In fact, Forrester reported that 40% of IT security executives were spending dollars on the wrong risks
- Cisco knew the wrong people: Cisco had built its networking empire through relationships with data networking experts. Now it needed to engage with security specialists who were biased toward security point products (e.g. firewall, VPNs) and wanted to restrict network access to avoid breaches – Cisco was not on their wish list. In addition, given the liability and cost of security incidents, Cisco also needed to start talking to business-decision makers (e.g. CEOs) who were playing an increasingly influential role in the IT security decision-making process.

What's The Network Got To Do With It?

The marketing challenge required in-depth defense. We had to use what Cisco was known for – the network – to reframe the market. Basically, convince executives that given the new nature of security threats, they needed a whole new type of security strategy – a holistic solution that only the company that built the network could deliver.

CAMPAIGN OBJECTIVES

Campaign Objectives Were Twofold:

1. Extend Cisco's brand equity into security: We needed to establish credibility for Cisco in the IT security space. This required creating awareness of Cisco as a security provider with a serious breadth of products, but also educating key decision-makers on a new approach to security with the network as foundation.
2. Gain market share: Given the swift market expansion, Cisco needed to gain a strong footing into the IT security space before other competitors could establish long term preference.

TARGET AUDIENCE

We needed to engage two types of audiences:

- Technology decision-makers: Both C-level (e.g. CIO, CTO) and Security Specialists involved at every step of the purchasing process from determining the need for security to recommending products and brands.
- Business decision-makers: C-level executives (e.g. CEO, CFO) not engaged with IT at a level that they would understand the difference between a firewall and a VPN, but increasingly involved in the technology decision-making process, especially concerning security because of its impact of the business and bottom line.

Target Insight: Security Is Getting Personal

The rapidly increasing pressure to comply with new government regulations (e.g. Sarbanes-Oxley, the Anti-Money Laundering Act) was putting senior executives in the hot seat. CEOs were forced to assume full responsibility for the information included in their financial reports, while CIOs had to address the potential legal and financial damage resulting from IT threats and misuse. With high-visibility prosecutions and executive jail sentences on the rise, companies were taking compliance issues very seriously – and making security a matter of personal responsibility.

CREATIVE STRATEGY

The Human Face of Security

Given the shifting cultural mindset toward security, we wanted to show that Cisco's approach to security was less about protecting technology systems per se, but about protecting people.

Creative Idea: "The Self-Defending Network"

We bundled all of Cisco's security solutions under one positioning umbrella: "The Self-Defending Network." This allowed us to link security with Cisco's core brand equity (the network) and suggest implicit leadership. Instead of talking about outside viruses, worms or other malevolent IT attacks, the work focused on the untold human stories around security: business travelers, telecommuters, executives and their kids.

Both the TV and print depicted stories of executives who had been – unbeknownst to them thanks to the Self Defending Network – exposed to a security breach. Two commercials ("Inside Job" and "Sarah's Escapade") specifically focused on threats not talked about: inside jobs. Research had revealed that inside internal attacks represented only 22% of security breaches in the US, but that they were ten times more damaging, although often not deliberate (source: FBI 2003 Crime & Security Survey).

All of the communication pieces (TV, print, outdoor, online, direct mail, etc.) were unified against one tagline "Self-Defending Networks Protect Against Human Nature."

MEDIA STRATEGY

Media echoed the creative strategy by engaging audiences in lifestyle, entertainment and business environments rather than technology-centric vehicles.

TV: Two creative executions ("Inside Job" and "Sarah's Escapade") were rotated from Jan-May 04 targeting Business decision-makers (men 24-54). Advertising ran in non-tech Sunday morning programming (Meet the Press, This Week, Face the Nation, CBS Market Watch), and on cable stations in lifestyle-oriented shows like National Geographic, Discovery Channel, ESPN and History Channel. Prime time was also purchased to reach a broader audience in entertainment style programs with shows like West Wing, CSI, Law and Order, CSI, 60 Minutes.

Print: Two print executions ("Woman on Pillow", "Little Girl") were launched in national newspapers (e.g. WSJ, Washington Post, NYT) and business magazines (e.g. Fortune, Forbes, the Economist) to reach thought leaders.

Out of Home: In Silicone Valley and San Francisco, we created buzz with a barbwire execution on major highways.

Online: On The Wall Street Journal website, we negotiated a front-page log-in screen to feature the Cisco Self-Defending Network – a media first in the history of the WSJ website. Advertising banners ran on The Economist

and Business Week web sites.

MEDIA

- Television
- Radio
- Newspaper
- Trade/Professional
- Consumer Magazine
- Direct Mail
- Out-of-Home
- Public Relations
- Sales Promotion
- Interactive/Online

Total Media Expenditures:

- $20 Million and over

OTHER COMMUNICATIONS PROGRAMS

- Trade Shows and Events: The “Self-Defending Network” campaign was used throughout all of Cisco's security trade shows and events from January to July 04. The TV commercials ran in the booths, brochures and speeches were all tailored against the tagline and new positioning.
- Direct Mail: An email program was sent to over 46,000 technical decision-makers. Web-based creative used the same concept as the print executions and a complimentary 'Self-Defending Network' book was used as incentive.
- Cisco Customer Magazine: “Packet Magazine” circulated to 116,000 businesses, dedicated its Vol. 16, No.1, First Quarter 2004 issue to the “Self-Defending Network” and used a picture of the TV character (little girl Sarah) on its cover page.
- **Cisco.com**: a dedicated “Self-Defending Network” micro-site was developed as an adjunct to the **Cisco.com** site with Whitepapers, and security business case studies.

EVIDENCE OF RESULTS

1. The Campaign Expanded Cisco'S Technology Leadership Into Security

All three security TV commercials outperformed prior Cisco advertising

- Beating the Cisco Average on Attention, Motivation and Brand Linkage.

- All the commercials were rated as being extremely likeable, entertaining, believable and relevant, outperforming both the Cisco Average (+19%) and Ameritest Tech Average (+31%). (Source: Ameritest, March 2004).

The Ads Generated a Positive Halo Effect on the Brand

While the ads were focused on security, they all exceeded the Cisco Average on a number of brand leadership measures including: “Is technologically innovative,” “Is a technology leader”, “Offers products that help your organization stay competitive.” (Source: Ameritest, March 2004).

Advertising Helped Firmly Position Cisco into the Security Space

Brand Tracking (source: Millward Brown, July 2004) showed Cisco's IT Security Brand Consideration among the business audience went from almost nothing (2%) to 21% (a 950% increase!) while it increased 54% among the tech audience from the pre-wave Oct-Dec 03 to the post-wave of April-July 2004.

2. The Campaign Established Cisco As The #1 Security Market Provider

Cisco gained 7 points in market share or $175M worth of business Cisco became the dominant player in the security market with 40% market share in Q1 04, up from 33% in 2003 (source: Infonetics) (see **Figure 1**)

Cisco increased market share for all of its security products

VPN and firewall appliances market share went up from 32% to 37% from 2003 to Q1 2004; hardware secure routers went up from 83% to 86% and Intrusion Detection went up from 19% to 28% (source: Infonetics) (see **Figures 2** and **3**)

Integrated elements of the campaign generated scores of leads

- Direct mail generated a 269% lift in security leads from Aug 03-Jan 04. to Feb-July 04, and garnered a response rate of (4.2%) – 4 times the industry average (source: Merry Law, Global Analytics)
- Traffic to **Cisco.com** security pages increased 96% with a 64% increase in security as a 'key interest' hit

According to the Yankee Group 2004 Managed Security Services Survey, Cisco was the only IT networking firm to rank as one of the most trusted security providers, alongside other security specialists like Symantec and VeriSign. ***“This survey result is really a testament to the power of Cisco's remarkable brand recognition”*** said Phebe Waterfield, Yankee Group Security Solutions & Services analyst.

NOTES & EXHIBITS

FIGURE 1

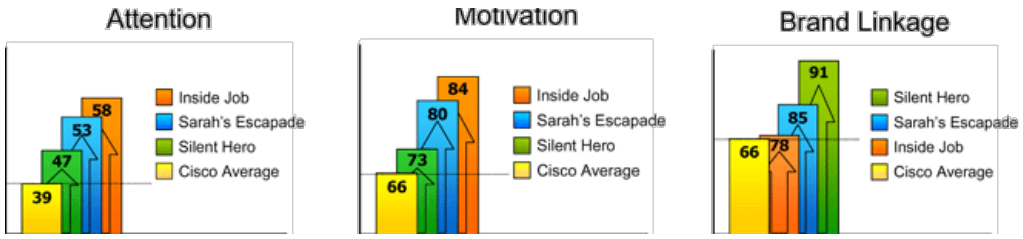


FIGURE 2

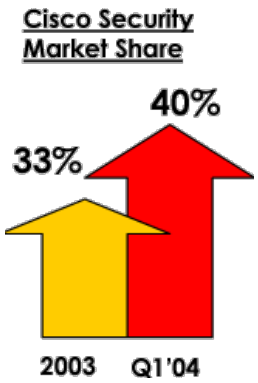
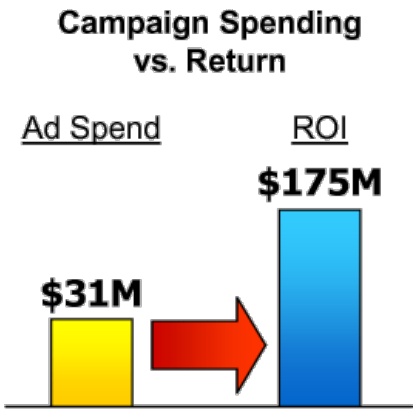


FIGURE 3



Effie Worldwide, Inc.
116 East 27th St., 6th Floor, New York, NY 10016. United States of America
Tel: +1 212-687-3280, Fax: +1 212-557-9242

www.warc.com

WARC