Cyveillance
a QinetiQ Company

World Leader in
Cyber Intelligence™

See the Threat in the Wild
Before It’s through Your Door

STRATEGIKA CONSULTING

Partner of Cyveillance in Middle East & North Africa

Adress: 09, rue Molière, Beauséjour, Annaba, Algeria
Phone : +213 38 80 48 66 mail: contact@strategika-consulting.com
Mobil : +213 770 322 311 website: www.strategika-consulting.com

Corporate Deck Table of Contents

Cyveillance
a QinetiQ Company

- **Cyveillance Overview**
- **Cyber Intelligence**
  - Information Security & Fraud
  - Physical Security
  - Brand Security
- **Professional Services**
- **Supplemental Slides**

CYVEILLANCE OVERVIEW

Corporate Overview

Headquarters in Fairfax, VA

- Founded in 1997
- Subsidiary of QinetiQ North America
- Trusted by Today’s Industry Leaders for Cyber Intelligence

Over 300 blue chip clients

- 40 of Fortune 100
- Over half of the Fortune 50
- Financial services: 8 of top 10
- Insurance: 2 of top 4
- Pharmaceuticals: 3 of top 4
- Energy: 3 of top 4
- Technology: 8 of top 10
- Retail: 4 of top 7
- Travel and hospitality: 4 of top 6

Global Partnerships

SANS

YAHOO!

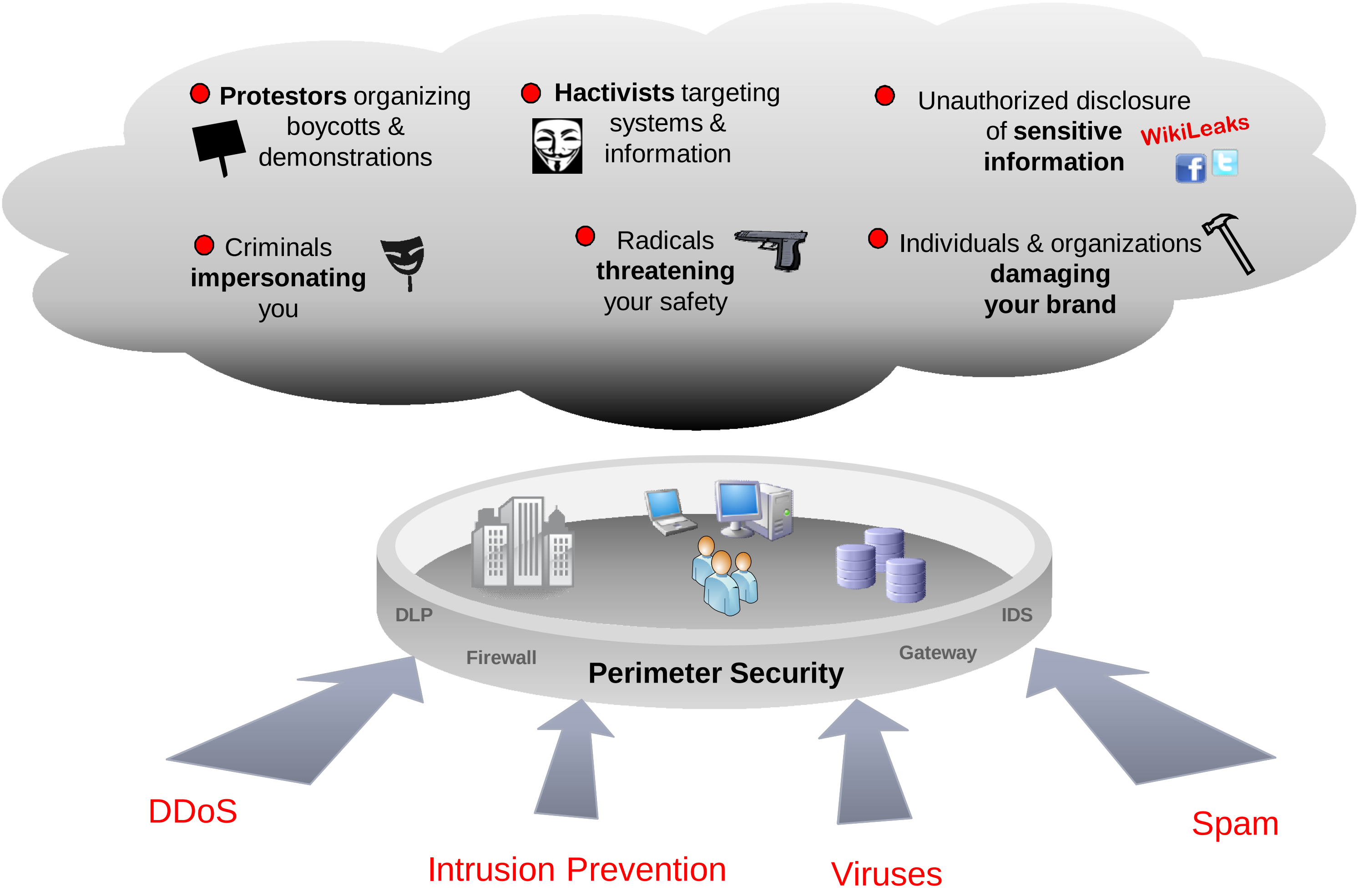
Microsoft

CERT

AOL

Cyber Threats Outside the Perimeter

Cyveillance
a QinetiQ Company

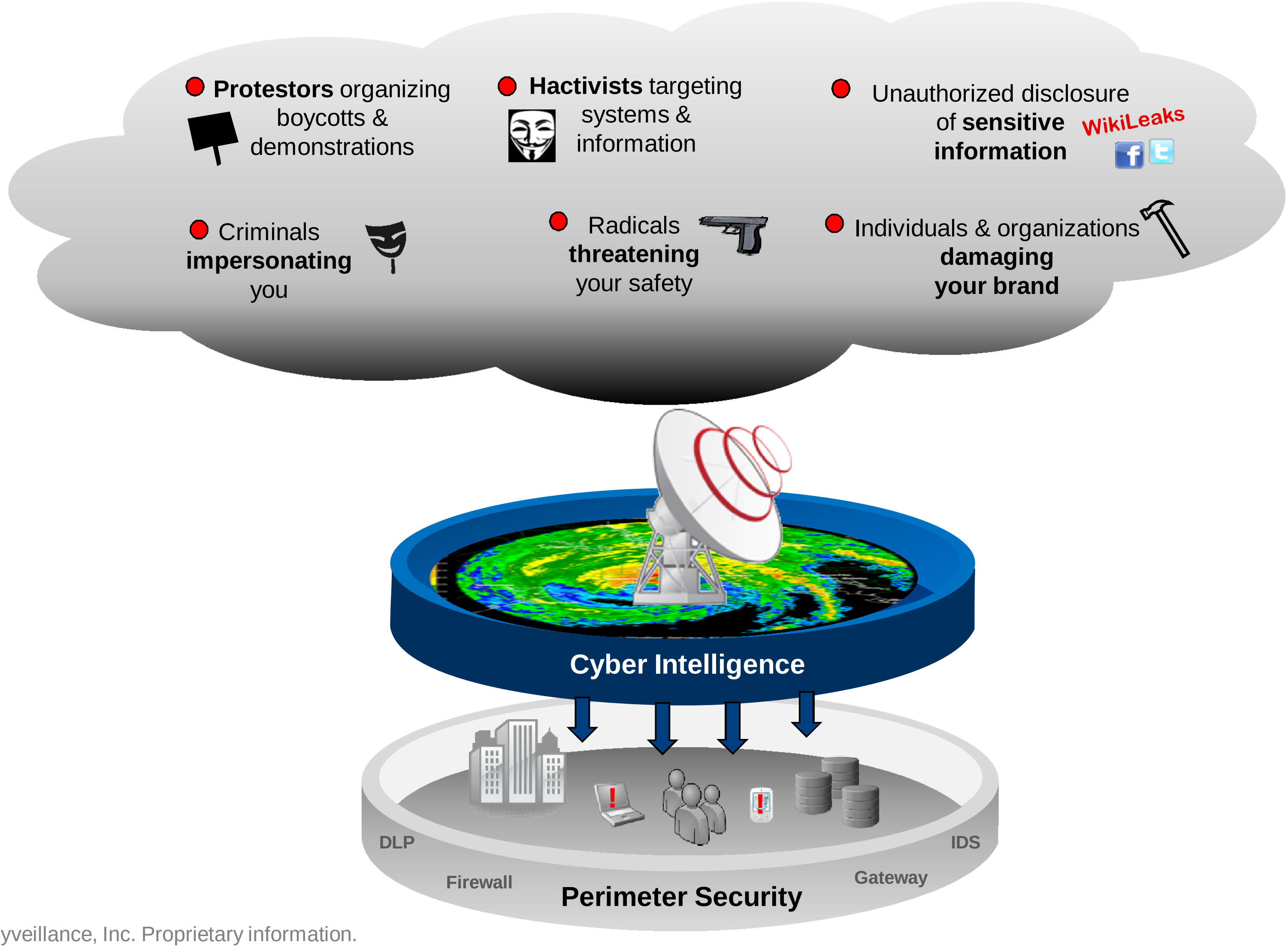


- **Protestors** organizing boycotts & demonstrations
- **Hactivists** targeting systems & information
- Unauthorized disclosure of **sensitive information**
- Criminals **impersonating** you
- Radicals **threatening** your safety
- Individuals & organizations **damaging your brand**

www.cyveillance.com

Cyveillance Cyber Intelligence

Cyveillance
a QinetiQ Company



- **Protestors** organizing boycotts & demonstrations
- **Hactivists** targeting systems & information
- Unauthorized disclosure of **sensitive information**
- Criminals **impersonating** you
- Radicals **threatening** your safety
- Individuals & organizations **damaging your brand**

Cyber Intelligence for the Enterprise

Cyveillance
a QinetiQ Company

Information Security & Fraud

- Phishing, malware and other forms of fraud
- Leaks of confidential information

Physical Security

- Threats to employees
- Planned activities to disrupt business operations
- Threats against facilities & resources

Brand Security

- Unauthorized and misuse of brand
- Negative commentary and issues that can impact a brand’s reputation

Professional Services & Training

Provided by leading cyber security experts

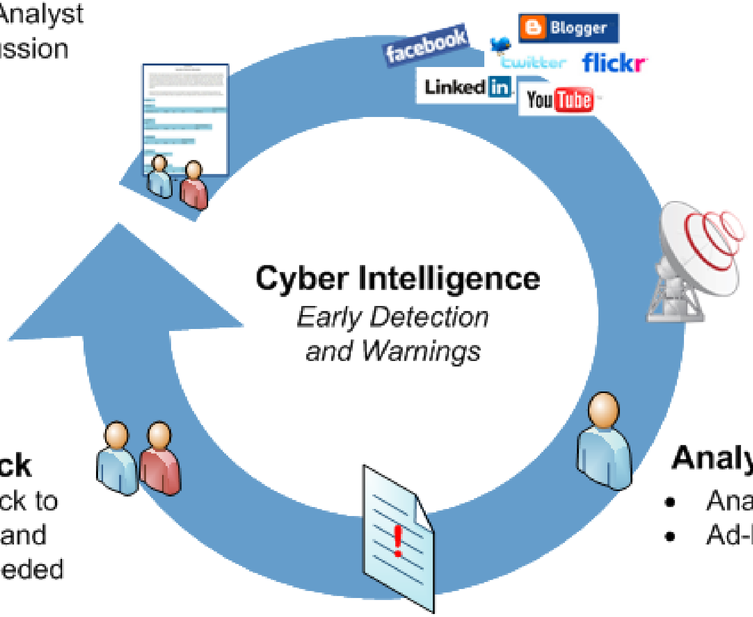
Investigations

Response Services

Training

Cyveillance Process for Delivering Relevant Intelligence

Cyveillance
a QinetiQ Company



Requirements Implementation
- Determine search & collection coverage based on customer needs

Requirements gathering
- Dedicated Analyst
- Goals discussion

Cyber Intelligence
Early Detection and Warnings

Collection
- Ongoing open source collection specific to customer criteria

Analysis
- Analyst review
- Ad-hoc research

Intelligence Delivery
- Alerts & Reports via email
- Permissions-based portal

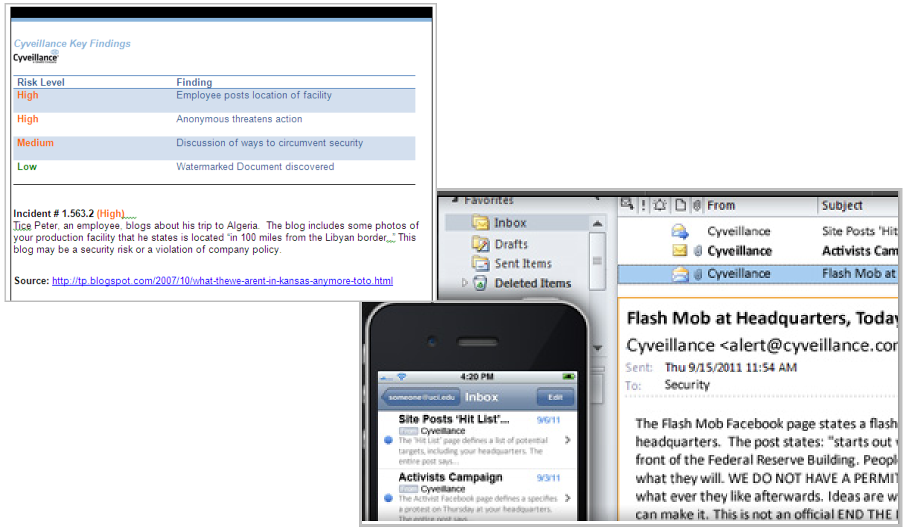
Customer Feedback
- Continuous feedback to review intelligence and refine criteria as needed

Cyber Intelligence Delivery

Cyveillance
a QinetiQ Company

Alerts and Reports via Email

- Prioritized list of findings to help you know where to focus efforts
- Summaries of each incident detected to help you quickly understand its relevance



Cyveillance Key Findings

Cyveillance

Risk Level	Finding
High	Employee posts location of facility
High	Anonymous threatens action
Medium	Discussion of ways to circumvent security
Low	Watermarked Document discovered

Incident # 1.563.2 (High)

Tice Peter, an employee, blogs about his trip to Algeria. The blog includes some photos of your production facility that he states is located "in 100 miles from the Libyan border." This blog may be a security risk or a violation of company policy.

Source: http://tp.blogspot.com/2007/10/what-thewe-arent-in-kansas-anymore-toto.html

From	Subject
Cyveillance	Site Posts 'Hit
Cyveillance	Activists Cam
Cyveillance	Flash Mob at

Flash Mob at Headquarters, Toda

Cyveillance <alert@cyveillance.co

Sent: Thu 9/15/2011 11:54 AM

To: Security

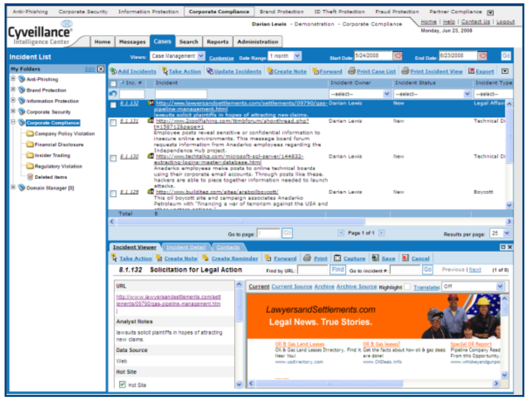
The Flash Mob Facebook page states a flash headquarters. The post states: "starts out front of the Federal Reserve Building. Peopl what they will. WE DO NOT HAVE A PERMI what ever they like afterwards. Ideas are w can make it. This is not an official END THE

Site Posts 'Hit List'... 9/6/11
From Cyveillance
The 'Hit List' page defines a list of potential targets, including your headquarters. The entire post says...

Activists Campaign 9/3/11
From Cyveillance
The Activist Facebook page defines a specifies a protest on Thursday at your headquarters. The entire post says...

Portal

- Workflow and case management
- Archive captured and stored for all incidents
- Integrated language translation tools



Darian Lewis - Demonstration - Corporate Compliance

Monday, Jun 23, 2008

Incident List

Views: Case Management
Customize
Date Range: 1 month
Start Date: 5/24/2008
End Date: 6/23/2008
Go

Inc. #	Incident	Incident Owner	Incident Status	Incident Type
		--select--	--select--	--select--
8.1.132	http://www.lawyersandsettlements.com/settlements/09790/gas-pipeline-management.html lawsuits solicit plaintiffs in hopes of attracting new claims.	Darian Lewis	New	Legal Affair
8.1.131	http://www.2coolfishing.com/ttmbforum/showthread.php?t=158712&page=1 Employee posts reveal sensitive or confidential information to insecure online environments. This message board forum requests information from Anadarko employees regarding the Independence Hub project.	Darian Lewis	New	Technical Di
8.1.130	http://www.techtalkz.com/microsoft-sql-server/144832-extracting-logins-master-database.html Anadarko employees make posts to online technical boards using their corporate email accounts. Through posts like these, hackers are able to piece together information needed to launch attacks.	Darian Lewis	New	Technical Di
8.1.129	http://www.builditez.com/sites/araboilboycott/ This oil boycott site and campaign associates Anadarko Petroleum with "financing a war of terrorism against the USA and	Darian Lewis	New	Boycott
Total	8			

Go to page: 1 Go
Page 1 of 1
Results per page: 25

8.1.132 Solicitation for Legal Action

Find by URL: Find
Go to incident #: Go
Previous | Next (1 of 8)

URL
http://www.lawyersandsettlements.com/settlements/09790/gas-pipeline-management.html

Analyst Notes
lawsuits solicit plaintiffs in hopes of attracting new claims.

Data Source
Web

Hot Site
☑ Hot Site

Translate: Off

LawyersandSettlements.com
Legal News. True Stories.

Oil & Gas Land Leases
Oil & Gas Land Leases Directory. Find it Near You!
www.usdirectory.com

Oil & Gas leases?
Get the facts about how oil & gas deals are done!
www.OilDeals.info

Special Oil Report
Pipeline Company Read From this Opportunity.
www.whiskeyandgunpo

Why Cyveillance?

Cyveillance
a QinetiQ Company

Industry Leading Cyber Intelligence

- **Rapid and Relevant** – Delivers rich, insightful intelligence reports - not just data, links or search results.

- **Expert** –Your reports are prepared by vertically-focused analysts with backgrounds in intelligence, law enforcement, security and deep experience in your industry. They understand your business and the specific threats arrayed against you.

- **Global** - Addresses threats across the globe with foreign language analyst support.

- **Trusted** - Leading Fortune 500 security and service professionals from several industry rely on Cyveillance intelligence

CYBER INTELLIGENCE:

INFORMATION SECURITY & FRAUD

Information Security & Fraud Cyber Intelligence

Cyveillance
a QinetiQ Company

Monitors for:

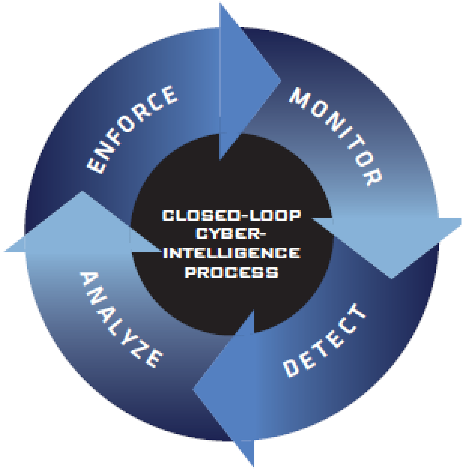
- **Fraud**
  - Phishing, Vishing, SMiShing and malware attacks
  - Valuable information about new fraud schemes and trends
- **Leaks of sensitive information leading to regulatory or compliance liabilities**
  - Exposed documents which contain confidential, proprietary or sensitive information
- **Hackers attempting to compromise corporate systems**
  - Chatter regarding threats against network assets – including denial of service attacks

Cyveillance Anti-Phishing Overview

Cyveillance
a QinetiQ Company

Cyveillance Anti-Phishing prevents, detects, disables, and helps you recover from phishing and malware attacks. The solution uniquely addresses the entire lifecycle, including:

- **Attack prevention** — Cyveillance Anti-Phishing deters phishers by making your organization a tough target
- **Attack detection** — Cyveillance provides the industry's best overall 24x7 monitoring coverage of junk (spam) email, and the web's domain registration system
- **Phishing and malware site takedown** — After a fraud scheme is detected, Cyveillance initiates site takedown procedures by leveraging the industry's best 24x7 Security Operations Center
- **Recovery** — Cyveillance Anti-Phishing has established post attacks processes in place to help minimize the impact of attacks



Investment Bank Information Leak

Cyveillance
a QinetiQ Company

Situation

A large investment bank/brokerage house experienced significant physical fraud occurring in Asia. The customer wanted to monitor for:

- Any fraudulent activity occurring online
- Sites infringing or posing as the investment bank
- Data leakage of intellectual property

Intelligence Gathered

- Cyveillance identified 37 investment reports that were leaked. Reports were found in Chinese as well as English.

Result

This detection and reporting assisted in identifying a major (human) leak within the company who was reselling and reposting confidential reports on the Internet.

Global Hotel Chain Fraud

Cyveillance
a QinetiQ Company

Situation

- Significant employee recruiting performed to support international expansion
- Fraudsters copy and leverage job solicitations to dupe job seekers
- Applicants required to fax personal information and copies of passport pages

Intelligence Gathered

- Technology intercepts fraudulent email-based job solicitations
- Analyst determines email respondents are directed to suspicious fax line

Result

- Client works with law enforcement to determine that victim identities are being used for money laundering and immigration fraud
- Intelligence agency taps fax line to monitor victim identities

CYBER INTELLIGENCE:

PHYSICAL SECURITY

Physical Security Cyber Intelligence

Monitors for:

- Organized demonstrations
- Planned boycotts against products and services
- Threats against employees, corporate officers, facilities and resources
- Planned activities to interrupt business operations and events
- Solicitations to conspire against the organization

Fortune 200 Energy Company

Cyveillance
a QinetiQ Company

Situation(s)

- Anti-nuclear activists target facilities, including power plants
- Former employee leaks IP to the Internet
- Sites spring up with misinformation about CEO

Cyber Intelligence Delivered

- Cyveillance technology intercepts activist chatter on “hidden” Internet
- Cyveillance technology identifies information leak on blog
- Cyveillance monitors discussion related to CEO

Results

- Client bolsters security at targeted power plants
- Client uses legal remedy with former employee to remove IP from personal blog
- Client counteracts misinformation through a combination of new web content and search engine optimization to move “bad” sites lower in search results

F100 Financial Services Company

Situation

- Client has a board member that also sits on board of a large pharmaceutical company associated with Huntington Life Sciences
- Pharmaceutical company is frequent target of animal rights groups like SHAC and ALF
- ALF begins targeting financial services company by vandalizing bank branches

Cyber Intelligence Delivered

- Technology intercepts anonymous online postings that document and brag about successful vandalisms
- Analyzes the dates of the vandal attacks and correlates them to meetings where a known ALF member presents

Result

- Client identifies key suspect in vandal cases
- Client works with local law enforcement to increase presence at events
- Acts end; suspect eventually arrested and convicted

US Embassy Compound Security Concern

Scenario

US entity enlisted Cyveillance to monitor for threats, risks or vulnerabilities regarding US properties, locations, and persons in a certain geographic region.

Cyber Intelligence Delivered

This finding was a blog posting which was addressed to "Mr. bin Ladin." The blog outlined in very fine detail the method in which to enter a specific US Embassy compound. The instructions indicated:

- **How to enter** the grounds without going through security for mirrored car checks – if the person dresses in sportswear and brings a soccer ball
- **The time of day** at which to enter the Embassy grounds with the false intent to play soccer
- **Which door** from the Embassy locker room would provide entry into the Embassy building

UN General Assembly

Scenario:

More than 150 foreign leaders were in New York City in October 2009 for the opening of U.N. General Assembly. The customer wanted to know of any incidents relating to:

- *Reports of protests or other actions directed at protectees*
- *Reports of protests which may affect transportation routes*
- *IT threats posed to facilities associated with UNGA (hotels/foreign missions). This included fax blasts, phone calls to front desks, and online email forms.*
- *OPSEC disclosures (pictures of agents, etc.)*
- *Monitoring flash mob activity (Twitter, forums, blogs, etc.)*

Project:

This project was in English only and reporting was conducted on a daily basis for the duration of the project.

Timeframe:

Total of 50 days of monitoring. Delivery was made in near real time by incident as well as a daily summary.

UN General Assembly Intelligence

Cyveillance
a QinetiQ Company

Cyber Intelligence Delivered:

1. Total High Priority Incidents Delivered =135
2. Direct threats to dignitaries of 8 countries.
3. Disruptive activity targeting Libyan delegation and Safehouse location in New Jersey – including tail number of Gadhafi's private jet
4. Protest plans, dates, locations and approximate number of activists attending. One set of protestors planned to set objects and themselves on fire.
5. 2 threats directly targeting customer's protective detail members
6. 2 "unknown" and suspicious package threats in vicinity in NYC

Customer comments

"Some of these incidents were not found in our classified sources"

"Many of your findings validated information we found through other means"

"The intelligence provided adequate time to plan and act on anticipated activities"

BRAND SECURITY

CYBER INTELLIGENCE

Brand Security Cyber Intelligence

Cyveillance
a QinetiQ Company

Monitors for:

- **Unauthorized and misuse of brand and content use**
  - Social media impersonation and account hijacking
  - Improper or unauthorized claimed relationships
  - Logo and Trademark Violations
  - Copyright Violations
  - Cyber Squatting and Typo-Piracy

- **Negative commentary and issues that can impact a brand's reputation**
  - Social Media and online community monitoring
  - Rapid intel on community and online views
  - Feedback on brands, marketing campaigns, products, services, quality and price

- **Unauthorized distribution**
  - Web distribution by unauthorized retailer sites or eBay Auctions
  - Suspected counterfeit or gray market goods

Enforcement and Site Revisit

- **Enforcement & Site Revisit consists of:**
  - Unlimited sending of template emails through the Cyveillance Intelligence Center
  - Site revisits for up to 600 incidents per year

- **Cyveillance analysts work with client to:**
  - Coordinate with the client’s legal department to determine the aggressiveness of the process and the language of the letters
  - Determine the amount of involvement by Cyveillance in the enforcement process
  - Determine when it becomes necessary for a domain to be escalated to the client

Large Credit Information Service

Situation

- Credit agency required by federal government to maintain a free credit reporting site
- In return, agency allowed to sell “for-fee” credit reports from own site
- FTC publicly warns client that any deceptive marketing practices will be result in termination of their credit report business
- 3rd party sets up sites using deceptive marketing practices to damage client reputation

Intelligence Gathered

- Technology identifies sites out of compliance with FTC requirements
- Analyst researches and determines 3rd party affiliation

Result

- **Bad marketing practices eliminated through legal enforcement**
- **Client’s reputation and line of business preserved**

Intercontinental Hotels

Problem

Revenue loss out of control within online distribution channels (travel agents, franchisees)

- Franchises diverting reservations to competing hotels in their owned groups
- Web site pricing out of compliance
- Online partners with competing offers
- Hotels featured in escort service sites
- Sites with InterContinental logo, but leading to other hotels
- Other diverted search engine traffic

Solution

- **Cyveillance Brand Security proactively monitors channels for issues**

Result

- **Recapture of “millions in annual business being diverted from websites”**

Insurance Company

Problem

- **Company saw significant challenges in managing 12,000 independent Agents**
  - Prior difficulties in offline Yellow Pages advertising by Agents
  - Massive inconsistency of brand
  - Agents made up their own slogans, logos
  - Geographical overlap problems created by lack of adherence to guidelines
  - Policy sales lost due to poor branding issues
- **Anticipated similar impact from growing Internet & Agent web sites**

Solution

- **Cyveillance cyber intelligence identifies relevant agent issues per customer requirements**

Result

- **Strengthened brand**
- **High ROI of over $3 million from improved operational efficiencies**

Frank Russell

Problem

- Licensing model of Frank Russell’s “Russell 2000” was leaking royalty revenue with many unlicensed sites featuring the market data index.

Solution

- Cyveillance provides online risk monitoring and management
- Pinpointed those Internet sites suitable for licensing
- Recaptured revenue for high-yield ROI

Result

- Over $300,000 in revenue identified in first six months

Leading Pharmaceutical Lab

Cyveillance
a QinetiQ Company

Problem

- Nutritional supplements sold to institutions in bulk
- Product was being diverted, broken down and resold on the Internet
- Expired gray market product being sold to consumers
- Client lost control of its distribution channels
- **Liability issues immense**

Solution

- Cyveillance delivers cyber intelligence to identify sites selling unauthorized products
- Ongoing monitoring and follow up actions to address issues

Result

- **Huge risk exposure on multiple brands mitigated**
- **Negative perceptions of product eliminated with shut-down of rogue sites**
- **Price points of product channels protected**

PROFESSIONAL SERVICES

Global Cyber Intelligence Expertise

Cyveillance
a QinetiQ Company

The Cyveillance Global Cyber Intelligence Division is built around a solid core of University and Institute training with significant field experience in intelligence and security operations.

Educational backgrounds

- Defense Language Institute
- National Cryptologic School
- Criminal Justice Studies
- Information Technology and Engineering
- Network Security
- International Commerce and Policy
- Administration of Justice and Applied Intelligence
- Political Science
- Finance
- Economics and Statistics
- Operations Research
- MBA
- International Trade
- International Business
- Government and International Politics

Former positions as employees or contractors of the following:

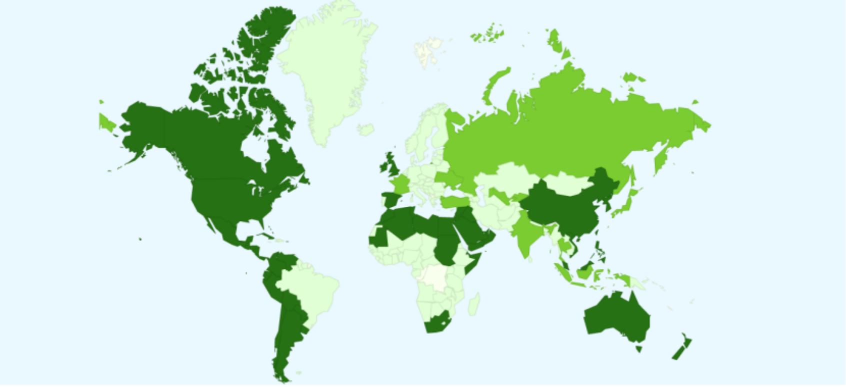
- FBI
- U.S. Air Force
- DOJ
- CIA
- Bureau of ATF
- NCMEC
- U.S. Marshals Service
- U.S. Navy
- Bureau of Customs and Border Protection
- INS
- DSS
- National Security Agency

Foreign Language Capabilities

- Cyveillance technology is language agnostic to detect threats in any language.
- Cyber Intelligence Analysts have the language skills required to monitor and provide analysis for over 88% of the users on the world wide web.

Analyst Foreign Languages Expertise

- English
- Cantonese
- French
- German
- Italian
- Japanese
- Korean
- Malay
- Mandarin
- Russian
- Spanish
- Thai
- Turkish
- Ukrainian
- Uyghur
- Vietnamese

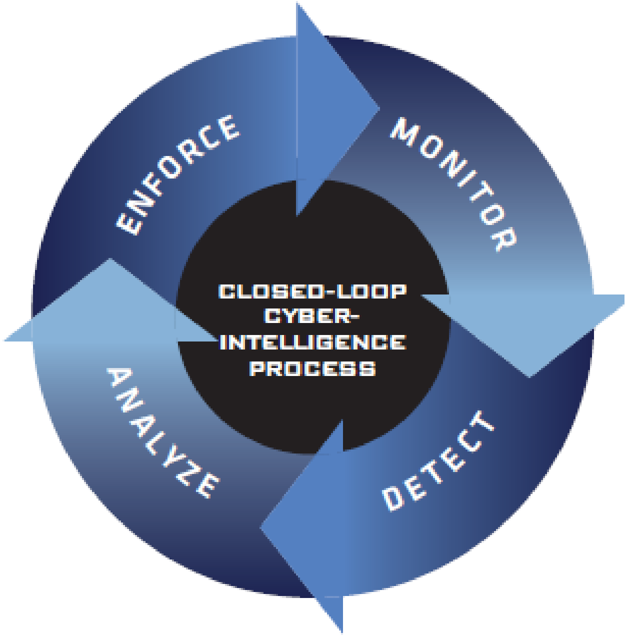


Violation Response Services

Cyveillance
a QinetiQ Company

Once a cyber threat has been detected, Cyveillance can provide the following response:

- **Phishing/Fraud Site Takedown**
- **Fraudulent mail account shutdown**
- **Fraudulent cell account shutdown**
- **Impersonation and content removal**
- **Cease & Desist Letters**
- **DMCA Notification Letters**
- **EU Copyright Directive Notification**
- **Enforcement and Site Revisit**
- **Terms &Conditions Violation/Social Media Action Letters**



Investigations and Professional Services

Cyveillance
a QinetiQ Company

Investigations may include one or more of the following components:

- **Open source internet collection, cataloging and analysis of relevant information and intelligence**
  - Death threats
  - Insider threat/disgruntled employee
  - Due diligence on a potential merger or acquisition
  - Event Monitoring and analysis
  - Adversarial group reports
  - Lawsuits
  - Executive threat profiles
- **Assessments and analyses of the collected relevant information**
  - Timelines and event chronologies
  - Psychological profile(s)
  - Recommendations
- **Response Actions**
  - Site or domain removal requests (i.e., C&D letters)
  - Fraudulent email shutdown requests

:

CYBER SAFETY TRAINING

Cyveillance Cyber Safety 101 Training

Cyveillance
a QinetiQ Company

Cyveillance Cyber Safety 101™ training provides employees with:

- A solid understanding of how the Internet actually works and what its weaknesses and vulnerabilities are
- Knowledge of the basics and limitations of the rules, polices and laws which govern, manage and safeguard users and information online
- Understanding of the level of sophistication of today's online threats
- An introduction to the new discipline of Cyber Intelligence and how the Internet can provide valuable information leading to a predictive defense against threats before they occur

Cyveillance Cyber Safety Awareness

Cyveillance Cyber Safety Awareness Training was developed with a particular focus to address the increasing risk of spear phishing and corporate cyber attacks that could lead to corporate network breaches.

The course consists of three 15-minute modules progressively making students aware of increasingly complex attacks:

- **Intro to Cyber Safety** — covers basic fundamentals of cyber safety using real-world examples combined with easy to remember steps to protect users and networks
- **Malware and Advanced Social Engineering Attacks** — covers the latest methods to infect users and the network through malware and how many of these infections can be avoided through safe Internet browsing habits
- **Focused, High-End Attacks** — covers how an employee’s Internet footprint can be leveraged to create a targeted attack and gain access to the network and sensitive information. The course also provides steps that employees can take to prevent falling victim to these types of attacks

Awards and Distinction

The feedback we have received from clients has been tremendous. In fact, the course has won the following awards:

- 2011 Marcomm Platinum Award
- Summit International Emerging Media Award
- Summit International Leader Award

Robust Training and Management Tools

Features

- Role management capabilities provide granular control of portal
- Status, score and duration shown for each attendee
- History reports available for all attendees
- Ability to require testing to ensure comprehension of course
- Customizable notifications including enrollment, drop, and utilization rates
- Administrative tools allow for the tracking of attendee activity
- Published in Articulate and compatible with Scorum 1.2

As part of training, students will receive:

- Course guide
- Cyber tips for home and work
- Cyber safety checklist
- Recommendations and links to online tools

Attendee Benefits

Cyveillance
a QinetiQ Company

After attending Cyveillance Cyber Safety, attendees will:

- Have a solid understanding of the latest online threats facing the company and its employees
- Know how the profile of an executive increases his exposure to targeted threats
- Understand how to protect family members from social engineering attacks
- Gain an understanding which threats pose the most danger now and in the future and how to protect against them

Benefits

Cyveillance Cyber Awareness program promotes a safer workforce.

Upon completion of these courses, employees will learn:

- How the most damaging attacks are actually executed
- How the profile of an individual increases exposure to threats
- How to better protect valuable data
- Which threats pose the greatest dangers today, which are likely to happen in the future, and practical tools and tactics to proactively protect against them

Optional Slides

Gartner Group Distinction

Cyveillance named in Gartner, Inc.'s recent *Cool Vendors in Security Services, 2008* report.

Gartner

"The cool vendors in security services that Gartner has chosen for 2008 represent **the "leading edge" in technological innovation** in these crucial areas. These vendors may not offer solutions that are appropriate for every enterprise's needs, but CISOs and other security decision makers should keep these vendors' offerings, and the changes in the business and threat environments they represent, on their "radar screens" in the coming year."

Third Party Endorsement

“Cyveillance owns a patented, homegrown data collection system that goes beyond the publicly searchable Internet, thus enabling the company to find threats that competitors who rely on public search engines and indices might miss.”

- Gartner, Brand Monitoring and Anti-Phishing Vendors, September 26, 2007

Intelligence Delivery Details

Cyveillance
a QinetiQ Company

As part of your Intelligence Delivery, your analyst will capture specific incident data which may include the following:

- **URL** - The incidents source URL
- **Supplemental URLs** - additional URLs and notes on additional sources relating to the same incident
- **Severity Level** - High/Medium/Low
- **Summary Title** - An incident summary that will appear in your emailed report
- **Analyst Notes** - The Analyst will summarize the main topics referenced in the incident
- **Message Type** - E-mail, Message Board, Standard Web, Usenet, Weblog
- **Sentiments** - Negative/Neutral/Positive
- **Topic** - Threat, Information Leak, Brand Violation, Other
- **Poster** - Employee, Activist, Agent, Vendor, Competitor, Customer, News & Journalist, Other
- **Subject** - Cyveillance Analyst will provide the subject of the post
- **Poster Screen name** - The posters screen name will be pasted out when available
- **Date** - The Date of the post
- **Geographic Location** - The posters location will be captured when available
- **Source** – Web/Blog/Twitter /Linkedn/ Myspace/ Facebook/ Youtube/ Other
- **Number of Visitors** - Metrics on Site Visitation
- **Client Feedback** - Clients can rate the value of the incident provided to ensure they remain relevant.
- **Client Note** - The CIC or portal provide the ability for our clients to create notes

Optional Other Case Studies

African Asset Search

Cyveillance
a QinetiQ Company

Scenario: Major aid donor provided funds to an African government for health, education and infrastructure. One-year audit revealed funds gone, but investments had not been made. Key questions were:

1. *Where had the money gone?*
2. *Could we identify target-owned seize-able/recoverable assets?*

Project: Given 24 specific targets (10 people, 14 business entities):

- Find the assets owned by the people
- Find relationships between the people and between them and the entities
- Find other related people and corporations – and their assets
- Immediately report assets/locations to client for photographing, repossession planning

Timeframe: 30-day project.

African Asset Search

Sample Findings:

1. More than 16,000 candidate documents found in open online sources; 396 relevant findings delivered

2. More than 100 specific assets identified, est. value >US$800m, including vehicle fleets, Russian cargo aircraft, cash hoards, corporate interests

3. Network mapping of 127 additional persons (involved family members, business associates) and 117 relevant companies and organizations

4. Specific details of a six-country diamond smuggling operation from East Africa to several Arab gulf states

Credit Card Issuing Retailer

Cyveillance
a QinetiQ Company

Problem

- **Retailer-issued credit cards being used to make fraudulent purchases**
  - Increasing fraud-related losses
  - Internal fraud detection systems not sufficient

Solution

- **Cyveillance provides identity theft protection module**
  - Internet Agents identify retailer-issued credit cards on the open Internet
  - Data feed delivered to retailer

Result

- **Cyveillance identified compromised accounts faster than other internal anti-fraud systems in 35% of all cases (including in-store transactions)**
- **Average fraud savings per compromised account of $4,700**

Global Credit Card Issuer

Cyveillance
a QinetiQ Company

Situation

- **Service provider felt that they were exposed to risk in number of areas:**
  - Credit card fraud
  - Merchants engaged in high risk or objectionable practices

Solution

- **Cyveillance hired to provide online risk monitoring and management**
- **Wide range of extraction agents turned on to monitor Internet for:**
  - Compromised credit and debit cards
  - Non-compliant merchants

Result

- **Identification of thousands of compromised credit cards**
- **Pinpointing of hundreds of merchants involved with tobacco sales, gambling and child pornography**

Leading ISP and Web Service Company

Situation

- ISPs' customers were frequent targets of phishing attacks
- Cyveillance desires end-point access to block consumers from phishing sites

Solution

- Cyveillance provides real time feed of phishing sites ISP
  - Integration of large scale spam feeds
- ISP's block millions of consumers from accessing dangerous websites

Result

- Improved security for ISP's customers
  - Competitive differentiation
  - Reduced support calls
- Enhanced value to Cyveillance enterprise anti-phishing customers

Operation Shady Rat

Who has been targeted?

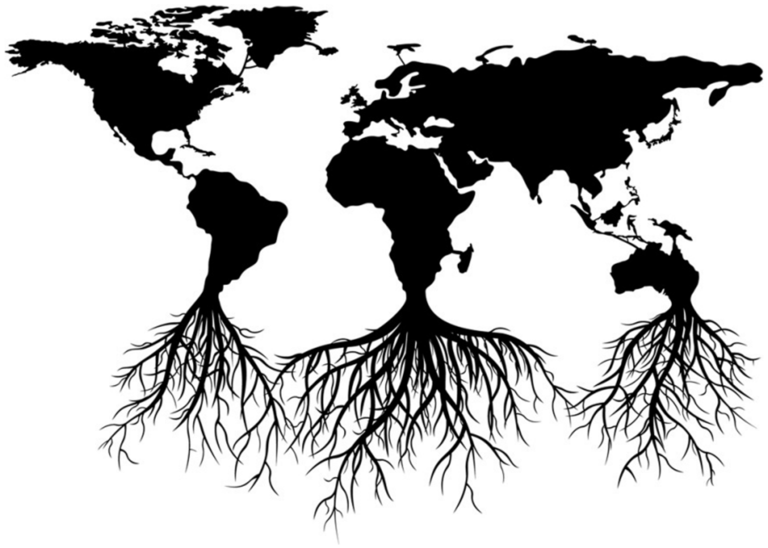
- More than 70 public and private sector organizations in 14 countries

What?

- What? Valuable intellectual property (including government secrets, e-mail archives, legal contracts, negotiation plans for business activities, and design schematics)

How?

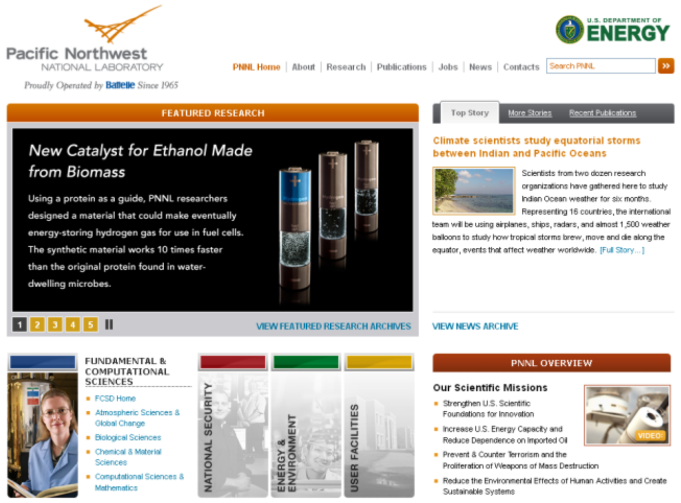
- Spear phishing attacks with email exploit that installed a back door



Source: http://www.vanityfair.com/culture/features/2011/09/operation-shady-rat-201109

Pacific Northwest National Laboratory

- Spear phishing attack on one of lab’s major business partners with which it shared network resources July 2011
- Hackers obtained a privileged account and compromised a root domain controller
- Intruders tried to recreate and elevate account privileges, but this action alerted the lab's cybersecurity team
- Within hours, the lab made decision to disconnect its network to prevent any further damage.



New Catalyst for Ethanol Made from Biomass

Using a protein as a guide, PNNL researchers designed a material that could make eventually energy-storing hydrogen gas for use in fuel cells. The synthetic material works 10 times faster than the original protein found in water-dwelling microbes.

Climate scientists study equatorial storms between Indian and Pacific Oceans

Scientists from two dozen research organizations have gathered here to study Indian Ocean weather for six months. Representing 16 countries, the international team will be using airplanes, ships, radars, and almost 1,500 weather balloons to study how tropical storms brew, move and die along the equator, events that affect weather worldwide. [Full Story...]

FUNDAMENTAL & COMPUTATIONAL SCIENCES

- FCSD Home
- Atmospheric Sciences & Global Change
- Biological Sciences
- Chemical & Material Sciences
- Computational Sciences & Mathematics

Our Scientific Missions

- Strengthen U.S. Scientific Foundations for Innovation
- Increase U.S. Energy Capacity and Reduce Dependence on Imported Oil
- Prevent & Counter Terrorism and the Proliferation of Weapons of Mass Destruction
- Reduce the Environmental Effects of Human Activities and Create Sustainable Systems

Source: http://www.informationweek.com/news/security/attacks/231601692

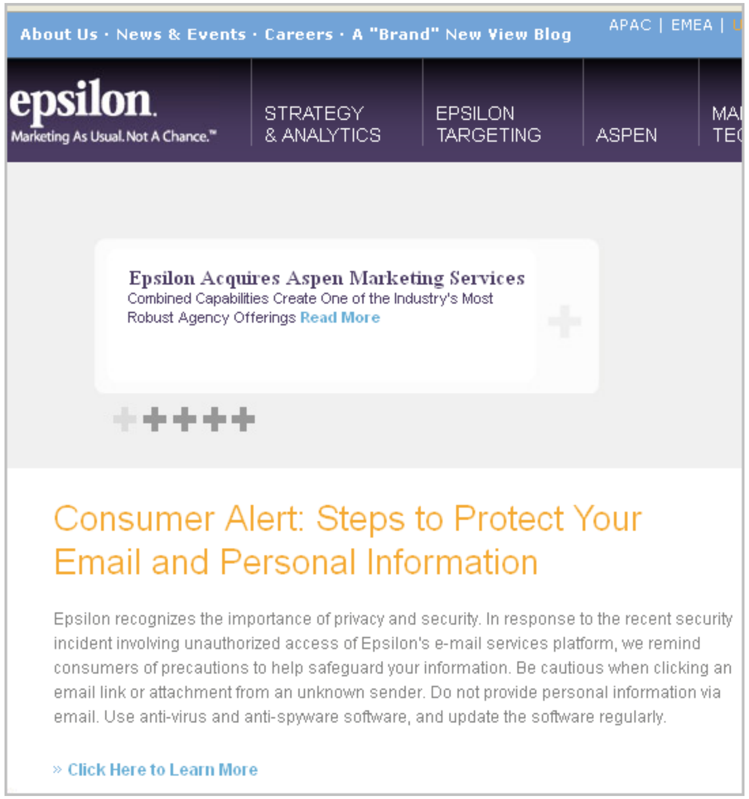
Epsilon: World’s Largest email service provider spear phished

Cyveillance
a QinetiQ Company

- Spear phishing attacks began in Dec 2010, but Epsilon didn’t discover breach until Feb. 2011.

- Attackers “only stole 2%” of customer data, but estimates state that Epsilon stores approximately 250 million emails.

- Big name customers of Epsilon were breached AND their customers were also put at risk.


About Us · News & Events · Careers · A "Brand" New View Blog
APAC | EMEA | U
epsilon.
Marketing As Usual. Not A Chance.™
STRATEGY & ANALYTICS
EPSILON TARGETING
ASPEN
MA TE

Epsilon Acquires Aspen Marketing Services
Combined Capabilities Create One of the Industry's Most Robust Agency Offerings Read More

Consumer Alert: Steps to Protect Your Email and Personal Information

Epsilon recognizes the importance of privacy and security. In response to the recent security incident involving unauthorized access of Epsilon's e-mail services platform, we remind consumers of precautions to help safeguard your information. Be cautious when clicking an email link or attachment from an unknown sender. Do not provide personal information via email. Use anti-virus and anti-spyware software, and update the software regularly.

» Click Here to Learn More

Oak Ridge National Laboratory

- Targeted in a spear phishing attack

- 57 of 530 employees targeted clicked on a malicious link – over 10%!!!

- Only a “few megabytes” of data were stolen before the lab discovered the breach