CMS NewsLine

June 2004 | Interpreting Technology and New Media | ISSN: 1540-5087

With Insecurity for All

Java as the Dark Star

By Leo B. Willner, Ph.D. with R. Gregory Kalsow,
Partners at Alvairi-Derfler Associates

Don't Miss the Last Word

CMS NewsLine offers items of interest for everyone.

Kalsow's Back-Channel offers candid comments from the publisher.

Each month you will enjoy commentary on the state of the industry, new media and technology.

CMS NewsLine accepts no advertising, so expect our point of view to be no-nonsense, and maybe even a little controversial.

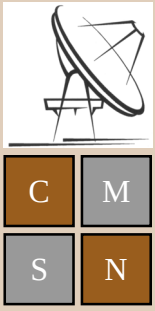
How much time and money are we as a technology based industrial society willing to spend to remain free of viruses, hackers, spam, worms, Trojan horses and popups on our PCs and coming soon also on our cell phones, TVs and PDAs? Unfortunately, the answer has to be ever more. With little notice great software houses such as Network Associates and Symantec have grown to multi billion-dollar status in the booming computer security game for good reason. When the likes of Microsoft and the US government are vulnerable to unexpected attack, is there a safe haven for anyone? No, indeed emphatically no! In what follows we probe the why and how nature of the present day information insecurity-for-all that has become an integral part of business reality, even to the point of invading our private lives. Try as we may few if any of us can fully escape this imminent danger. Just ask brother Bill Gates, master keeper of the Windows Seal. He may soon need to ransom an empire held hostage by the cyber-attack gangs and their nefarious schemes. As for the rest of us, we remain vulnerable — so read on.

"When the likes of Microsoft and the US government are vulnerable to unexpected attack, is there a safe haven for anyone?"

The fact of the matter is that we have now tethered many of our critical information systems and related resources together, like ships assembled in convoy or to await a pending storm. The reasons for this approach are many, but mainly the appeal and favorable economics of vast amounts of information made easily accessible, affordable and convenient to all. Unfortunately, this came at the high risk-price of 'insecurity for all'. By way of historic example we may recall that in its day the greatest library in the world in Alexandria, Egypt was the

CMS NewsLine

"Validating the Middle Ground"



CMS NewsLine
Alvairi-Derfler Associates
Lake Forest, CA 92630
Tel: +1.949.584.0989
www.ad-assoc.com
newsline@ad-assoc.com

repository of much of the knowledge of antiquity housed together in one great complex. In the year 272 AD this priceless archive was caught up in the winds of a temporal political change and tragically destroyed. As a result much of what was known of the history of the ancient world including vestiges of its art and culture went up in flames and was lost forever. Today, a somewhat equivalent danger exists whenever major information systems are linked together within ubiquitous global networks that are subject to viral and other attacks. Should we risk repeating history by linking together the systems housed in the Internet, the Intranets and VPNs? Or does Caveat Actor — let those who would take such a risk beware? Only the Shadow knows.

"In fact the popular term 'malicious code' nicely defines the nature of the beast and communicates the essence of the danger."

But what, may dilettantes and worshipers of technology for technology's sake ask, is the reality of the danger? Surely with sufficient backup, as in grandfather copies of electronic files, redundancy of systems, advance security systems and the like, can a major problem still remain one might ask? Pish, surely all will be well if we are just real careful! Not so fast, as the dangers inherent in the malicious–code cyber wars have a proven insidious robustness and vitality greater by far then has been broadly understood. After all, in the ready transference of executable code from computer to computer by the likes of Java engines, we have the makings of an immortal robust viral system that will test our systems in full. When you combine Java like packets with such tools as XML and put them both on the Internet and wire everyone and everything together, you've got yourself a potent devilish brew for producing self–replicating mayhem. In fact the popular term 'malicious code' nicely defines the nature of the beast and communicates the essence of the danger. When such malicious code finds itself in your electronic device, as in your PC, guess what, it can do malice, as in messing up, damaging or even destroying your vital files — such as tax records and credit card account numbers — or just stealing it and passing it on to others. For some corporate interests the one massive networked world may spell greater profit. For the rest of us a good deal of frustration and danger is also at hand, as when the Siren tried to lure the great Ulysses upon the rocks of a looming shore.

As the Internet and Java styled computer code are still in their early days, there is little in the US Code of Justice to fully protect the many business interests and private citizens from the varieties of dangers that lurk therein. Indeed the viral nature that underlies these invasions of privacy and private property are still evolving rapidly in unpredictable ways. Thus knowledge of the vectors and underlying processes that propagate these malicious cyber troubles and ensure the survival of their progeny are still unknown. In fact we are unable to discern the direction that future generations of these maladies will take.

As observed in the journals InfoWorld and InformationWeek, a record one thousand new viruses boarded the misdeed train just this past month, and overall the problem continues to worsen. In a fundamental way we need to appreciate the fact that complex degenerative 'disease' systems are inherently feasible within various complex systems, not just biological forms. Therefore, an arsenal of safeguards and cures is needed to protect any complex system from possible attack by dangerous 'viruses' and other miscreants so as to ensure its long–term effectiveness and survival.

At this juncture we are indeed far from establishing an overall solution to what ails the computer world and the Internet. Welcome to an era of computer intrusions, popup ads, viruses, worms, Trojan horses and yet to be imagined cyber destroyers — En Garde. That is to say that while temporary patches may yield some relief, nothing like a cure is yet in sight — not by a long shot. Indeed no foolproof encryption scheme is expected anytime soon. As to firewalls, they can all in time be breached as well. As to viruses including worms and Trojan horses, they are generally detected after an infection not before. As to Microsoft's Active Protection Technology — we will have to wait and see, but with a jaundiced eye for sure. IDS or intrusion detection systems are a good way to go, but unless you know what to expect, can you really do much about an unknown assailant? Regarding popups, there is no limit to the genius of Madison Avenue when it comes to fooling our minds and forcing us to watch, so they will continue to come over the parapet — bet on it.

"...a record one thousand new viruses boarded the misdeed train just this past month, and overall the problem continues to worsen."

Is the Internet likely to become moribund as the current rash of hackers and viruses persists for a few more years? That possibility does indeed exist; so it is up to us all to support workable partial solutions based on good safe practices and enforceable commercial and criminal law. Allowing individuals and corporations to willy–nilly invade the private space of others is indeed a great problem without a complete enforceable solution. When an individual trespasses onto the private physical premises of another without permission we have an illegal act that can be corrected by enforceable statute. Yet when someone sends Java like code into your computer without permission via the Internet, or gains permission by subterfuge, little can be done to correct the problem and the guilty go mostly unpunished while enriching themselves at our expense in the process — as with the Popup Advertising folks. Cookies anyone? Some folks might wish the 'baker' to choke on his fare.

As it is helpful to know the source of any serious problem, a consideration of the causes behind the danger to the network is in order. Consider the following: when you receive a letter

in the mail, it is a benign thing — as it can only be read or copied. It just sits there unable to represent a danger — as in the Jerry Lewis line "Sticks and stones may break my bones but words can never harm me." However, when someone sends a letter containing Anthrax to a US Senate office, as happened several years ago, we have a most dangerous situation. Specifically, the fact that it contains an active ingredient that can cause great harm is the issue — and it did great damage in that case. Similarly, when you receive an email containing only text, data or a picture, it is also benign and unable to cause any harm. However, when a sender is able to include executable computer code (read: a computer program that triggers the computer to follow specific written instructions) in his or her email to you, great danger may be at hand. Indeed when such instructions reach the primary registers of the computer's CPU (central processing unit) it will execute them. If the instruction says to wipe out one of your files, or copy some of your private information or send some of your material out to someone else, guess what, that is what is likely to happen. Please note that the Java concept continues to resonate favorably in the minds of many thoughtful computer experts, the problem is how to prevent and control transmission and infection by fellow–traveler piggy back malicious executable programs!

"The fact of the matter is that the so–called 'bad guys' are still gaining ground and winning, if not the war then at least the present battle."

Thus, and this is the central point, we must now face the downside of a Java concept powered world — although in honest duty Java truly represents a marvelous useful idea from the folks at SUN Microsystems. Used properly, the executable code generated by Java (or such related things as Active–X controls) and incorporated into email attachments can indeed be of great value to sender and receiver alike. Used with malicious intent it can do a great deal of harm. In the case of computer viruses, as hidden executable code in an email attachment, there is no limit to the harm that can be done. The answer is to buy, install and carefully use an arsenal of defenses including firewalls, popup blockers, anti–virus tools, anti–spam methods and intrusion detection systems (IDS) to defend our PCs, computer servers, set top boxes or other systems. Sometimes this works well while at other times it fails — but shame on us for not trying.

To the rescue have come great varieties of products and services from software houses offering useful but somewhat vulnerable PC barriers and other solutions. Unfortunately, all the progress made by the likes of Avaya, Cisco, Microsoft, Netgear, Network Associates, Symantec along with such less well known companies such as Ahn Lab, Air Defense, Barracuda, Blue Socket, FaceTime, Forum Systems, Lancope, PepiMK, Pest Patrol, Trapeze Networks, Trend Micro, Webroot and many others remains insufficient to turn the tide and fully relieve the danger. The fact of the matter is that the so–called 'bad guys' are still gaining

ground and winning, if not the war then at least the present battle. You, as the computer user or the client at the end of the network, are still at best only partially protected from the next evolution of cyber weapons. Make no mistake about it; this is serious business upon which the very security of the nation and its great institutions depends. For you personally, identity theft, privacy lost and the vulnerability of private assets at risk is a major problem today and perhaps even tomorrow.

There you have it; an email with a little Java like code and a spoonful of XML (fancied up web page text and designs that contains the data basis for its fulfillment) sitting on an open or partially secured network, and malicious mayhem is made possible. Now you have every right to be indignant and frustrated by this nasty turn of events. After all you are paying good money for your PC, for your LAN, your Internet access and its broadband and you rightfully insist that it work satisfactorily for you, but it may not and often does not. Indeed the main drivers for the success of the Internet and the PC lie in our ability to use email and to do web browsing and searching; say to locate a hotel, make an airline reservation or just get the local news or weather. Yet each of these actions is taken at some risk and may hide an attendant problem or even a disaster just for you.

A little Internet banking is easy to do and a real benefit, or so says the Bank of America. A little e–commerce is just the ticket, say on e–Bay, or so they say. But wait a minute, are you, your information and your system truly secure during these transactions — not exactly, for the systems you are using are proven by painful experience to be vulnerable — so say the experts. But not to worry, as (tongue in cheek) all will surely be well again soon, as once promised Little Red Riding Hood by that mean old hungry wolf. Comcast, HP, IBM, Microsoft, Time–Warner and Verizon can you save your world and rescue ours?

"Make no mistake about it; this is serious business upon which the very security of the nation and its great institutions depends."

A word of caution is also in order concerning all those grand networking schemes which favor putting all of one's e–world eggs into one basket, simply because we are able to do so. Here we point at a Holy Grail of electronic technology, the Quixotic–like quest for full media convergence. Is such chasing after windmills really a sound idea? We have been told — in truth propagandized into believing — that combining telecommunication, electronic information sources like the Internet and electronic entertainment from games, videos and television would be a great leap forward. But, in a world of viruses and electronic intrusion, is it also a leap into a bottomless pit of further mysterious failures and endless complexities? What indeed is wrong with a telephone that is just a telephone, a computer that is a computer and a TV that is little more than a TV? Is it truly necessary that our toothbrushes also substitute

as our razor or that our hairbrush contain a Bluetooth wireless connection to our stereo so we can in this way hear the news of the day in our bathroom as we brush our hair? If the great secular trinity of media is to inform, communicate and entertain, why must they be combined? The fact that it is possible to design underwear that can also double as a bathing suit need not lead us to want to swim in our underwear! If the network is indeed the computer, must we always be tethered to some great colossal all–in–one network? In a world of so much unknown cyber danger is it wise to do so?

In this Jeffersonian democracy the people are indeed still sovereign and must, as Jefferson implored, always act vigorously to protect their freedom and their vital interests from fools and from others who would violate their rights. There is no need to be passive in the defense of one's own privacy, private property or inherent right to sequester one's private world from unwanted commercial or malicious intrusion. The business community and well meaning citizens need to act in their own defense and counteract cyber crime and nail the cyber criminals. In this case the Bill of Rights may need some augmenting to ensure that backdoor Java and similar incursions are not allowed to penetrate and command the private affairs of citizens and their businesses. That is, that Java and its progeny working through the Internet not be allowed to empower any 'Great Satan' as its dark star.

In the struggle to make the electronic world and its networks as efficient as possible it makes sense to place computing power at the core, on the fringe and at the client end of the network. Under these circumstances it is only logical to consider the utility of moving some computer code down the network directly into client boxes or computers. The fact that this vector is also a potent channel for the transmission of viral and other computer diseases is the problem — and a great unintended consequence. For now this is a menacing danger that must be fully understood and against which great power must be arraigned or else we will all continue to suffer harsh consequences. After all, the purpose of individual computing stations is to achieve convenience, productivity and efficiency, all of which can be destroyed by hackers, spyware, pop–ups, viruses, worms and other unwanted intruders that invade the Java enabled cyber space.

"...this is a menacing danger that must be fully understood and against which great power must be arraigned or else we will all continue to suffer..."

Bedside Computer Insecurity

Doctor Heal Thyself

By Leo B. Willner, Ph.D. with R. Gregory Kalsow, Partners at Alvairi-Derfler Associates

Via their discovery of cellular DNA and its workings, the Nobel Prize winning biologists Crick and Watson revealed to the world the self–replication code structure that underlies all known biological life. Of course that includes the DNA mechanism of pesky and even deadly varieties of viruses, preons and bacteria. Unfortunately the analogy between biological forms and other complex systems extends to many structures of electronic computing including the sources of pestilence in computers. In recent years we have all become only too aware of the insidious malicious computer codes that destroy computer files, steal its content, take over its screens and even the keyboard and generally cause havoc. This form of pestilence represents an arsenal of annoying and harmful miscreants that can harm PCs, servers, network devices and other computers and spread their maladies across the broad network. Herein we visit the bedside of stricken 'sick' computers and consider what can be done today.

"...we have all become only too aware of the insidious malicious computer codes that destroy computer files, steal its content, take over its screens..."

In the process we must guard against losing perspective, exaggerating the danger or by too much analysis fail to act. As in biology, most computer code is benign and much of it can be helpful. Even a future symbiosis among the many computer systems can be imagined. In her seminal book ***Symbiotic Planet*** Lynn Margulis, the famous biologist, demonstrates that cooperation is the dominant basis of life on Earth, not competition – except among the largest varieties of animal life such as mammals. Over 3.6 billion years the primitive single–cell life form plants and animals evolved and prospered by cooperation and symbiosis, demonstrating thereby that 'survival of the fittest' via competition and warfare is generally not the only or most effective solution. Yes, most bacteria are generally your friend and often the source of your good health and nutrition. No doubt about it, but there is little solace in that knowledge for one suffering from a cold or the flu.

Similarly, only a rare combination of instructions within a computer program can damage a computer or its content. Yet, as with any destructive device, such self–replicating malicious software once discovered can be used to cause great harm. With the analogous situation of harmful microbes in mind, we can understand that computer–based 'sickness' will also be very hard to eliminate, i.e. the genie once released cannot be readily put back in the bottle. If this is indeed so, sick computers are with us to stay. Therefore, as with real viruses, we will simply have to learn to 'live' with computer disease as best we

can, and only cure what we can.

This brings us down to the computer battlefield and the practical matter of what to do to minimize the damage and protect computers and networks from intrusions and computer viruses today. What we suggest herein is a mostly defensive, adaptive and conservative approach. This may be a more protective scenario than what is commonly accepted to be best practice today. The latter suggesting that a more optimistic view based on patience, trust and a sense that all will soon be well again should be sufficient. Indeed, as outlined above, the nature and level of the threat appears far more severe than is understood by the general population and many of its business leaders. In what follows our approach is also meant to be simplistic and pragmatic to the max:

"Install Zone Alarm or Norton Firewall, on every PC even if hardware or software firewalls are already in place upstream on your network and its routers."

Employ Multiple Defensive Solutions

For example, to catch and rid yourself of all the computer spies lurking inside your computer do not simply rely on any one anti–spyware system. Instead use a combination of, say, Spybot Search & Destroy, SpywareBlaster and Lavasoft Ad–aware to protect yourself. To your surprise you will discover as we did that it takes all of these and more to fully do the job of cleansing and immunizing your system.

Install a Software Firewall

Install Zone Alarm or Norton Firewall, on every PC even if hardware or software firewalls are already in place upstream on your network and its routers. Configure your firewall to the maximum or stealth level security.

Properly Configure Your Firewall

Verify that the SPI, or Stateful Packet Inspection, feature on your broadband access router is turned ON. In general, take the time to become familiar with all other security features available on your systems. Also make it a habit to deny most on–screen prompts for access to the Internet, except when you are certain of its benefit to you – as when, say, your Windows XP or Norton SystemWorks makes such a request.

Shoot The Messenger

Unless you truly have a need, turn off Windows Messaging, DCOM and universal plug and play (UPnP) on your computers, as these can become gateways to big trouble. The website www.GRC.com contains many helpful tools for locking down and protecting the more than one thousand access ports to your PC. In particular, such programs as Shields Up, Unplug n' Pray, Shoot the Messenger and DCOMbolbulator available on that site can at no cost do the job for you.

Separate Lean–Forward and Lean–Back

Avoid permanently networking your TV with your PC. This advice may sound like a bit of reactionary heresy, but a little caution may be called for in this arena as well.

Don't Chat on the Internet

For the time being, be late to depend on Voice over Internet Protocol or VoIP: Encrypted it may be, but your voice communications on the Internet are accessible to all as well as subject to failure and loss. As to its sound quality and fidelity, these are improving.

Avoid the Triple Play

An all–in–one service provider for telephony, broadband and cable sounds good but also represents some exposure. Time–Warner and the other cable companies want to sell you these 'big three' as a bundle, but be careful. For example, when the Comcast cable service to this office went down yesterday, the SBC telephones continued to work while Internet service via DSL stayed online.

Pull the Plug

Keep one computer private and off the networks. In today's pathologically infected cyber world, better to keep one computer virginal and fully uninfected. This computer should house the most private and valuable documents such as trade secrets, business strategy, tax records and the like. Of course the likes of the accounting firm Arthur Anderson, the FBI and the IRS would find it most inconvenient were you to follow this advice.

"Keep one computer private and off the networks. In today's pathologically infected cyber world, better to keep one computer virginal and fully uninfected."

Do Not WiFi in Public

We just got zapped very severely after using one of our laptop computers in a coffee shop. Apparently their network was not well protected, and our firewall failed to defend. Unless you are forced to, avoid WiFi wireless access in public places.

Maintain Some Hardwired Telephones

Cell phones are very useful, satellite phones are an exciting development and VoIP is surely part of the future, but hard line telephones are still by far the most reliable and the most secure.

Use Multiple Layers of Backup

As infections can be insidious and failures hard to predict, for critical documents and valuable systems, the more the merrier. Even the largest systems in the world, say at the Pentagon and at the IRS do go down and do at times fail to recover critical records. Believe it or not.

Keep Paper Copies of Key Records

What a backward pointing commentary it is to suggest that paper records are still of real value and even a necessity. Nonetheless, face it, in some emergencies that will be your only workable backup or accessible source of critical information.

Protect Your Plastic

Exercise caution with credit card usage on e–Commerce. While the systems keep improving and many credit card schemes are sophisticated, they need only fail once for you to be badly hurt. Furthermore, without a lawyer, see if you can ever get anyone from Visa or Master Card on the telephone in an emergency; except a lowly clerk reading off a cheat–sheet while reluctantly responding to your distress call.

Keep Banking Personal

Use caution while e–Banking. Ditto the previous point. Identity theft is a major crime today and banks still have the nasty habit of violating their own privacy rules when it comes to information about you or fully protecting your records.

Don't Trash Your ATM Use Cash

Avoid using ATM cards for purchases. Electronic money is not your friend. ATM cards are good for getting cash or

Send a question or comment by e-mail:
Click Here

doing ATM bank transactions. When you use your ATM card to make a purchase you are inviting outside parties to access your private bank accounts. Caveat Emptor and Caveat Actor.

Rotate Your License Plates

Change your email address and password often. Sometimes it is the simplest most primitive solutions that work best. In the security business discontinuities in patterns of behavior can often be the best defense. And what is more of a discontinuity then changing one's address and one's locks.

After the Binge: Purge

Delete unnecessary old files. A simple but effective way to reduce the size of the target and the level of exposure you represent. Such files may contain information that is of no value to you but can be of use to criminals and illegal databases.

"Change your email address and password often. Sometimes it is the simplest most primitive solutions that work best."

Your Business Card

Use flash memory cards for secondary backup. This approach appears to have a number of advantages such as access keys, no mechanical parts, stability, easy of use, storage and transport and the like. Nonetheless, this approach should only be employed in conjunction with other backup systems.

Beware the Abyss

Avoid unknown files, websites and e–mails: Obvious but true. Avoid illegal software: It may indeed contain all sorts of hidden dangers. Avoid public P2P systems: Here is the best place to get an infection and destroy your computer. Be careful with freeware: Quality and possible corruption are the dangers that may be lurking therein.

The Ounce of Prevention

Be Ever Vigilant and Proactive: This is your first and best defense. The PC on which this article is being written is at the present moment infected with several worms, Trojan horses and spyware. That is a fact of life, even though it has just undergone a most thorough cleaning with the latest and greatest anti–everything software this very morning.

Scan the Horizon

Read PC World of June 2004: There you will find a lot more useful information and detail on the best current products and services to consider.

These prescriptions do not represent a mutually exclusive or collectively exhaustive approach to the great problem of sick computers. Neither does it necessarily suggest today's best science. Mainly what is intended herein is to ring the alarm loudly, give you a leg up and recruit you to the line of best defense.

(Leo Willner and Greg Kalsow contributed to this issue. In order to discuss any of these points with the authors, please e-mail them at: leo@ad-assoc.com and greg@ad-assoc.com)

[CMS NewsLine frequently publishes the works of contributing writers. The views expressed are strictly those of the contributors. CMS NewsLine makes no endorsement of their opinions.
—Georgia Pech, Editor]

■ Digital Millennium Copyright Act — "There you go again!" Ronald Reagan would have said! It seems that the reactionary forces are as always blocking the road, again. In this case Representative Dick Boucher of Virginia is seeking to bring balance back to the DMCA with his Digital Media Consumers' Rights Act of 2003 and those who might, say, resist replacing a broken lock if it interferes with tradition, are raising 'there you go again' barriers to its passage in the US Congress. The fact that Jack Valenti is about to depart the scene and retire from the MPAA may indeed finally herald in a day when 'copy once' balance is brought back to Fair Use in copyright jurisprudence. In the final reckoning this new law will help and not hurt the motion picture business and the electronic media industry in general. All hail Dick Boucher!

■ No One Is Safe From Attack — In the past few weeks we have read headlines that read: "Cisco Posts Vulnerability", "Big Internet Hole Found", "War Against Spam Rages On", "Tiny Evil Things", "The WiFi Security Challenge", "Virus Fix Slows Down Cox E–Mail Server" and many more. Face it; if the likes of Cox, Cisco, Microsoft and the rest have problems you've got problems too. The cost in time lost and system inefficiencies that attend these difficulties is massive, say scores of billions of dollars, and the computer insecurity problem continues to worsen. This is indeed a form of modern terrorism.

■ On Broadband World War Revisited — The announcement that Verizon is after a media triple–play of its own in competition with the national cable companies heralds in a great new battle for media hegemony. We can just hear the gnomes at Comcast and Time–Warner casting bones and conjuring up evil spirits! How dare those pathetic telephone guys confront mighty cable? Where are all the well–paid sycophants housed in the US Congress when you need them? Don't they remember their newfound loyalty to cable, vis a vis their old patrons — the soon to be discarded folks in the telephone biz? I guess it is fair after all. If the cable folks with their triple–play of broadband, TV and Voice over IP are allowed to challenge the telephone business of Verizon, guess what, Verizon can run fiber to the home as well and offer its own version of the triple–play. In truth, in contrast to the sometimes slow–to–think cable dreamers, those Verizon guys are smart, hot and on the ball. Nonetheless, monopolists as always have the early advantage. Can you hear us AT&T, US Steel, Kodak, Dupont and the old Standard Oil? But wait a minute; all these former 'monopolies' are now dead and buried — surviving only as shackled shadows of their former selves! So Teddy Roosevelt was heroic after all and Verizon may indeed be on the right track. Still, for the lowly consumer — as in you and me — the triple–play does not spell greater service or security but a 'goulash' as in a mixed up stew!

[Your mileage may vary. —RGK]

Send a question or comment by e-mail:
Click Here

About CMS NewsLine

CMS NewsLine is published monthly by Alvairi–Derfler Associates, a Market Development company, which specializes in assisting corporations with:

- Full Life Cycle Marketing Support
- Product Development and Product Strategy
- Branding and Positioning
- Business Development and Strategic Alliances
- Communications, Launch and Deployment Plans

At Alvairi–Derfler Associates, senior partners personally manage every engagement.
Contact us today at:
info@ad–assoc.com or +1.831.427.3833

Alvairi™-Derfler Associates

Better Marketing Execution

Alvairi-Derfler Associates is a MARKET DEVELOPMENT company situated to help your company navigate through its most challenging marketing problems. It is also there to assist you sort through and exploit the marketing opportunities your company now faces. Alvairi-Derfler partners, each with twenty or more years of direct field experience, can help prepare broad-based, professional, time-tested alternatives for action by you and your team.

Working hand-in-glove with your in-house corporate team, Alvairi-Derfler partners can:

- Assess New Product Opportunities
- Gauge Competitive Threats to Products and Markets
- Refine Specific Pricing Tactics
- Determine How to Reposition Products and Services
- Provide Comprehensive Support for Your Trade Shows
- Optimize Advertising Campaigns and Promotional Programs

Better Marketing Tools

Clients of Alvairi-Derfler Associates enjoy the confidence gained from thorough analysis, meticulous preparation and crisp execution leading to:

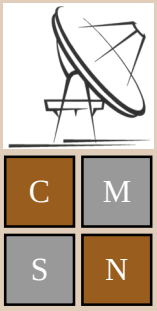
- Better Targeting of Products
- More Effective Branding
- Sharper Pricing
- Improved Sales Promotions
- Better Communications
- More Effective Advertising
- More Efficient Distribution Systems
- Crisper Command and Control

Alvairi-Derfler partners also participate in business development activities involving new marketing relationships with third parties to help create advantageous alliances, organize licensing and joint development agreements and the like. When needed, its senior staff can help facilitate a client's outside business relationships in new markets at home or abroad.

Please contact Alvairi-Derfler today for an informal chat, to discuss a business situation, or to get advice on a new product or a changing market.

Silicon Valley: +1.831.427.3833

So. California: +1.949.584.0989



CMS NewsLine
Alvairi–Derfler Associates
Lake Forest, CA 92630
Tel: +1.949.584.0989
www.ad–assoc.com
newsline@ad–assoc.com

Subscribe to CMS NewsLine

CMS NewsLine is available only by subscription, and is e–mailed to our subscribers at no additional charge.
To subscribe using your credit card, please visit:
http://www.ad–assoc.com/ or Click Here
Send a question or comment by e-mail: Click Here

Every month you will enjoy thought–provoking analysis of the significant issues driving the growth of new media, technology and entertainment.

Georgia Pech, Editor
CMS NewsLine