



TRIDENT NEWS

SPECIAL EDITION - THE SECURITY INDUSTRY

TRIDENT CAPITAL®

Volume III, Issue 2 • 2005

TRIDENT CAPITAL'S SECURITY FOCUS

by Rebecca Bace, Trident Capital Venture Consultant

Even before the events of September 11, 2001, Trident Capital had an interest in the area of information security, with early investments in message understanding products and vulnerability management technology for networked systems. In late 2001, however, Trident made an enhanced commitment to investing in security technologies, and has built an impressive portfolio of security firms. With the recent close of a new \$400M fund, we are well positioned to add other security firms to the portfolio as the opportunity arises.

It seems that no day is complete without a press report of yet another critical system breached, another system failure diagnosed as stemming from a hacker attack. However, strategies applied by commercial enterprises, especially those in security-sensitive financial and health care markets, to protect their online assets rarely rates coverage.

There is a critical difference between the technologist's and the business person's views of information security. Technologists often focus on attacks, the associated effects of those attacks, and techniques for preventing the attacks or blunting their impact. When business people consider security, they focus on different things. As in other aspects of business, the core issue is *risk* – how much does the attack cost, in denial of access, in damage to reputation, in fines levied by regulators, and in extreme cases, in damages awarded in legal actions? The other factor in risk equations, of course, is the cost of prevention. As many classic security practices originated in Cold War era military settings, where the ramifications of security failures were grave and protection budgets generous, cost containment can be a novel idea in some security circles. In the commercial world (and increasingly, in government markets as well) cost matters.











Trident established its portfolio using an integrated strategy drawn from a deep understanding of how enterprises secure their information assets and how those protection needs are likely to evolve over time. The portfolio companies provide complementary functions, enabling strong strategic alliances.

Let's use the enterprise security and protection process model to structure a discussion of the role each portfolio firm plays. Note that all processes are not populated with portfolio firms. These processes include:

Security Planning and Strategy – this includes identifying key assets, performing tradeoff analyses in the context of a risk model, and documenting a security policy, both for network services and the data systems that are connected by those networks.

continued on page 6

Trident Investments in Security Technology

	Wireless Security
	Software Anti-Tamper Solutions
	Message Understanding
	Robotics - Homeland Security
	Virtual Private Network (VPN) - Network Protection
	Vulnerability Assessment and Management
	Endpoint Protection
	Provisioning – Identification, Authentication & Authorization
	Identification, Authentication & Authorization
	Intelligent Video Surveillance - Homeland Security

Trident Capital Security Team

Peter Meekin

Managing Director
pmeekin@tridentcap.com

Becky Bace

Venture Consultant
rbace@tridentcap.com

Don Dixon

Managing Director
ddixon@tridentcap.com

Howard Schmidt

Venture Consultant
howard@schmidt.org



AirTight Enables Secure and Reliable Wireless Networks

According to industry analysts Radicati Group, by 2008 wireless networks will be a mainstay of over half of U.S. enterprises. Security is considered one of the issues that will accompany this transition. "AirTight's goal is to enable enterprises to deploy WLANs that are as secure and reliable as their wireline counterparts," said David C. King, AirTight Networks' CEO. "With SpectraGuard, CIOs and CSOs gain control of their 'enterprise air' and know that only authorized Wi-Fi users are con-



provides

ected to the trusted enterprise network."

Companies such as Katera Technologies are using AirTight to ensure that their Wi-Fi deployments are secure. "We required a wireless security solution to protect us from the threat of rogue AP's and from client machines connecting to neighboring wireless networks," said Ron Leedy, Director of Managed Services, Katera. "SpectraGuard 2.0's accurate auto-classification and reliable intrusion protection us with real air cover for both

our wired and wireless network security."

"As wireless LANs become the default network connection for so many mobile users, there is an increasing emphasis on the security aspects of both the fixed and wireless components of an enterprise network," said Craig J. Mathias, a Principal with the wireless and mobile advisory firm Farpoint Group. "AirTight's Spectra Guard product has a great combination of features to address both of these elements, and will appeal equally to enterprises using wireless LANs as well as those simply seeking a greater level of security for their wired infrastructures." ❖

www.airtightnetworks.net

Arxan Enables Legal Online Sharing of Copyrighted Material

Peer to peer (P2P) networking has given the music and movie recording industry considerable problems enforcing copyrighted material. A P2P network allows users to share network bandwidth, storage, and swap digital content (including music and movies). These networks, until recently, have been unmonitored, allowing billions of copyrighted digital files to be traded annually between P2P users. Overall, it has been estimated that P2P



illegal file sharing has knocked off 17% of record label sales in the past three years.

The RIAA has followed up on this concern with a series of lawsuits against the legal P2P companies that among other things mandate that they better protect their copyright filtering software against hacking. As part of an RIAA settlement mandate, one of the larger P2P music/ video/game/software companies recently retained Arxan to help them solve this

copyright protection challenge.

Utilizing its EnforcIT-S products, Arxan quickly created and implemented a unique guard network that was inserted into the binary code of the filtering software. The protection passed several RIAA approved hacking evaluations and is currently deployed. With several similar RIAA lawsuit settlements already awarded and the MPAA just beginning a similar legal strategy for the copyright protection of movies, Arxan is positioned to become an important part of the effort in promoting a legal file sharing Internet environment. ❖

www.arxan.com

Cymfony Awarded U.S. Government Contracts to Develop Information Discovery Software

Cymfony, Inc., an award-winning market intelligence and media analysis firm, has been awarded a series of significant research and development contracts from the Air Force Research Laboratory (AFRL), Information Directorate. Under these contracts, Cymfony will develop information extraction, text mining and analysis software to assist in Air Force Intelligence

and Homeland Security efforts.

Included in the work funded under these contracts is the research and development of software that will enable the government to extract and consolidate information on individuals and organizations from thousands of textual



documents, pinpointing time and dates of events, and identifying specific entities. These capabilities significantly enhance homeland security efforts.

Cymfony develops innovative market, business and gov-

continued on page 3



Cymfony continued from page 3

ernment intelligence solutions based on its proprietary information extraction technology called InfoXtract. The InfoXtract engine performs statistical and grammatical analysis using a unique

approach to natural language processing (NLP) to automatically extract relevant information from text documents – including key entities, relationships, people, companies, events and associations. Cymfony’s flagship market intelli-

gence solution, Cymfony Dashboard, is used by many of the world’s leading global brands and provides the industry’s most comprehensive real time media analysis solution. ❖

www.Cymfony.com

iRobot G&I Division Expands Government Market Presence

Beginning with the June 2004 opening of its new office in Crystal City, Virginia (within view of the Pentagon), iRobot’s Government & Industrial Robotics (G&I) division has maintained and expanded its visibility and stature in government markets.

iRobot’s PackBot, a reconnaissance and tactical robot, continues to be a vital tool for the U.S. military. Today over 100 PackBots are deployed, mainly in Iraq and Afghanistan, disarming improvised explosive devices, and searching potentially hostile caves and buildings for terrorists. The PackBot EOD system is



**Colin Angle
CEO**

used on a daily basis to defuse roadside bombs and other dangerous explosives, saving soldiers’ lives in the process. The military values PackBot for its lightweight, rugged design and its ability to rapidly respond to numerous dangerous scenarios.

The U.S. Army’s Future Combat Systems (FCS) program awarded iRobot additional funds to develop a next-generation Small Unmanned Ground Vehicle,

bringing the total contract to over \$37 million. Much of these funds will be used for simulation work and field deployments. iRobot continues to score

high marks from the military and the Lead Systems Integrator, Boeing, for iRobot’s responsiveness and performance in the program.

The G&I division also unveiled a joint effort with John Deere to develop and deploy an intelligent unmanned ground vehicle that can autonomously perform dangerous and taxing military missions. Dubbed the R-Gator, the vehicle is built on John Deere’s M-Gator platform and utilizes iRobot’s military robotic controls and navigation technology. Working together, the companies will share expertise and insight to further grow the military robots market. ❖

www.irobot.com

Single Source Model Key to MegaPath Success

One indication that information security is a permanent fixture in commercial enterprises is the fact that cost of protection is considered in the selection of security solution vendors and delivery models. The existence of good information security means little unless it is affordable, reliable and non-disruptive to the business activities enabled by the secured networks. There is significant advantage to those who can deliver security integrated with core network access. MegaPath Networks, an early

Trident investment which provides managed secure network solutions to businesses, has translated this insight into an award-winning growth rate.

MegaPath currently serves in excess of 65,000 endpoints through its nationwide private network, for 18,000 customers that range from large distributed enterprises to small professional storefronts. It delivers secure access and managed network services to distributed enterprises.

MegaPath’s success is recognized by its inclusion (ranked

#127) in *Inc.* Magazine’s 2004 list of the 500 fastest growing private companies in the U.S., in recognition of its four-year average sales growth of 239 percent. In addition to the *Inc.* 500, MegaPath was also named to the *East Bay Business Times* list of the 50 fastest growing private firms in the East Bay and to the *San Francisco Business Times* Fast 100 list for the second consecutive year. MegaPath has been both a visionary and a leader in Gartner’s Magic Quadrant over the last two years. In 2003, MegaPath won the VPN Product of the year award from Network Magazine. ❖

www.megapath.net



**Harry Taxin, Chairman,
President & CEO**



Qualys and the Laws of Vulnerabilities

by Gerhard Eschelbeck,
CTO and VP Engineering,
Qualys, Inc.

Successful defenses against network vulnerabilities require understanding the nature of the risk they pose. The uncertainty of conventional, human-led security efforts frustrates security officers trying to guarantee protection for their organizations.

New research analyzing nearly 4 million network vulnerabilities shows their frustration is warranted. Specifically, the research concludes that companies currently take 62 days to patch their internal systems, as opposed to 21 days for systems connected directly to the Internet. This window leaves internal systems and applications, such as Internet browsers and mail servers, vulnerable to attack.

The data reveals four “Laws of Vulnerabilities”:



Philippe Courtot
Chairman & CEO

Half-Life: The half-life identifies the length of time it takes users to patch half of their systems, reducing their window of exposure. The half-life of critical vulnerabilities for external systems is 21 days and for internal systems is 62 days. This number doubles with lowering degrees of severity.

Prevalence: 50 percent of the most prevalent and critical vulnerabilities are replaced by new vulnerabilities on an annual basis. In other words,

there is a constant flow of new critical vulnerabilities to manage.

Persistence: The lifespan of some vulnerabilities and worms is unlimited. In fact, the research shows significant spikes in the reoccurrence of Blaster and Nachi worm infections in 2004, months after they originally appeared.

Exploitation: The vulnerability-to-exploit cycle is shrinking faster than the remediation cycle. 80% of worms and

automated exploits are targeting the first two half-life periods of critical vulnerabilities.

These Laws of Vulnerabilities document the effects of human-based security efforts, and the persistent ability of attackers to gain full control of systems – including access to highly sensitive information. Resolving issues revealed by this research requires understanding the causes and means for prevention.

Network security attacks are increasing in number and sophistication and new research shows that some vulnerabilities linger on, often without end. New attacks are capable of spreading faster than any possible human response effort necessitating automated defense mechanisms. The timely and complete detection of security vulnerabilities with automated techniques and rapid application of remedies is the most effective preventive measure security managers can use to thwart automated attacks and preserve network security. ❖

www.qualys.com

Sygate Sweeps Industry Awards

Sygate Technologies, the industry leader in Enterprise Endpoint Security, has had an extraordinary year. Beginning in May 2004 with Sygate’s recognition by Red Herring Magazine as one of the “Red Herring 100,” the 100 most promising private companies, Sygate has racked up an impressive array of industry awards and accolades. These awards include:

- Innovative Technology



John DeSantis
President & CEO

Award from Computer-world (for a Sygate deployment at Partner Re)

- 8.1 (on a ten point scale) rating in Info World’s client security review – Sygate scored better than industry giants such as Symantec and Trend Micro
- “2004 Product of the Year” award from Information Security Magazine for the security management systems category (based on cus-

tomers feedback)

- Nomination as “Best New Security Solution for 2004” by SC Magazine
- “Tester’s Choice Award” - Network Computing Magazine’s Secure Enterprise Competitive Network Access Control & Enforcement Review
- “2004 Codie Award” - Finalist, Best Enterprise Security Solution Category, by Software and Information Industry Association (SIIA)
- Gartner Magic Quadrant leader, Personal Firewalls ❖

www.sygate.com



Lehman Brothers Relies on Thor for Provisioning

One might wonder how identity management systems such as Thor's Xcellerate address enterprise needs. Consider this account from Lehman Brothers, a Thor customer:

"After reviewing a number of provisioning vendors, we chose a system from Thor Technologies and began rolling it out in December. To date, we've made it available in three regions—the Americas, Asia and Europe—providing all 15,000 employees with access to core



Alberto Yopez
Chairman & CEO

applications. More than 200 applications will be integrated with the system by the end of this year. When complete, the provisioning system will manage roughly 250,000 IDs.

"We estimate that automated provisioning for the major platforms alone saved us 1.3 worker-years in the first four months—96,050 hours in creating accounts and 40,590 in disabling them. The user efficiency and security gains have been of even greater value. We streamlined the

request and approval processes, and new users now gain access to applications and become productive far more quickly. We enhanced overall security as well. Consistent business policies are applied to every request; users are automatically de-provisioned when they leave the company; and auditing and reporting capabilities give our management visibility into every aspect of who has access to what."

Thanks to positive customer experiences such as at Lehman Brothers, Thor reports that in 2004 revenues increased more than 100% over 2003, and Thor quadrupled its customer base. ❖

www.thortech.com

TriCipher Launches at RSA Security Conference

Incubated as a division of NSD Japan, a multi-billion dollar Japanese systems integration firm, TriCipher launched as a stand alone entity in the US in February 2005. The company has been developing its unique strong authentication technology for more than four years while working with selected customers in health care, financial serv-

ices and government. The technology is based on patents developed by the founders while working at Bellcore and now licensed exclusively from Verizon Communications. TriCipher recently closed a \$10+ million round led by Trident Capital and



Ravi Ganesan
CEO

ArrowPath Venture Capital. Additional investors include INTEL Capital, Zions Bank and Wasatch Ventures. ❖

www.TriCipher.com

Vidient SmartCatch Gains Broad Acceptance in Market

Driven by modern needs for intelligent video surveillance, Vidient Systems' SmartCatch video surveillance software is in use today in selected applications at major airports, such as San Francisco International, Salt Lake City International and San Diego International, and within major corporations and public institutions, including Raytheon and the Jewish Community Center of San Francisco.

"Security demands and



Brooks McChesney
President & CEO

mandates at airports are constantly changing, and we were looking for a more sophisticated technological approach to monitoring and controlling employee access to our most secure areas," said Paul Foster, Aviation Security Manager at SFO. "We wanted a system that could accurately identify and track people failing to control access—more specifically, people tail-gating or piggy-backing, even people behaving suspiciously near high security areas.

"With SmartCatch, we can

monitor specific, high security access doors to ensure compliance with access control procedures and to take corrective action, whether it's immediately or at an appropriate later time."

Vidient was formed by a spinout of technology developed at NEC Labs. Vidient provides video surveillance software for CCTV networks, a \$3 billion global market in 2003 that is projected to grow 25-30 percent annually for the next five years, according to New York City-based Mallon Associates, a leading firm that tracks the global security industry. ❖

www.vidient.com



TRIDENT CAPITAL'S SECURITY FOCUS *(cont'd from page 1)*

Vulnerability Assessment and Remediation – *Vulnerability Assessment* includes discovering what systems are connected to the enterprise network, and testing them for known vulnerabilities. *Remediation* is the process of addressing the vulnerabilities so identified, and includes tracking the application of software patches to vulnerable systems, thereby closing the security holds before they can be exploited. **Qualys, Inc.**, one of Trident Capital's earliest security investments, is a market leader in Vulnerability Assessment and Remediation. It offers full-spectrum support for this critical security function, ranging from R&D that tracks vulnerabilities from earliest indications, to its flagship service, QualysGuard, which provides web-based continuous assessment at reasonable cost.

Identification, Authentication, and Authorization – *Identification* is establishing exactly who is accessing a system or other enterprise asset. Authentication is establishing that the person so identified is really who they say they are. The final ele-

ment of the triumvirate is Authorization, which addresses the question "are you allowed to access the asset you're attempting to access? IA&A includes Provisioning (which handles the issue of managing identity across multiple systems), authentication devices (including biometrics and tokens,) and public key infrastructure (PKI), which allows the operation of IA&A, across large networks. One of Trident Capital's newest security investments **TriCipher**, provides strong authentication, using an easy-to-manage appliance-based approach. Another Trident investment, **Thor Technologies**, is considered a major force in identity management and user provisioning. Thor's flagship identity management product, Xcellerate, features adapters that ease integration pains when enterprises bring legacy and custom applications under identity management system control.

Network Protections – This covers the protection against attacks targeting the network infrastructure and the data traveling over that network. Protections include

VPNs (Virtual Private Networks), which encrypt network traffic so that someone eavesdropping on the network traffic can't read the transmitted data; Network Firewalls, which allow one to limit the types of network connections that can occur on a network; and Network Intrusion Detection/Intrusion Prevention systems, which monitor the network traffic looking for either symptoms of known attacks or abnormal traffic patterns or content. **MegaPath Networks** is considered a market leader in secure access and managed network services, and provides award-winning managed VPN services.

Endpoint Protections – This covers the measures, usually software residing on the servers, desktops, and other systems in enterprises, which protect those systems from attack. The protections placed at the endpoint systems include antivirus software, and personal firewalls, which limit the traffic that can be admitted to the system from the network as well as the traffic that can be transmitted by the system out

continued on page 7

Boards of Directors

AirTight Networks

David King - AirTight Networks
Kiran Deshpande - AirTight Networks
Danial Faizullahoy - Walden International
Mark Smith - Infoblox
Eric Zimits - Granite Ventures
Woody Marshall - Trident Capital (board observer)
John Moragne - Trident Capital (board observer)

Arxan

Richard P. Earley - Arxan
Peter Meekin - Trident Capital
John Klein - Trident Capital/Polarex, Inc.
Brian Gannon - Lunn Partners
Beau D. Laskey - EDF Ventures
Lt. General Kenneth A. Minihan - USAF (Ret.), Paladin Capital

Cymfony

Andrew Bernstein - Cymfony
Rohini K. Srihari - Cymfony
Peter Meekin - Trident Capital
Scott English - Hearst Interactive Media
Alfred C. Sikes - former President, Hearst Interactive Media

iRobot

Colin Angle - iRobot
Helen Greiner - iRobot
Rodney Brooks - CSAIL at MIT, iRobot
Peter Meekin - Trident Capital
Ronald Chwang - Acer Technology Ventures
Jacques S. Gansler - University of Maryland School of Public Affairs
Andrea Geisser - Fenway Partners
George C. McNamee - First Albany Co's

MegaPath Networks

Dr. Harry M. Taxin - MegaPath
Woody Marshall - Trident Capital
Lawrence M. Howell - Howell Capital
Steven M. Krausz - U.S. Venture Partners
Thomas E. Pardun - retired Chairman of the Board, Western Digital Corp.
John Peters - Former CEO, Netli & Sigma Networks

Qualys

Philippe Courtot - Qualys
Don Dixon - Trident Capital
Yves Sisteron - GRP Partners
Howard Schmidt - eBay
Alex Vieux - Dasar/Red Herring

Sygate

John DeSantis - Sygate Technologies
Chris Guo - Sygate Technologies
Peter Meekin - Trident Capital
Skip Glass - former CEO, uRoam
Bernard Harguindeguy - Critical Path
Keng Lim - former Pres/CEO, Escalate, Inc.
Howard Schmidt - eBay Inc.

Thor Technologies

J. Alberto Yopez - Thor Technologies
Peter Meekin - Trident Capital
Peter Roberts - Longworth Venture Partners
Jeff Schwartz - Bain Capital Ventures
Kevin Talbot - RBC Technology Ventures, Inc.

TriCipher

Ravi Ganesan - TriCipher Inc.
Peter Meekin - Trident Capital
Sandra Bergeron - McAfee Corp
Nick Efstratis - Wasatch Ventures
Rick Friedman - ArrowPath VC
Christopher Lawless - INTEL Corp

Vidient

Brooks McChesney - Vidient
Peter Meekin - Trident Capital
George Hoyem - Blueprint Ventures
Masaru Sakamoto - NEC Corporation



TRIDENT CAPITAL'S SECURITY FOCUS *(cont'd from page 6)*

to the network. Trident investment **Sygate Technologies** is considered a market leader in endpoint security, winning the lead position in the Gartner Magic Quadrant for multiple endpoint security market segments. Another endpoint protection is software anti-tamper technology, which limits the capabilities of a specific piece of software, keeping an attacker from subverting existing software in order to violate policy. Trident security portfolio firm, **Arxan Technologies**, specializes in this groundbreaking security domain, with clientele drawn from military and civilian customer bases alike. Arxan's technology was developed at the CERIAS Institute at Purdue University, an academic center of excellence for information security.

Wireless Security - Wireless networks offer considerable savings and have proliferated throughout many commercial settings. Such networks come with their own challenges, especially security. Wireless security technologies enable enterprises to maintain some control over what systems are able to connect via wireless channels to what networks. As more devices are equipped for wireless access, the need for such security management features will grow. Trident portfolio firm **AirTight Networks** (formerly Wibhu Technologies) has received a great deal of acclaim for its appliance-based wireless security. Its offerings include SpectraGuard, which prevents unauthorized devices from transmitting in an enterprise's airspace, and SpectraPlan, which allows enterprise network management to plan WLAN deployments. Both offerings enable enterprises to gracefully transition from traditional hard-wired networks to more flexible and cost-effective wireless networking while controlling security risks.

Data-centric Protection - *Data-centric Protection* focuses on protecting the data itself vs. the systems and networks on which data resides. Examples include storage security systems, which protect data that is archived in either disk array or tape form. Some also include the growing area of database security in this category.

Homeland Security — Homeland security needs have blurred the lines between information security and physical security. There are three areas of particular interest here, intelligent data mining, intelligent pattern recognition, and the use of robotics in circumstances dangerous for direct human intervention. Intelligent data mining, or information extraction, enables government and private entities to monitor information on networks and other channels, spotting symptoms of impending attacks. Trident portfolio firm **Cymfony** is considered a major player in the area of information extraction technology. The company's core competence in information aggregation and analysis allows Cymfony to address needs in the Homeland Security arena. The firm has also successfully transferred its core technology to a non-technical target market – its initial product offerings provide tools that are used by public relations professionals to track the effectiveness of advertising campaigns.

Once attacks are underway, intelligent pattern recognition can enable prompt reaction, preventing or limiting damage. **Vidient Systems**, one of Trident's 2004 investments, uses sophisticated image processing and interpretation technology, developed at NEC Labs, to pinpoint security-significant activity monitored by CCTV cameras. Vidient's SmartCatch systems are in operational use in several major airports as well as other security-critical commercial and public environments.

In the case when an attack is imminent or underway, intervention by humans may be life-threatening. Using technology to respond without putting humans at risk is of considerable appeal to government and commercial customers alike. We wrap up this discussion of homeland security technology with **iRobot**, Trident's portfolio firm that has made robotics accessible to the general public. Although iRobot's robotic consumer products, (such as the Roomba vacuum cleaner) are familiar to many, the companies Government and Industrial

Robotics Division plays a major role in military and homeland security markets. This division of iRobot focuses on providing robots that can perform tasks that are too "dangerous, dirty, or dull" for humans. iRobot devices have been successful in conducting surveillance inside caves and disarming roadside bombs in Iraq and Afghanistan.

The Road Ahead

As in other technology areas, there are trends that will likely affect security requirements (and associated markets.) The trends we see include:

- Growth in wireless networking
- More security issues associated with embedded devices
- Network protection capabilities moving into infrastructure devices
- More focus on application-layer protection
- A convergence of security management and general enterprise IS management
- Attacks targeting protective technologies themselves

Trident's current portfolio companies both enable current best practices in enterprise security management as well as serve the needs of the future, all while honoring the management objectives of modern businesses. We believe that investing in firms that understand how to strike this balance of cost and protection is a winning strategy. ❖

Becky Bace joined Trident Capital as a Venture Consultant in 2002. An internationally recognized expert in computer system intrusion detection and network security, Becky has over 20 years of experience in software and systems, 15 of those in computer and network security. From 1984-1996, at the National Security Agency she built an intrusion detection research program that earned her a Distinguished Leadership Award. Next, at the Los Alamos National Laboratory, she served as Deputy Security Officer for the Computing Division. In 1998, she started Infidel, Inc., a network security consulting firm serving a variety of commercial customers.

TRIDENT CAPITAL

Trident Capital was founded in 1993 to invest in information and business outsourcing companies. By consistently helping entrepreneurs build industry leading technology and services businesses, Trident has become one of the most successful private equity firms in the country. The firm leverages a partnership that has invested in more than 100 companies and has held senior operating, consulting and investment banking roles at organizations such as AT&T, IBM, Dun & Bradstreet, Morgan Stanley and Bain. To date, Trident has raised six funds and manages \$1.5 billion in committed capital. The firm operates out of offices in Palo Alto, CA and Westport, CT.

Trident invests principally in the following sectors:

- IT Security
- Payments and Transaction Processing
- IT Services and Outsourcing
- Communications/Wireless
- Marketing Services
- Enterprise Software
- Healthcare IT Services
- Product Innovation

Investment Sizes: Up to \$30M

Transaction Types:

- Early Stage Growth Capital
- Expansion Stage Financings
- Management Buyouts
- Spinouts

This newsletter contains trademarks and registered trademarks of Trident Capital, Inc. and other entities.

TRIDENT CAPITAL OFFICES

505 Hamilton Avenue
Suite 200
Palo Alto, CA 94301
Tel: (650) 289-4400
Fax: (650) 289-4444

325 Riverside Avenue
Westport, CT 06880
Tel: (203) 222-4590
Fax: (203) 222-4592

WWW.TRIDENTCAP.COM



TRIDENT
CAPITAL

325 Riverside Avenue
Westport, CT 06880