



SECURITY
INDUSTRY
ASSOCIATION

The Quarterly Supplement from the
Security Industry Association

Research Update

Featuring the *Security Industry Business Confidence Index*

Report for First Quarter 2004

US Security Market Growing at Healthy Pace

The overall US security market is a multi-billion-dollar market and is growing at a healthy double-digit growth rate, according to a new series of research report by Frost & Sullivan. The series includes analysis of the US end user market including commercial, government and residential.

The studies found that the commercial end user market generated revenues of \$14.15 billion in 2002; the government end user market generated \$7.49 billion; and the residential market generated \$1.72 billion.

“In the government and commercial end user security studies, the important finding was that although there were funds allocated for security, not much was being spent. The reason for this was that most government agencies and commercial establishments were analyzing their security infrastructure and investing only where necessary. Of course, this does not include certain areas such as airports, critical infrastructure which had to have a higher level of security,” Julie Paulson of Frost & Sullivan says.

“In the residential end user market study, the economic downturns and upturns drive the market. Healthy residential construction added to some revenue generation, but there has been very high competition and razor thin profit margins. In all the three studies, integration of different security technologies is the trend.”

Among the most surprising findings in the study: There was no sudden spurt in security spending after the events of Sept. 11, 2001. Paulson believes that companies did an analysis of their infrastructure and only spent where necessary. “It took a couple of years before one saw high growth in the market. So security companies should be cautious about what they offer and what they expect from companies. End users have become very knowledgeable about

End User Security Market Growth

2002:

US Commercial End User Market: **\$14.15 Billion**

US Government End User Market: **\$7.49 Billion**

US Residential End User Market: **\$1.72 Billion**

2009:

US Commercial End User Market: **\$29.36 Billion**

US Government End User Market: **\$16 Billion**

US Residential End User Market: **\$3.21 Billion**

Source: The Freedonia Group, Inc.

The biometric sector will realize the most growth, reaching \$550 million in 2007.

security and know exactly what their requirements are. Unless security companies offer something that could add value to the end user's existing security system, it will be hard to penetrate. Large multinationals have entered the market which makes it hard for smaller companies. Unless these smaller companies have a product portfolio that differentiates them from the others, it is hard. Although capital investments for security are being made, security companies have to be very competitive to get a share of the pie,” Paulson concludes.

Commercial End User Market

The end user market is anticipated to reach \$29.36 billion by 2009, with a compound annual growth rate of 10.9 percent. The primary forces driving this market, according to the

Continued on Page 2

In This Report:

- **U.S. Security Market Growth**
- **Smart Labels Expand**
- **Access Control Products Gaining**
- **Confidence Lacking in Information Security**
- **Business Confidence Index**
- **Cyber Attacks**
- **Workplace Violence**
- **Fraud Prevention**
- **Emergency Planning for Disabilities**

Security Industry Association
635 Slaters Lane #110
Alexandria, VA 22314-1177
phone: 703/683-2075
fax: 703/683-2469
E-mail: info@siaonline.org
www.siaonline.org



Part of SecurityGateway.com

US Security Market Growing at Healthy Pace

continued from front cover

study, are decreasing prices and increasing demand for security in the last two years, especially in the utilities and industrial market sectors.

The market is growing the fastest in the food and healthcare and financial market sector because of falling equipment prices and a growing concern about crime.

The industrial end user segment accounts for the largest percentage of revenues with 24.2 percent of the total market, followed by utilities with 23.1 percent and the retail end user with 18.1 percent.

Overall, the study concludes that the US commercial end user security market has a healthy double-digit growth rate. With falling prices, increased technological capabilities, and the terrorist attacks on Sept. 11, 2001, security systems such as CCTV, biometrics, proximity cards, monitoring and surveillance services, etc. have seen a rise in demand.

Government Market

The government market is forecast to reach \$16 billion by 2009. Gainful strides were achieved in the last few years with the introduction of innovative products, a drive towards integration of security systems and the availability of funds.

Some of the other factors contributing to the growth include: the initiatives taken by the Department of Homeland Security; improved technological capabilities, declining prices; and integration of IT and physical security.

Almost every government agency has increased security budgets since 9/11. "Departments that didn't have a high level of security in the past have increased security

by installing new security systems or are evaluating new technologies," Deepak Shetty, senior industry analyst, says. "These upgrades and new installations will result in additional revenues for security system providers."

Residential Market

The residential market is forecast to reach \$3.21 billion by 2009. Revenue growth is expected to be driven by: increasing security consciousness across the United States; decreasing prices making security systems more affordable; increasing technological advances creating technology-upgrade opportunities; and emerging and growing markets such as video surveillance.

In addition, a healthy construction market and growing security awareness have contributed to the spurt in demand. Penetration levels are still low in the residential market, and the need for upgrades after September 11 creates new demand.

"Selling residential security systems has become a tough proposition post 9/11 terrorist attacks," Shetty says. "Consumers, though highly security conscious, are equally cautious about their spending and have cut back large-scale capital investments."

However, Shetty added, "Residential security providers are buoyed by the huge revenue potential of bundled products and integrated systems, though it has increased competition from companies in related arenas."

For more information on these studies contact Julia Paulson at Frost & Sullivan, at (210) 247-3870, or e-mail jpaulson@frost.com. □

Smart Labels Expand, RFID Hot

US demand for smart labels is expected to expand over 14 percent annually through the year 2007, approaching 11 billion units valued at \$460 million, according to a recent study from The Freedonia Group.

By 2012, demand will surpass 30 billion units, worth over \$1.2 billion. Smart labels will penetrate both existing and new labeling applications, ranging from enhancing security and brand building to improving customer service and merchandising efficiency.

According to the study, the best gains will occur in the radio frequency identification (RFID) segment, where market size will nearly triple each year. RFID smart labels have the potential to revolutionize supply chain management and logistics operations across a range of industries.

In the near term the best opportunities will be in the labeling of mail and packages, crates and pallets, airline baggage, library books and military assets.

Continued on Page 3

Smart Labels Expand, RFID Hot

continued from page 2

Basic electronic article surveillance anti-shoplifting labels will also continue to dominate sales into the next decade, based on their established record as a successful crime deterrent and their widespread use in the retail sector. Another factor: the largest retail chains are demanding their vendors embed tracking technology into skeds, pallets and products.

For more information on this study contact Corinne Gangloff at The Freedonia Group at (440) 684-9600 or e-mail pr@freedoniagroup.com. □

US Smart Label Demand (million units)

Item	2002	2007	2012	% Annual Growth	
				07/02	12/07
Smart Label Sales	5510	10700	30400	14.2	23.2
Retail & Distribution	4482	8420	18380	13.4	16.9
Gov. & Institutional	817	1525	5920	13.3	31.2
Services & Other	211	755	6100	29.0	51.9

Source: The Freedonia Group, Inc.

Smart label sales are expected to grow to 30 billion units by 2012, with a value of over \$1.2 billion.

Access Control Products Gaining Momentum, Biometrics Especially Strong

Biometric systems will enjoy especially strong growth in the next few years, reaching \$550 million in 2007, according to a recent study by The Freedonia Group, Inc. Biometric & Electronic Access Control Systems found that the US market for electronic access control products and systems is projected to increase 10 percent per year through 2007 to \$7.3 billion.

Fueling gains will be ongoing preoccupation with upgrading homeland security in the face of security threats.

“As private security industries and markets have restructured and globalized, the competitive dynamics of the business have been altered, most likely irrevocably,” says Edward Hester, analyst for The Freedonia Group. “In particular, financial and technological barriers to entry have been erected, achieving economies of scale and scope has become a consideration in many segments, and niche market opportunities – while still prevalent, especially in higher-technology segments such as biometric-based access controls – are less numerous than historically.

“Access controls, as one of the most technology-intensive and inherently competitive segments of the private security sector, has been and will continue to be impacted by these still-evolving dynamics.”

Along with fingerprint and hand geometry systems, nonintrusive biometric technologies such as facial and voice recognition hold the potential to develop into fairly sizeable markets. Iris scanners hold favorable prospects as well.

Smart card-based access control systems will register nominally rapid growth from an even smaller base than

US Electronic Access Controls Demand (million dollars)

Item	1997	2002	2007	% Annual Growth	
				02/97	07/02
Electronic Access Controls Demand	2443	4540	7325	13.2	10.0
Biometric	28	95	550	27.7	42.1
Card-Based	814	1285	1950	9.6	8.7
Keypad/Combination	396	575	800	7.7	6.8
Software & Other	1039	1700	2825	10.3	10.7

Source: The Freedonia Group, Inc.

The biometric sector will realize the most growth, reaching \$550 million in 2007.

biometrics, but demand will be limited to \$100 million in 2007, due to stiff functional competition from cost-effective alternatives. Most smart card interest still comes from financial and healthcare applications. Also of note: end user advances more often occur outside of the US market.

Overall, most end user markets will register healthy growth in electronic access controls demand through 2007.

For more information on this study contact Corinne Gangloff at The Freedonia Group at (440) 684-9600 or e-mail pr@freedoniagroup.com. □

Chief Security Officers Lack Confidence in Information Security Efforts

A new poll of 520 chief security officers (CSOs) and senior security executives conducted by IDG's CSO magazine found that a majority (52%) of CSOs are only "somewhat confident" that their information security measures are effective, with 12 percent saying they are "not very" or "not at all" confident. Only one-third characterize their security investment as "on plan," with 45 percent playing catch-up and 15 percent falling behind.

"CSOs face a unique challenge in measuring the return on their security investments," Lew McCreary, editor in chief of CSO magazine and editorial director of CXO Media Inc., says. "Organizational confidence comes from weaving security into the business process and culture. The goal should be to create metrics that emphasize that and get away from expectations that nothing bad should ever happen, because that's unrealistic."

Not surprisingly, CSOs who reported being extremely or very confident in their security measures were those with the highest budgets.

Regarding cybercrime, only 22 percent reported no incidents in the past 12 months.

Moreover, security executives continue to consider their own employees and other "trusted insiders" (contractors, consultants, business partners) as posing the greatest cyber security threat to their organizations.

Nearly three-quarters (74 percent) of CSOs report security concerns as the main reason they engage in employee monitoring, followed by legal liabilities (59 percent) and legal compliance (47 percent).

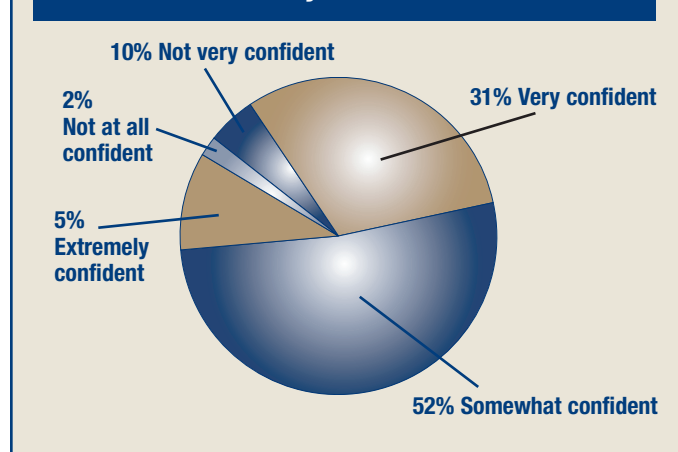
"Security has surpassed performance and productivity as the main impetus for employee monitoring," McCreary added.

Other findings included the top security management priorities for 2004. Among them: training and educating about security policies (70 percent), assessing risks (64 percent) and enforcing existing policy (30 percent).

Only 30 percent listed security the physical workplace as a top priority, and just 17 percent listed increasing security spending/ budgets.

For more information on this study contact Karen Fogerty at CXO Media Inc. at (508) 935-4091, or e-mail fogerty@cxo.com. □

How confident are you that your organization's information security activities are effective?



Source: CSO Magazine

Only 36 percent of respondents are very or extremely confident about their company's information security, while 64 percent are only somewhat confident or less.

What are your organization's top security management priorities for 2004?

Training and educating employees about security policies and procedures	70%
Assessing risks	64%
Assuring business continuity, business resiliency, and disaster recovery	64%
Reducing risks	64%
Enforcing security policy	61%
Aligning security strategy with business goals	53%
Putting security policies in place	47%
Securing the physical workplace/enhancing employee safety	30%
Fostering realistic executive expectations for security success	30%
Measuring return on security investment	26%
Increasing security spending/budgets	17%
Other	6%

Source: CSO Magazine

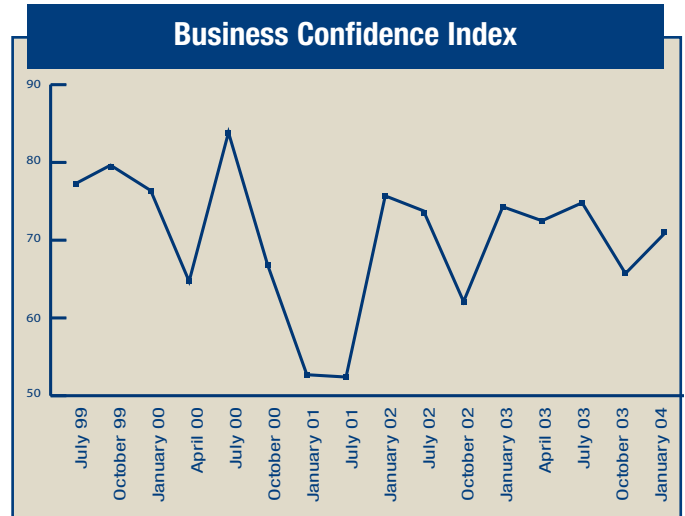
Maintaining existing security procedures is high on the list for 2004, while instituting new measures and budgets is less of a concern.

Business Confidence Index: Bullish Attitude as Spending Increases

The juices are flowing in the security industry. More manufacturers are spending on capital investments and increasing their inventories as they anticipate and book new orders. Almost four in ten (36 percent) say they expect business conditions to be much better in the coming quarter and a surprising 76 percent say they expect to increase their company's aggregate level of capital spending for both plant and equipment over the next twelve months.

The bottom line: as compared to the fourth quarter 2003 and, frankly, the whole last year, executives participating in the Security Industry Business Confidence Index are bullish on business for 2004 and believe it will continue to build as the year progresses. What's most critical – in the long term -- is that these firms intend to spend significantly more on plant and equipment to ramp up production, modernize or shift to newer generation products.

Continued on Page 7



Source: Security Industry Business Confidence Index

A bullish attitude has taken over during the start of 2004 as security industry executives see increased new orders and plan to spend more dollars on plant and equipment this year.

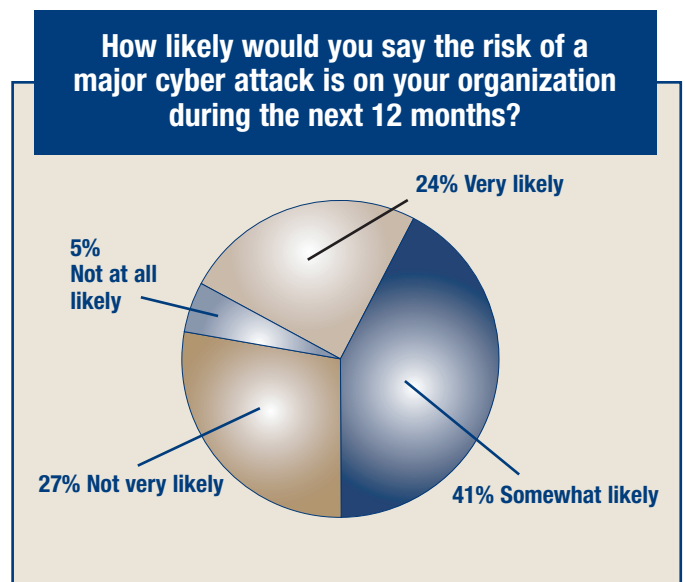
Businesses Feel Prepared for Cyber Attacks, but Challenges Remain

While information security professionals believe their organizations are at risk for major cyber attack, 78 percent say they are prepared to defend against intrusions, according to a new survey by the Business Software Alliance (BSA) and the Information Systems Security Association (ISSA).

The survey of ISSA members also pointed out the information security challenges that remain for businesses and organizations, including employee awareness and employee training.

Among the key findings of the survey:

- Sixty-five percent of information security professionals believe that their organizations are at risk of a major cyber attack.
- Seventy-eight percent say their organization is prepared to defend against a major cyber attack.
- While 55 percent of information security professionals say their companies have active information security awareness and training programs for employees, only 16 percent say their company's workers are adequately trained.
- The majority of organizations (61 percent) now have formal plans in place such as documented business continuity plans and disaster recovery plans.



Source: BSA/ISSA

Sixty-five percent of respondents feel a major cyber attack is likely in the next year.

- Of those plans, specific information security practices include access controls (78%), written information security policy (72%), and regular monitoring, reviewing and auditing (57%).

Continued on Page 6

Businesses Feel Prepared for Cyber Attacks, but Challenges Remain

continued from page 5

• Vulnerability scanners, encrypted e-mail and network intrusion detection systems top the list of new technologies companies plan to deploy in the next 12 months.

“The results of this survey speak volumes about the enormous efforts that the private sector has undertaken to ensure the security of their enterprises,” says Steve

Haydostian, executive vice president of ISSA. “To be sure, we still have a journey ahead of us in the realm of cyber security preparedness, but companies – with executive management approval – are taking action and giving a top priority to the issue of cyber security.”

For more information on this survey contact Diane Smirolodo at (202) 530-5136. □

Which of the following practices is part of your information security program?

Access controls	73%
Written information security policy	72%
Compliance with existing laws and regulations	66%
Creation of organization and process to implement policy	59%
Awareness and training program	58%
Monitoring, reviewing, and auditing	58%
Business continuity planning	57%
Risk assessment and risk management	56%
Life cycle management of products and processes	35%

Source: BSA/ISSA

Access controls and written policies top the list of practices in an information security program.

New technologies either currently deployed or planned within the next 12 months include:

	Currently Deployed	Plan to Deploy
Anti-virus software	99%	1%
Firewalls	97%	1%
E-mail filtering	74%	10%
Intrusion detection systems – network	62%	12%
E-mail attachment blocking	62%	3%
Internet website blocking	59%	5%
Vulnerability scanners – network systems	43%	18%
Encrypted e-mail – Internet	31%	15%

Source: BSA/ISSA

While virtually all companies have anti-virus software, several plan to implement new technologies such as vulnerability scanners, encrypted e-mails and intrusion detection in the next year.

Workplace Violence Cues Not Recognized

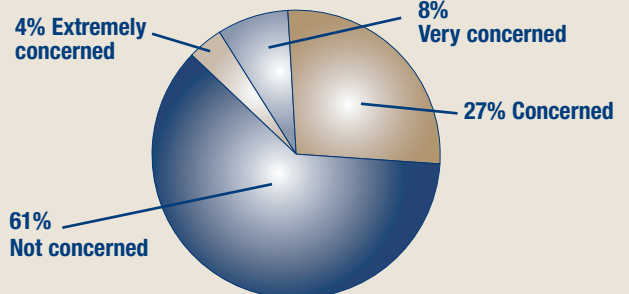
In a recent study of occupational health nurses, nearly 20 percent of respondents reported that they had experienced an episode of workplace violence firsthand, yet the majority did not know what to look for to determine potential offenders.

The study, which was commissioned by the American Association of Occupational Health Nurses (AAOHN), included criteria from the FBI’s National Center for Analysis and Violent Crime.

When given a list of “red flag” behaviors, less than four percent of respondents were able to identify some of the most common warning signs usually seen in potential offenders.

“We were surprised that when asked to identify certain behavioral traits as possible warning signs for acts of workplace violence, most respondents failed to recognize some of the most common signs,” says Susan Randolph, MSN, RN, president of the AAOHN.

Employee Concern



Source: AAOHN

The majority of respondents are not concerned about workplace violence, yet 20 percent have experienced it personally.

These warning signs include: changes in mood, personal hardships, mental health issues, negative behavior, verbal threats and past history of violence.

Continued on Page 7

Workplace Violence Cues Not Recognized

continued from page 6

For example, while 75 percent of respondents identified use of alcohol or drugs as a potential trait, and 71 percent identified expressing anger regularly in the workplace, only one percent identified verbal threats or abuse, or mental illness, and just two percent identified past history of violence.

Many respondents feel that their current work environment is safe from threats of violence. Only 12 percent indicated a level of concern that they would experience an act of workplace violence.

“Employee awareness is an essential way to reduce the risk of violence in the workplace,” Randolph says. “By studying the perceptions and concerns currently prevalent in the workforce, AAOHN found a significant need for more education. We hope that the study will help businesses develop violence prevention education programs so that employees will be able to recognize and report potentially dangerous situations before an incident occurs.”

For more information on this study contact Jennifer McDuffee at (770) 455-7757, ext. 105, or e-mail jmcduffee@aaohn.org. □

Recognizing the Warning Signs

Use of alcohol or drugs	75%
Expressing anger regularly in the workplace	71%
Loud and aggressive nature.....	53%
Quiet, keeps to themselves	30%
Passive in nature	21%
Negative behavior, lying.....	3%
Personal hardships	2%
Past history of violence	2%
Mental illness, bi-polar, depression	1.7%
Verbal threats or abuse.....	1%

Source: AAOHN

While most identified drugs and alcohol use as the top indicator, almost none thought mental illness or verbal threats were an indicator of potential workplace violence.

Business Confidence Index: Bullish Attitude as Spending Increases

continued from page 5

The Index is based on a quarterly telephone survey of 100 top executives at Security Industry Association member companies which manufacturer products or provide security services to end users.

For the first quarter 2004, the Index pushed higher to 71.1 as compared to 66.5 last quarter.

The survey asks executives to rank their expectation in nine areas ranging from number of employees or hours worked to marketing spending and product inventories to new product introductions.

Unlike the previous two quarters, respondents to the Security Industry Business Confidence Index report more positive news, especially in terms of new orders (88 percent say they expect new orders to increase); product sales (80 percent say sales will increase); and number of employees or hours worked (50 percent expect an increase).

As important, 54 percent of respondents expect to increase product inventories over the next three months. In a prolonged period of cost containment, increasing inventories is a good indication that manufacturers expect increased short-term sales.

Specifics of Business Confidence

Current Conditions?	4thQ2003	1stQ2004
<i>Good</i>58%	.76%
<i>Excellent</i>12%	.20%
Specific Conditions to Increase?	4thQ2003	1stQ2004
<i>Product Production</i>53%	.43%
<i>Capital Spending</i>28%	.38%
<i>Inventories</i>5%	.54%
<i>New Product Introductions</i>53%	.43%
<i>Product Sales</i>28%	.38%
<i>New Orders Booked</i>5%	.54%
Next Quarter Conditions?	4thQ2003	1stQ2004
<i>A Little Better</i>76%	.58%
<i>Much Better</i>8%	.36%

Source: Security Industry Business Confidence Index

More careful control of production and a little less emphasis on new products, combined with strong sales and more new orders, add up to more manufacturers saying they see current business as excellent or good.

Fraud Prevention Works

Online fraud is decreasing for merchants that invest in fraud prevention methods, according to the 2003 Merchant Risk Council member survey.

In general, merchants are spending higher rates of revenue on fraud prevention, with 17 percent spending more than 2 percent on fraud prevention this year, versus 13 percent in 2002.

The number of online businesses with fraudulent chargeback rates greater than one percent has reduced to single digit levels, down nearly 50 percent from 2002.

However, international fraud is still a problem. Thirty-eight percent of responding businesses in 2003 stated international fraud to be “out of control” or “a big problem.” That’s down only 3 percent from 2002.

For more information on this study contact Susan Henson of the Merchant Risk Council at (714) 830-5129. □

Need for More Emergency Planning for and by People with Disabilities

In the event of a terrorist attack, natural disaster, or other crisis, only 44 percent of people with disabilities say they know whom to contact about emergency plans for their community, according to a recent Harris Poll. Just 39 percent have made plans to evacuate quickly and safely from their homes. These figures have barely changed from two years ago (40 and 38 percent, respectively), when Harris conducted the same survey following the September 11, 2001 terrorist attacks.

The new survey found improvement, however, in the workplace preparedness of people with disabilities who are employed. Sixty-eight percent now say that plans have been made to quickly and safely evacuate from their jobs, a dramatic increase from 45 percent in 2001.

“With thorough planning, those of us with disabilities will have a good chance of survival with the interruption to our lives minimized. Without it, we are at particular risk in the chaos,” says National Organization on Disability (N.O.D.) President Alan A. Reich.

However, anxiety levels are still high. Forty-three percent of people with disabilities describe themselves as at least “somewhat anxious” about their personal safety, compared to 36 percent of people without disabilities. Thirty-six percent of people with disabilities say they are more concerned about their personal safety than they were before September 11, 2001. Twenty-seven percent of other Americans say they are more concerned about their safety than before the terrorist attacks.

For more information on this study contact Brewster Thackeray of N.O.D. at (202) 955-6327, or e-mail thackeray@nod.org. □

Contributor Acknowledgements

Contributions from Frost & Sullivan, The Freedonia Group, CSO Magazine, Symantec, the Business Software Alliance (BSA) and the Information Systems Security Association (ISSA), AAOHN, the Merchant Risk Council, Harris Interactive. Project management and writing services by Karyn Hodgson (847) 940-0895. E-mail: musikjh@aol.com. □

President:
Joseph Grillo
ASSA ABLOY North America

Immediate Past President:
Allen Fritts, Sr.
Honeywell Fire Systems Group

First Vice President:
John Carter
Biometric Corporation

Second Vice President:
George Fletcher
Secutronix Corporation

Secretary:
Wendy Diddell
Richardson Electronics

Treasurer:
Chris Cage
Brinks Home Security

Directors:
Frank Abram
Panasonic Security & Digital Imaging
Jon Chorey
Fidelity Security Services

Chuck Durant
GE Interlogix
William Gorski
Siemens Building Technologies, Inc.

Hunter Knight
Integrated Command Software, Inc.
Ray Krickmier
Fire-Lite Alarms

Peter Michel
VisionTEK, Inc.

Peter Ribinski
Bosch

Gerald Rooks
X10 PRO

Ron Rothman
Ademco Security Group

Dean Russo
Reed Expositions and Services

Dave Smith
Pelco

Paul Talley
Cascadia Capital

Joseph J. Turek, Jr.
Biometrics 2000 Corporation

Thomas M. Wade
Samsung CCTV

Executive Director / CEO:
Richard Chace

Industry Representatives:
Andrea Ferrando
ALAS

Cecil Hogan
NBFAA

Dick Sampson
CSAA

Ivan Spector
CANASA

Non-Voting V.P.'s:
Charlie Darsch
System Sensor

Lessing E. Gold
Mitchell, Silberberg & Knupp LLP

Sandra Jones
Sandra Jones & Company

Marc Mineau