

# Acredula

**BRICKER & ECKLER LLP**

100 South Third Street  
Columbus, Ohio 43215-4291  
(614) 227-2300  
FAX (614) 227-2390

info@bricker.com  
www.bricker.com  
www.Acredula.com  
www.BoardandExecutive.net

Bricker & Eckler LLP's *Acredula* is available to clients and friends of the firm, and highlights information of particular importance to boards and executives. The information contained in this newsletter is not to be construed as legal advice or opinion.

We invite you to photocopy and distribute this newsletter as you wish. Or, request additional copies from us.

*Acredula is the Latin word for "owl," connoting wisdom. This newsletter is intended as wise counsel for boards and executives.*

## Surviving in the post-Enron environment

This issue completes our series on strategic alliances with a readership survey conducted last summer. The survey confirms the reported trend favoring an increase in alliances over traditional mergers and acquisitions for the future. Based upon the survey, we expect an increase in resource sharing through joint ventures, marketing agreements, outsourcing, franchise and licensing agreements and partnerships rather than traditional acquisitions involving a change in control, particularly as the economy emerges from the recent slowdown, September 11<sup>th</sup> and the fallout from Enron.

A special thanks to Alison Belfrage of Bricker & Eckler LLP who designed the survey and analyzed its results and to Bruce Wimbish, an MBA student at The Ohio State University's Fisher College of Business, who provided research and ideas.

This issue also begins a new series on director and officer liability for oversight with an article on the potential liability of directors and officers for information securities lapses. This article was written with September 11<sup>th</sup> in mind.

Upcoming issues will focus on what both publicly and closely held companies can do

### Editor's Note



**John P. Beavers**  
Partner,  
Bricker & Eckler LLP

to increase the confidence of both investors and creditors in their operations in a post-Enron environment. Our next issue will focus on the importance of independent directors, the meaning of "independence," and the reliance on independent experts and counsel in providing oversight. The following issue will focus on pro-active steps that management and their governing boards can take to give assurance to investors and creditors that transactions have been reviewed with independent oversight where there is a possibility of self dealing and that obligations, both on and off the balance sheet, have been reviewed along with analyses of where the cash will come from to service the debt.

Forward thinking management and boards can take steps to distinguish their companies from the rest of the pack in a post-Enron environment.

# Survey confirms trend toward strategic alliances

**A**credula's readers confirm the reported trend favoring an increase of alliances over traditional merger and acquisition transactions for the future. That was the key finding of our summer 2001 survey about the use of strategic alliances versus traditional mergers and acquisitions.

*Fifty percent of the companies participated in a strategic alliance in the last two years and nearly 70% of those companies indicated the alliance created value for their company.*

Survey respondents included businesses from Ohio, Indiana, Illinois, Michigan, New York, Texas, and Wisconsin, to name a few. The survey was designed to explore the perceptions of business leaders on the outlook of strategic alliances compared to the traditional merger and acquisition market.

The survey confirmed that our readers have seen the traditional mergers and acquisitions as more frequent than alliances in the past:

Mergers and acquisitions more frequent in the past	59.9%
Strategic alliances more frequent in the past	37.1%

However, 61.3% of those surveyed believed there is a slight trend or very much of a trend toward using strategic alliances rather than traditional mergers and acquisitions in the future:

Very much a trend toward strategic alliances	17.2%
Slight trend toward strategic alliances	44.1%
No trend toward strategic alliances	28.4%
Uncertain	10.3%

A similar trend toward using strategic alliances is also evident for respondents within their own industry, with 62.7% indicating a slight to a strong trend. Of those surveyed, 56.7% believed in general that alliances presented a better

opportunity than traditional merger and acquisition transactions for their businesses in the future:

Strategic alliances offer better opportunities	56.7%
Opportunities are about even	28.9%
Mergers and acquisitions offer better opportunities	14.4%

Those surveyed have seen a variety of different types of strategic alliances, the most popular of which is the joint venture:

Joint venture	26.0%
Marketing agreement	17.8%
Outsourcing	17.3%
License and franchise agreements	13.5%
Partnerships	13.5%
Information sharing	8.3%
Sharing intellectual property	4.0%

The survey responses show that outsourcing is the form of alliance that is most likely to increase within the respondents' industries. Outsourcing ranked third with 17.3% in the outlook of those surveyed in general, but ranked second with 21.9% with respect to frequency of expected transactions within their industry.

Fifty percent of the companies participated in a strategic alliance in the last two years, with market growth identified as the most common strategic objective for those alliances, followed by internal consolidation and industry consolidation. Of those companies, nearly 70% indicated the alliance created value for their company. When asked about future plans for their businesses, alliances were the most frequently mentioned:

Strategic alliances	40.0%
Mergers and acquisitions	32.0%
Public offerings	2.4%
No plans for future transactions	15.7%

The results seem to suggest that many companies have experienced successful alliances and may be open to or may consider more than one type of strategic alliance. The survey responses show that 86% of the companies consider strategic alliances a higher priority for success more now than in past years.

*The survey responses show that 86% of the companies consider strategic alliances a higher priority for success more now than in past years.*

In terms of amount of revenues, those who responded identified themselves as representing organizations with revenues of:

\$1+ Billion	16.5%
\$500+ Million	6.3%
\$100+ Million	13.6%
\$10+ Million	32.5%
\$5+ Million	7.8%

When asked to rate on a scale of 1 through 4, with 4 being very important, the most important objectives in pursuing a transaction such as an alliance, merger or acquisition, the mean ratings were:

Market growth and/or geographic expansion	3.39
Competitive strategic positioning	3.34
Industry and environmental changes	3.07
Need for consolidation	2.79
Expanding opportunities for employees	2.72
Research and development, technological innovation	2.63
Increased attractiveness because of globalization	2.31

In conclusion, the survey confirms that businesses across the country have noticed a trend in general and within their own industry toward using strategic alliances rather than traditional mergers and acquisitions. It will be interesting to see how the strategic alliance trend fares in the present business climate. The recent slowdown in the economy, September 11th, and the Enron fallout are all significant factors affecting today's corporate activities. We hope this study will be a valuable resource for business leaders addressing current trends in corporate activity. Lastly, we would like to take this opportunity to thank all of the businesses that completed our survey.

The results of any survey are only as good as the breadth of those surveyed. Those who responded to the survey identified themselves as representing the following industries:

Communications	2.9%
Construction and related industries	4.4%
Distribution and wholesale	4.9%
Financial services	28.4%
Internet and e-commerce	1.5%
Manufacturing	11.8%
Medical services	26.0%
Technology, internet and e-commerce	8.9%
Utilities	2.5%
Other	10.3%

## Collecting email addresses

In an effort to keep our records current, we are updating our Acredula database to include email addresses. To accomplish this task, we will need your assistance. Please email your name, company and email address to [info@acredula.com](mailto:info@acredula.com). Thank you for your help!

# Directors and Officers Face Potential Liability for Information Security Lapses

Mark C. Pomeroy

**T**echnology is rapidly changing the way business is conducted throughout the United States and the world. Many businesses are now exposed to potential risks due to advances in technology, such as attacks on computer systems by hackers. Personal information and other valuable data entrusted to companies may fall prey to malicious hackers who break into vulnerable computer systems and steal or deface such information for their own purposes.

Although many companies have either employed or have begun to employ a wide array of security measures to protect their systems from hacking activities, businesses may nevertheless be held liable for security lapses in the event of an attack by a hacker. Yet, companies may not be the only liable party when hackers have been successful in disrupting a business' computer system. Corporate directors and officers may also be liable because they are legally responsible for the protection of their companies' tangible and intangible assets.

## Attacks by Hackers

The San Francisco-based Computer Security Institute recently released its 2001 Computer Crime and Security Survey, in which 85 percent of the respondents reported breaches of their computer security systems within the past year. Forty percent of the respondents reported that outsiders had breached their security systems during the past year, up from 25 percent the previous year. Seventy percent of the respondents reported that their Internet connections were a frequent point of attack, while 31 percent stated that their internal systems were the target of such attacks. The financial impact of these attacks, reported by 186 of the 538 total respondents, amounted to \$378 million. (The survey is available at [www.gocsi.com](http://www.gocsi.com)).

## Company Liability

Although Congress and many states have enacted a number of laws to combat the spread of computer hacking, many hackers

often lack the financial resources to make an injured party whole. Companies that maintain the computer security systems tend to have deeper pockets and, as a consequence, victims of security breaches are more likely to seek redress from them. However, for many industries, existing law is not clear regarding a company's duty to protect its computer network from third-party threats.



**Mark C. Pomeroy**  
Partner,  
Bricker & Eckler LLP

## 1. Financial Institutions

Recently, federal legislation has clearly stated the responsibilities and duties of certain institutions, such as banks, health care providers, and insurers that store highly sensitive information. The Gramm-Leach-Bliley Act (GLB) is a comprehensive piece of financial privacy legislation imposing a number of new security requirements for financial institutions to:

- Insure the security and confidentiality of customer information;
- Protect against anticipated threats to the security of the information; and
- Protect against unauthorized access to information which could result in substantial customer harm or inconvenience.

Boards of Directors of financial institutions are also required to:

- Approve the institution's written security program; and
- Oversee the development, implementation and maintenance of the financial information security program.

*Corporate directors and officers may be liable for information security lapses because they are legally responsible for the protection of their companies' assets.*

## 2. Health Care Providers and Insurers

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) changes the way health care providers and insurers protect the privacy of a patient's health information. HIPAA contains security procedures to:

- Insure the integrity and confidentiality of the information;
- Protect against any reasonably anticipated threats or hazards to the information's security or integrity and unauthorized use or disclosure of the information; and
- Ensure compliance by officers and employees of applicable entities.

## 3. Other Industries

Due to the lack of regulatory guidance provided to other industries with respect to information security, many companies have implemented security policies, while others have formed alliances and organizations to promote industry wide security standards. Generally, the following eight basic security measures are suggested:

- Undertake network vulnerability assessments and implement appropriate security policies;
- Take steps to prevent unauthorized access to systems;
- Enact administrative controls designed to ensure that security policies are followed;
- Install firewalls to monitor and restrict the flow of information;
- Implement encryption technology;
- Take measures to protect computer systems from inside abuses;
- Continually monitor computer security policies and update them as necessary; and
- Create a disaster recovery plan to minimize damages in the event of a security breach.

While implementing the above measures may exonerate a company or at least mitigate liability in the event of an information security breach, it is important to note that due to the rapidly evolving nature of the Internet, the meaning of adequate security is not static and must be constantly reevaluated.

## Director and Officer Liability

Recently, the fear of breaches in information security has prompted many senior business executives to play a more direct role in setting information security policy, according to George Hulme's September 2001 article in *Information Week*, "Management Takes Notice." While more involvement certainly reflects a desire to minimize the financial losses that result from web site attacks, increased upper management involvement may also suggest a fear of personal liability. Although director and officer liability for hacking attacks is an area of law that has not been directly addressed by the courts, certain standards can be established based on basic director and officer liability principles, director and officer liability established for Y2K problems, and the availability of sophisticated director and officer insurance coverage.

### 1. Duties

A corporation's directors and officers are responsible for making decisions about the activities and operations of the corporation. Their primary responsibilities are the duties of care and loyalty to the corporation and its shareholders. Directors and officers must also protect their company's physical and non-physical assets, guarding their company's information security with the same degree of care that they would use in protecting its physical security. And, while many companies often delegate the responsibility for information assets to the IS department, the responsibility for making the information security decisions still remains in the directors' and officers' hands.

### 2. Y2K Liability

This duty to protect information assets came to the forefront during Y2K, the most recent global threat to corporate data and systems. As the Year 2000 approached, discussions centered around the potential for shareholder derivative suits against directors and officers for Y2K failures. In preparing for Y2K, directors and officers were responsible for ensuring that their computer systems were Year 2000 compliant and for verifying that the companies with whom they interfaced were compliant as well, according to Sara Cook and Kristin Dvorsky's article in the September 1998 Illinois Bar Journal, "D&O Liability and the Year 2000—A Repeat of the 1980s?"

*Despite the fact that insurance companies now offer D & O coverage that specifically addresses Internet liability, many of the nation's largest companies are not prepared to handle Internet risks.*

## Hacker Liability

The information security threat posed by hackers has certain parallels to the Y2K issues faced by directors and officers. However, there are two important differences: (1) the information security threat, unlike Y2K, is already causing actual losses, and (2) the threat is ongoing and will not be resolved by a given date, reports Daniel J. Langin in "Out of the NOC and Into the Boardroom: Director and Officer Responsibility for Information Security," available at [www.recourse.com](http://www.recourse.com). Like the Y2K threat, the risk of losing information assets due to security breaches is "known, or should be known, to all officers and directors by now," said Langin.

Langin further explains that under the fiduciary duty to protect information assets, directors and officers must comply with the "prudent man rule," which requires them to act with the duty of care of an ordinarily prudent person in a like position under the circumstances, and in a manner which is in the best interests of the corporation and its shareholders. The directors and officers of a corporation are bound to use due care and to be diligent with respect to the management and administration of the corporation's affairs. For a breach or neglect of duty in this regard, directors and officers are liable for resulting losses or injuries. Again, directors and officers must take an active role in securing their companies' information systems, Langin stated.

The more recent emergence of sophisticated director and officer liability coverage reveals a growing concern regarding the potential responsibility and liability for information security. Insurance companies are beginning to offer director and officer coverage that specifically addresses Internet liabilities. Despite this offering, reports still reveal that many of the nation's largest companies are not prepared to handle Internet risks.

A survey conducted on behalf of Assurex International, the world's largest privately held commercial insurance brokerage group, revealed that although companies are doing a good job with basic prevention, few U.S. businesses have purchased "einsurance" products to mitigate risks and reduce liability costs after Internet disasters strike. While only 53 percent of the Fortune 500 companies and associations surveyed reported owning director and officer insurance, the development of this type of einsurance product reflects a growing desire among companies to protect their directors and officers. (More information on the survey is available at [www.epolicyinstitute.com](http://www.epolicyinstitute.com)).

Under their fiduciary duties, directors and officers are required to respond to known and reasonably anticipated threats to their company's physical and non-physical assets. At one time, companies considered their buildings, inventories, equipment, and vehicles to be their most valuable assets. Today, however, intellectual property, technical services, and other non-physical corporate assets are considered the most valuable assets.

"Companies must recognize and protect their critical resources, not only for their own sake, but also for the sake of their customers, shareholders, partners, even the general public," said Frank Huerta, president and CEO of Recourse Technologies, in a July 2001 news release available at [www.recourse.com](http://www.recourse.com). While the fiduciary duty permits directors and officers to seek insight and advice from IS experts, directors and officers must take deliberate action with respect to their company's stance on information security. In accordance with the prudent man rule, directors and officers must lead the way in selecting products and services that will protect both their companies' information assets and their own personal assets.

### Counsel for BOARDS AND EXECUTIVES

*A Bricker & Eckler Initiative*

John P. Beavers, Chair  
(614) 227-2361  
[jbeavers@bricker.com](mailto:jbeavers@bricker.com)

Thomas R. Brownlee, Jr.  
(614) 227-2301  
[bbrownlee@bricker.com](mailto:bbrownlee@bricker.com)

Jerry O. Allen  
(614) 227-8834  
[jallen@bricker.com](mailto:jallen@bricker.com)

John W. Cook, III  
(614) 227-2383  
[jcook@bricker.com](mailto:jcook@bricker.com)

Michael K. Gire  
(614) 227-2318  
[mgire@bricker.com](mailto:mgire@bricker.com)

Gordon F. Litt  
(614) 227-2305  
[glitt@bricker.com](mailto:glitt@bricker.com)

Richard D. Rogovin  
(614) 227-2352  
[rrogovin@bricker.com](mailto:rrogovin@bricker.com)

Betsy A. Swift  
(614) 227-8850  
[bswift@bricker.com](mailto:bswift@bricker.com)

Laurie A. Briggs  
(614) 227-2355  
[lbriggs@bricker.com](mailto:lbriggs@bricker.com)

Michael E. Flowers  
(614) 227-2340  
[mflowers@bricker.com](mailto:mflowers@bricker.com)

Steven R. Kerber  
(614) 227-2356  
[skerber@bricker.com](mailto:skerber@bricker.com)

Mark C. Pomeroy  
(614) 227-2326  
[mpomeroy@bricker.com](mailto:mpomeroy@bricker.com)

David C. Spialter  
(614) 227-2342  
[dspialter@bricker.com](mailto:dspialter@bricker.com)

Faith M. Williams  
(614) 227-2374  
[fwilliams@bricker.com](mailto:fwilliams@bricker.com)

Alex M. Brown  
(614) 227-2344  
[abrown@bricker.com](mailto:abrown@bricker.com)

James F. Flynn  
(614) 227-8855  
[jflynn@bricker.com](mailto:jflynn@bricker.com)

Quintin F. Lindsmith  
(614) 227-8802  
[qlindsmith@bricker.com](mailto:qlindsmith@bricker.com)

Christine M. Poth  
(614) 227-2395  
[cpoth@bricker.com](mailto:cpoth@bricker.com)

Michael F. Sullivan  
(614) 227-2337  
[msullivan@bricker.com](mailto:msullivan@bricker.com)

Randolph C. Wiseman  
(614) 227-2310  
[rwiseman@bricker.com](mailto:rwiseman@bricker.com)