Virtue In a Virtual World:
Cyber Ethics and the New Global Economy
Remarks for the Ethical Leadership Forum 2000
Hong Kong, March 30, 2000

By:
Robert H. Dunn
President & CEO
Business for Social Responsibility

Good morning.

It is a pleasure and an honor to be here for such an important gathering of business leaders.

I’d like to start this conversation in an interactive way, since that’s the direction much of information technology is going.

It would be interesting for me to learn something from you about the information technology you make use of in your business or organization, and in your personal lives.

How many of you use a computer at work?

At home?

How many of you have purchased something online?

Now I’d like to ask you another question:

How many of you work for a technology company?
If you didn’t raise your hand, I would encourage you to reconsider how you think about your business. The reason I believe my topic this morning is
relevant for each of you is because increasingly, all of us are working for technology companies. Some are producing hardware or software. Others market through the Internet. But the rest of us, whatever products or services we may be offering, need to think of ourselves as technology companies too.

It has always been my experience that stories are a useful way to stimulate new thinking. I want to share three brief stories because they illustrate three cyber ethics challenges I want to discuss in these remarks.

**Story #1**
Recently a teenager in Russia found a way to hack into -- or access -- the database of a large U.S.-based company that sells compact disks online. He or she stole several hundred thousand credit card numbers, then tried to blackmail the company. When those efforts were unsuccessful, the hacker released the numbers on the Internet, forcing major credit card companies to replace tens of thousands of cards for customers who had used the site.

The hacker’s actions were clearly wrong and criminal -- but how should we view the compact disc company and its failure to safeguard the personal information of its customers? And what is the ultimate price it will pay for its mistakes?

**Story #2**
One of the largest financial services companies in the world recently found itself in the embarrassing position of learning that one of its own vice presidents had posted hundreds of negative Internet messages about a tiny competitor. These messages were anonymous, and included personal attacks on the integrity of the competing company’s founder. The small competitor traced the messages back to the vice president, and is now suing the financial services company. In this case, offensive behavior by a single employee, a vice president, did serious damage to one of the world’s best known brands and financial institutions. Could this have been prevented?

**Story #3**
The Financial Times and USA Today recently reported that for a small fee, you or I can go onto the Internet, enter someone’s name, and learn the following information about that person: personal identification numbers; address and phone numbers; height, weight, and eye color; a list of the property they own; traffic tickets; the companies the person is involved with; their bank balances and debts; even the names of neighbors, and their addresses and phone numbers.
In one case a journalist searched her own name and learned the size of her mortgage, her favorite color, and the number of times she had visited the White House. If a journalist can do this kind of cyber-search on herself, someone else can do it on you.

Imagine a business adversary, an insurance company, or a company considering an acquisition or merger having access to all this information -- and more -- about you and your business colleagues. Is this appropriate or wrong? Could this have an impact on your success or your competitive position with customers?

I hope these three stories help make the point that issues of cyber ethics are not just of marginal importance, nor can they be left to your Information Technology staff.

Cyber ethics failures can lead to huge financial losses and serious damage to reputation, not only for companies but for government agencies and non-profit organizations. In truth, all the institutions within our society.

If you participate in today’s economy, you proceed with great peril if you do not have a comprehensive ethics policy, and one that is designed specifically to meet the new challenges presented by cyber ethics.

Because ethics is a term that is often misunderstood, I would like to talk briefly about the definition I am using, and then explain how I would encourage you to think about cyber ethics.

BUSINESS ETHICS

As you well know, people hold different ethical values within individual cultures and countries. There are important differences as well amongst the many cultures and countries of our more-and-more connected global economy. However, despite all of these differences, there are some basic ethical values about which there is virtually universal agreement.

These ethical values include:

- Honesty
- Integrity
- Promise keeping
- Fairness, and
- Respect for others
Business ethics involves the use of these kinds of values in determining our moral duties and obligations to others when we are engaged in doing commerce.

Business ethics also involves applying these values utilizing processes that are fair and that produce outcomes which have integrity. Often this involves reconciling competing ethical claims and finding ways to act that minimize ethical harm.

The application of business ethics principles to the use of new information technologies is called cyber ethics. Cyber ethics sometimes present us with brand new ethical challenges. In other cases, they simply translate existing challenges into a new realm. How do cyber ethics differ from traditional business ethics? I would identify four important ways.

First: cyber ethics operates in a virtual realm – a world made up of electrons and images, rather than bricks and mortar or geographical community. Thus, it involves people interacting without direct personal contact. This can result in ethical misbehavior that wouldn’t happen in other contexts.

For example: many individuals who would never vandalize a store or business are more than willing to perform an equivalent act in cyberspace. Hackers -- who break into and alter company or government websites – generally do not see themselves as having done something wrong. In fact, they often see themselves as heroes.

Second: cyber ethics is driven by new information technologies. Most especially the Internet, but also by new forms of wireless technology, software, and even remote surveillance. These technologies have brought about a dramatic reduction in transaction costs for gathering, storing, and communicating information about individuals or companies.

- The Internet portal Yahoo gathers 400 billion – or in English usage, 400 thousand million -- bytes of information a day, which is equivalent to a library of 800,000 volumes.
- According to data from Elliot Maxwell of the U.S. Department of Commerce, new database technologies have reduced the cost of storing a unit of information 100 million times since 1950.
- Similarly, fiber optic technology has reduced the cost of sending a unit of information over long distances by about the same amount.

These changes, of course, represent both an ethical opportunity and an ethical threat.
Third: cyber ethics operate at the speed of the Internet, that is, in a greatly accelerated time frame. This can cheat people of the opportunity for the careful deliberation and reflection necessary for ethical decision making. It is hard to imagine how managers and employees can make decisions at the speed of the Internet if they do not have a clear underlying ethical framework to guide them.

Fourth: cyber ethics are global ethics. Information now flows across the Internet to every part of the globe instantaneously. The usual face-to-face interaction between two people with similar values, cultures, laws and customs may now involve two strangers who have never met, have little in common, and may never interact again.

For this reason, global companies must work toward integrating their ethical practices across virtually every culture, county, and legal system in the world. As the transnational nature of Internet technology accelerates, it will be less and less possible for companies to have different ethical standards and practices in different countries -- or different practices in cyberspace -- than they do in the brick-and-mortar world.

Because the virtual world has the distinct characteristics I've described, cyber ethics sometimes involves addressing ethical issues that are altogether new. In many instances, however, cyber ethics involves traditional ethical issues that present themselves in new ways because of Internet technology.

Let me illustrate this point with another story.

The largest Internet advertising company in the United States has ad banners on more than 1,000 websites. On those banners the company places what are called cookies, tiny coded files that attach to a web user’s computer and then track all the sites the user visits on the Internet. Using this technology, the company created a database of more than 100 million individual files -- then combined that information with names, addresses, and other data it obtained by purchasing a large market research firm. By putting these two databases together, the company was able to create individual online profiles of more than 90 percent of American households, making it possible to target these households with customized advertisements.

If you’re wondering why this raises serious ethical questions, let me provide you with one bit of additional information.
The company did not tell consumers it was gathering data on them. Nor did it obtain permission to use this data. To make matters worse, it had a privacy policy posted on its site that said it would not engage in these practices.

The company has paid a heavy price in breaching the trust of its customers. It is also under investigation by federal and state agencies and has been the target of numerous lawsuits. It has suffered severe and continuing damage to its reputation, and a steep drop in its share price.

Making false or misleading statements is not a new business ethics issue. Nor is wrestling with the boundaries of customer privacy.

CUSTOMERS FEAR MISUSE OF PERSONAL INFORMATION

A range of studies shows that the most important reason potential customers do not make purchases over the Internet is that they are afraid companies will misuse their personally identifiable information (PII). One study found that 70 percent of U.S. consumers are uncomfortable with giving online companies their PII.

Customers are looking for a trusted transaction. In privacy terms, this means doing business with companies that:
- Only collect as much information as is needed for a transaction
- Tell their customers how that information will be used
- Give customers a choice as to how the information is used
- Make sure the information is secure from theft or misuse
- Provide some means for customers to access and verify information about them
- Provide redress, a means of enforcing the above principles

This “privacy mantra” can be summarized as notice, choice, security, access, and redress.

CYBER-CONSUMER PRIVACY IN A GLOBAL CONTEXT

If the Information Economy is to continue to expand and flow easily across borders, we will clearly need to forge a global consensus on some basic rules for how to protect consumer privacy in cyberspace.
In the United States, the approach to date has largely been to allow business to regulate itself.

The European approach is quite different.

The European Privacy Directive, passed in 1998, requires companies to tell consumers when they are collecting data, and how they plan to use it. It lets consumers see and make changes to their data profiles, and it allows individual consumers to opt out of data collecting mechanisms.

The Directive also makes it unlawful for companies to transmit personal information about EU citizens to countries whose privacy laws do not meet European standards. At the moment, if you were to go to Germany, enter a customer’s address in your handheld electronic datebook – mine happens to be a Palm Pilot -- and then return to Hong Kong, you may have violated European law.

The two sides appear finally to have developed a consensus that companies on both sides of the Atlantic should inform consumers of what information they are collecting, how they will use it, and allow consumers to “opt-out” if they choose.

EMPLOYEE PRIVACY

Privacy is a cyber ethics issue not only for customers, but for employees as well. With workplace access to the Internet and emails, many companies are struggling to craft a proper policy for employee use of technology.

Last year a major computer company terminated more than 300 people, and a large office equipment company about 40 employees, for improper use of the Internet. This included activities such as sending racist, sexist, or threatening emails; viewing pornography, gambling, or selling goods online; even running a side business online.

Employee use of computers is not only about what’s appropriate or personal. It can also impact a company’s proprietary information, since the Internet makes it so easy for employees to share legitimate company secrets. A disgruntled employee no longer has to smuggle hard copy documents out of a building to pass along private information to the press, or even to a rival company. All it takes is the click of a mouse.
The ethical challenge here for companies is to develop policy that respects an appropriate zone of employee privacy covering legitimate personal needs, while also respecting the rights and responsibilities of an employer to protect its business and legal interests.

OTHER ISSUES

It’s impossible to be comprehensive in a short speech; however, I would like to mention briefly a few other major challenges that have emerged around cyber ethics.

You may have heard of the Digital Divide. Essentially this describes the growing gap between a new group of haves and have nots.

Arguably the single most compelling ethical question in this field is how we can shape the Information Economy in ways that do not exclude a vast number of people who we want to have as participants. Whether these people are poor, uneducated, living in remote areas, or disabled, we must find ways to allow them to become active consumers – even producers – of information, goods, and services.

Another key cyber ethics issue relates to the environment. People often assume that information technology is clean, compared to smokestack industries such as auto making. In fact, the chip making process uses large amounts of toxic chemicals, the short shelf life of computers has led to enormous challenges with disposition and recycling, and tons of software packaging goes straight into landfills every day. Those of us who use and benefit from the new technology must help find ways to harness its benefits without degrading the quality of life available to future generations.

Employee health issues are also important. Working at a computer all day can cause employees to develop eye, wrist, and back problems, and serious questions remain about whether daily exposure to monitors may cause still other, serious health problems.

Intellectual property issues arise with regard to replicating software, and public policy questions arise regarding whether and how to tax e-commerce transactions.

Finally, there are significant ethical issues around the vast amount of unauthorized information that may become available to you electronically. What if you found a competitor’s marketing plans for the next quarter posted –
unethically, and possibly illegally -- on the Internet? Would your managers know what you would expect of them in such a circumstance?

Your companies will likely face all these issues, and others as well.

So what does a cyber ethical company look like? It probably has at least these fundamental characteristics:

- A strong statement of company values, an ethical framework applied to all business decisions, and an explicit acknowledgement that all aspects of business operations, including ethical values, apply in cyberspace.
- An ethics-based code of conduct that goes beyond legal compliance, and gives specific guidance on cyber ethics challenges.
- High visibility support for the ethics program on the part of senior managers.
- Effective, ongoing communications and training that address the special ethical challenges of operating in cyberspace.
- Helping resources to support employees in making good and timely decisions.
- Clear rewards and sanctions that hold people accountable, and
- Some system of stakeholder engagement to ensure that you are adequately addressing and balancing the ethical concerns of all those impacted by your decisions.

Finally, cyber ethical companies should explore ways they can harness new information technologies to promote ethical behavior – not simply to build a firewall against the risks that technology creates. And, they should ensure that their policies and practices lead to socially and environmentally responsible uses of the new information technology.

It is my strong belief that having a comprehensive business framework for decision making that addresses these ethical issues has already become a business requirement, not an option.

Companies that behave ethically in cyber space, and act in a trustworthy way, will create enduring relationships with their customers, investors, employees, business partners, and communities. These will be the companies that survive and prosper.

Two thousand years ago Asia gave the world a precious gift – paper. This new technology allowed for easy storage and transmission of data, and led to the creation of the first global Information Economy. Paper not only changed
the world, it helped invent it, making civilization and commerce – the world as we know it today -- possible.

Two thousand years later, we are in Hong Kong brought together by the birth of a new Information Economy.

I hope all of us here today can work together so that two thousand years from now, when people look back and study how we conducted business in this century, they will honor us for creating a legacy that makes the world a better place. A legacy of ethical behavior that makes all of us more successful, and contributes to the well being of all society’s members.

Thank you.

These remarks were prepared in collaboration with Steve Voien, Manager in BSR’s Global Business Responsibility Resource Center.

Further information about cyber ethics and other issues of corporate social responsibility are available on-line at www.bsr.org/resourcecenter