Chapter 4

AVOIDING LEGAL ISSUES

4.1 Global Contracts

4.1.1 Legal Preface

Due to the uncertain state of a global legal framework for the Internet, the information in this chapter should be not construed as legal advice or opinion on any specific facts or circumstances. There is a lot of movement on regulations regarding the Internet, both on a national and international basis; therefore, you are advised to contact a qualified lawyer for specific advice. The contents are intended for general information purposes only and will most likely change.

4.1.2 Doing Business over the Internet

The Internet drove the trend to global business and global business enforced the trend towards e-business. But the greatest obstacle to truly global e-business is the myriad legal restrictions. Italy, for example, bans online auctions that sell used goods. In Singapore, it's illegal to post ads for Viagra. Germany bars retailers from offering unlimited guarantees. China does not allow sites to carry telephone traffic over an IP network, so a company with a call center as a part of its Web could be locked out of doing business in China. And so on. Many other laws are in place, which are not compatible with globalized companies.

Paper contracts, for example, are not the ideal document form in the global village. I found out myself the hard way. I got the contract for this book from Prentice Hall and had to sign it and send it on to Hewlett-Packard Press. Unfortunately, HP Press moved on the day I sent out the contract, so it never got to the destination. I waited for two weeks and sent out a new set of contracts to HP Press. The day the new contracts arrived at HP Press, the old ones arrived there as well. You can imagine that this is not how it should have happened. And believe it or not, the same happened to the contract of the second edition. I sent it out and it got lost again.

Disputes on the Internet in an online shopping scenario often occur because of one of the following reasons:

- The customer pays, but the merchant does not deliver.
- The customer pays, but the merchant delivers the wrong goods, the wrong quantity or broken goods.
- The customers pays, but the money does not arrive at the merchant.
- The merchant delivers, but the customer refuses to pay.
- The merchant delivers, but the customer has not ordered anything.

Table 4.1. Legal Disputes on the Internet

Although all information regarding the book was transmitted electronically from southern Germany to northern California, the contract could not be signed electronically. It was technically possible to sign the document electronically, but legally there was no way at the time that such a signature could be validated and authenticated, in the event of a problem.

As the Internet is available worldwide, business does not stop at national borders. An online offering in a Web store can be seen from any country, and usually, anybody is able to buy the goods. If everything goes well, nobody has to bother about laws and regulations. But what needs to be done if something goes wrong? If we look at our simple example of the Web store, we can identify several possible issues between a merchant and a customer in this e-commerce online shopping scenario, which you can find in Table 4.1.

These are the most common issues between buyer and seller. In order to resolve them, laws are in place to support both the buyer and the seller. The problem that arises with the Internet is that, unlike in a local shop, the buyer and the seller may be in two different countries, and the Web server could be in a third country.

The important thing for the courts to decide is *where* the business transaction has taken place. Laws are enforced depending on the country where the transaction has taken place. In most cases, the country in which the Web server is placed is not taken into consideration. (It is not always clear where a server is located.) The top-level domains (TLDs)—such as .de, .uk or .com—can be bought by anyone who is willing to spend money. There are no legal restric-

tions on where such a TLD can or cannot be used. What counts is the country where the *seller* is located.

In many countries, casinos need to follow special regulations to open and conduct business. The same applies to online casinos, so many entrepreneurs have decided to move their business venture to a country where gambling is allowed with little regulation. Many Caribbean countries have an excellent connection to the Internet, and many online casinos are hosted there. Just putting the Web server there is not enough, however, in order to make this a legal offering for American entrepreneurs. An American company needs to establish a subsidiary in the Caribbean in order to legally pursue this venture. The same applies to many other countries. Some countries in Europe, for example, have high taxes on gambling; the casinos have to pay more than 90 percent of their income to the state. Moving the digital business to another country may help them circumvent these tax issues.

The European Union published some guidelines for online business in May 2000 that need to be implemented in national law by the end of 2001 (see Table 4.2). These guidelines ensure that at least within the European Union, a common legal framework is in place.

The following summarizes the guidelines of the European Union on E-Business.

- **Terms and Conditions**—Terms and Conditions must be presented before anything can be bought over the Internet.
- **Equalization**—Electronic contracts are now equal to paper contracts. Together with the guidelines on the digital signature, digital contracts can be used in court.
- **Establishment**—The location where a company is established is independent of the location of the web server.
- **Single Market**—The dealer can sell in the whole of the EU, if this is in line with the laws and regulations of the country where the dealer is established.

Table 4.2. EU guidelines for E-Business

These guidelines enhance already existing guidelines for the electronic signature and telesales. Further projects are already in progress to unite national laws and simplifying the use of intellectual property. This will make cross-

border business easier for all parties involved. By harmonizing laws and taxes cross-border business becomes more transparent to the businesses and to the customers.

4.1.3 Jurisdiction on the Internet

As the Internet creates a global village without global laws, jurisdiction on the Internet is a very important topic. When business is done over the Internet, it is important to know if it is covered by the jurisdictions of other countries. The concept of *extra territoriality* is critical for any type of business on the Web.

If the electronic business is located in France and the customers are in Italy and Spain, it is necessary to know which jurisdictions are in control. In the real world, there are many regulations that support customers by making the laws of their countries take precedence.

Most businesses in the real world have terms and conditions that fit the country the customers and the business are in. On the Internet, customers from all over the world are suddenly able to deal with a particular company. The electronic business needs to create online terms and conditions that will comply with the laws of every country.

Putting up a Web page and starting an online business without any limitations regarding terms and conditions will most probably infringe on the laws in most countries around the world. As there is no way to restrict a Web page to a certain country, a global solution is required. Global terms and conditions may not be available; therefore, it is necessary to look into all countries where you expect to do business.

For all other countries, it is important to draw the attention of a customer to the terms and conditions of your country of origin, including information on how to enter a contract or reject it and which law will be applied in the event of a dispute. This text should be presented on the home page and a link should be provided from each Web page on the site.

In August 1999, Amazon.com was accused by the Simon Wiesenthal Center[1] of selling banned books in Germany. In Germany, Adolf Hitler's *Mein Kampf* and other hateful literature is banned by law. While Amazon.com offers these books on its Web site, its German subsidiary Amazon.de does not. Other online booksellers, such as Barnes & Noble,[2] also offer these books on their Web sites, which is a problem for German law. Although these companies are based in the United States, they are suddenly liable in Germany.

Amazon.com is of the opinion that international customers who order books at their site are treated like tourists who are responsible for the import of books into their country. Amazon.com has no program or person looking into each sale to check if the book is banned in the buyer's country. But Amazon.com is risking the loss of the German market. Amazon.com is exposed to German laws

[1] http://www.wiesenthal.com/
[2] http://www.barnesandnoble.com/

because it has a German subsidiary. It is not clear who is violating the law—Amazon.com for offering the book to German customers, DHL for delivering it to Germany, or the German customer for ordering it.

4.2 The Web Site

4.2.1 The Domain Name Battle

Once a company decides to conduct electronic business, it needs to register a domain name. This translates the numeric IP address into a more friendly form of text. Instead of typing a series of numbers, most people prefer to type meaningful words, such as www.wired.com, which is much easier to remember and less error prone. Registering a domain name is not difficult, but getting one that fits your business name, logo, or trademark can be difficult.

On the Internet, every domain name needs to be unique to avoid communication errors. But they are assigned on a first-come, first-served basis, meaning that *anybody* can register the domain name that you would like to use for your company or product.

Internet domain names are composed of two distinct elements: the TLD, and the second-level domain (SLD). The TLD contains information on the origin of the Web site, such as .it for Italy, .jp for Japan, and .za for South Africa. The SLD completes the domain name by adding a company name, trademark, acronym, abbreviation, noun, or any other word to the TLD.

The problem with domain names is that they are not trademarks. Anyone can register a domain name for an already-established trademark, and many people have registered domain names with trademarks, without any relationship to the trademark owners. In some cases people have been using the trademark without knowing about the trademark, and in most of these cases, a court battle was not necessary. One example is altavista.com. A small company called Altavista Technologies used to own the trademark to represent its company. A company named Digital[3] started to offer a highly successful search engine with the name Altavista, but as the domain name was already registered, Digital used altavista.digital.com for the search engine. In 1998, shortly after Compaq acquired Digital, it paid more than three million dollars to the owners of the altavista.com domain in order to expand its search engine business.

Other companies buy domain names with trademarks in order to sell them to their rightful owners. Prices for these registered domains have ranged from a few hundred dollars to a few million dollars, compared to the approximately one hundred dollar biyearly fee paid for purchasing a domain name in the first place. At the time, there was no court interested in a legal battle over domain names, so it was quite easy for these companies to get the money they were requesting.

[3] http://www.digital.com/

In order to prevent domain name issues, you should consider the following steps:

1. **Check for existing trademarks**—Conduct a trademark search prior to applying for a domain name to determine whether the proposed domain name would infringe on an existing trademark used in connection with goods or services similar to those that you propose to offer.
2. **Check for famous marks**—A name or trademark that is famous can't be used in any other product or service. Offering "Coca-Cola translations" would be a violation of this law.
3. **Register trademark**—In order to make sure that your domain name is secured, register the domain name as a trademark and start using the domain name at the same time.
4. **Check foreign countries**—Register the trademark and the domain name in all countries that are relevant to your business now and in the future.

Table 4.3. Preventing Domain Name Issues

The domain name for MTV,[4] for example, was acquired by a former employee of the company at a time when MTV had no plans to go online, and it even supported the use of MTV.com by the employee. Soon after, the company wanted to go online and was not able to use the domain name. Hasbro[5] attempted to register the domain name "candyland.com" for use in connection with its popular children's game, but the name had already been registered by a company to identify a sexually explicit adult Web site. In the early years, there was no way to get these domain names back.

But since then, things have changed. An individual who had registered panavision.com had to hand over the domain name to Panavision,[6] because the defendant was violating the U.S. Federal Trademark Dilution Act. Many similar cases have happened in the U.S. and all over the world. Although a domain name is still not a trademark, it has become much easier for trademark

[4] http://www.mtv.com/
[5] http://www.hasbro.com/
[6] http://www.panavision.com/

owners to reregister the domain names that contain their trademark names. See Table 4.3 for a short introduction to acquiring domain names.

New regulations for the registration of domain names have also helped resolve court battles. Depending on what has been registered first, the priority will be given to the owner. If a trademark, such as Panavision, has been registered before the domain name, the trademark owner will also be granted the domain name. On the other hand, if the trademark has been established after the domain name has been registered, as in the case of Altavista, the owner of the trademark has no rights to obtain the domain name.

In May 2000, a discussion on generic-terms domains began and another judge in Hamburg decided that it was unfair to use generic terms in domain names. The judge decided that a generic term would provide an unfair advantage over the competition.

In order to prevent legal issues for your company, check both the availability of domain names and registered trademarks before applying for your domain name. If you want to be on the safe side, register the trademark if you have a domain name, and vice versa.

Besides the legal issues on a particular domain name, it often happens that unhappy customers of a particular Web site get a domain name that puts a negative light on the company. Chase Manhattan Bank, for example, preemptively bought the domains Chasesucks.com, IhateChase.com, and ChaseStinks.com, while Walker Digital, a company founded by Priceline.com chief executive Jay Walker, registered Priceline-sucks.com and Pricelinesucks.com, to prevent customers from using these domains to express their views on these companies.

It is not possible to ban people from using these domains, especially in the United States, where citizens are protected under the laws of free speech. It is also not possible to register all domains that contain a certain keyword; therefore, randomly buying domain names is not very effective and only costs money. The better way is to understand the needs of your customers and try to resolve their issues. There will always be some customers who are never satisfied.

4.2.2 Linking and Framing Issues

The hypertext format allows the interlinking of documents on the Web. The links are not restricted to a particular part of the Web. Any Web page can be linked to any other Web page without restrictions. Links are provided as a service to other information resources with similar content or as a means to link advertising into a Web page.

As there are no legal restrictions for the Web, everybody is interlinking with other sites, and this is common practice. The problem arises as soon as links are used to pretend to provide pieces of information that have been created by others. It is very simple to create a news service by providing headlines to the latest news on other servers. People will come to your site because you have the latest news headlines, but all you did was provide links to the work of others.

Although there are no rules regarding linking, over the past few years it has become clear that so-called *deep linking* (i.e., direct linking of a particular Web page) is considered pirating a Web site if done in large scale. But providing a single link to a particular document is no problem.

In 1997, Microsoft was sued by Ticketmaster[7] because it was providing direct links to the ticket sales portion on the Web site. Through the direct link, it was bypassing the Ticketmaster home page, its associated advertising, and the disclaimer. Many customers were not aware that they were moving on to another site and to another company. Hewlett-Packard also links to other companies from its home page,[8] but displays a disclaimer before leaving the Hewlett-Packard home page. This ensures that the customers understand that they are leaving a certain site and that the owner of that particular site is not responsible for the content, services, or products of the sites that are outside of its realm.

Many others should have used this same technique to prevent damage to its image. The ministry for family affairs in Germany[9] should have provided information when visitors left its page. The opposition in Germany started a campaign against the government, because it was possible to get from the home page of the ministry "directly" to a pornographic home page. By clicking only six times, a visitor could get from the ministry's home page to the pornographic home page. What was not mentioned on the site was that the home page of the ministry linked to a Web directory, which in return linked to some other sites before getting to the undesired home page. This created some hysteria in Germany. By providing a short text making clear that by pressing the link, the user leaves the home page, this ambiguity would not have occurred.

Framing is considered to be an even worse problem. Frames have been invented to partition a Web page into several parts that can be loaded individually. With frames, it is possible to separate the navigation bar from the content. It also makes it easy to place a different banner ad every 30 seconds on the screen without the need to reload the complete window. Although the idea itself is not bad, frames create more problems than they are able to resolve. With frames, it is also very easy to create a navigational bar with your company logo and then link to other sites. As people see your logo, they will think that the document in the other frame is also part of the site. Web site owners will object in most cases if they find their content being framed at another site, particularly if their content is surrounded by paid banner advertising.

Some students in Germany tried to circumvent paid advertising on the *Spiegel* homepage.[10] The site consists of three frames: the upper frame contains advertising, the left frame is used for navigational purposes, and the lower right frame contains the content. The students created a no-advertising

[7] http://www.ticketmaster.com/
[8] http://www.hp.com/
[9] http://www.bmfsfj.de/
[10] http://www.spiegel.de/

Spiegel Web page that allowed anyone to navigate through the *Spiegel* site without looking at the advertising. This reduced download times and increased the number of visits to the Web site. The *Spiegel* advocates brought this case to court and tried to remove the other site from cyberspace, which eventually was ordered by the court, as *Spiegel* was losing money on banner advertising. In order to prevent "attacks" from other sites, a small JavaScript now checks if the site is being framed or if frames are missing, and resets the browser windows to the original URL of the *Spiegel* company.

Fortunately, search engines such as HotBot[11] are able to search not only for content, but also for sites that link to your site. Check these sites on a regular basis to see if they are linking to or framing your site in a manner that is not appropriate.

4.2.3 Online Disclaimers

A problem with having a Web site is that everyone could become an adversary in the event that a difficulty arises with the information, services, or products that you have provided. In order to prevent financial loss and damage, every Web site needs a properly worded disclaimer. It needs to be written in a clear and unequivocal manner in order to be understood by anyone in the world. But because of differing national laws, a disclaimer or parts of it may not be valid in all countries.

If your Web site contains only some contact information, then a simple disclaimer will be enough, but as soon as you provide information, products, or services that businesses rely or act on, the disclaimer on your Web page needs to be as watertight as possible. If your company deals a lot with French-speaking and German-speaking countries, it is advisable to translate the disclaimer, as it may not be understood correctly by nonnative English speakers. A simple translation will not do it. It is necessary to check the local law and see if the disclaimer applies or if it needs to be adapted.

Once the wording of the disclaimer has been completed, it is necessary to find a good location for it on the Web page in order to make it easily accessible. On some sites the disclaimer is almost hidden, which renders it very ineffective. In some countries, such as Germany, it may even be illegal if the disclaimer is not presented in a highly visible manner. Putting the full disclaimer on the homepage, on the other hand, would be overkill. Typically, a link from all pages should be provided to the disclaimer, and in the case of accepting a business transaction of any kind, the customer should be notified about the disclaimer. The text could be presented in a text box on the Web page, as done, for example, by Lufthansa Cargo when customers order the SameDay online service.[12]

[11] http://www.hotbot.com/
[12] http://www.sameday.de/

4.2.4 Content Liability

The liability for content will vary in different countries. If your Web site contains only information about your company, it is necessary to create a process for the automatic verification of the content. Other than a magazine, for example, which is published periodically, Internet content is updated constantly. Therefore, the publishing processes need to be adapted to support the Internet presence. If you have to wait a week until you can publish anything on the Internet, you will eventually lose out, and since your company is liable for the content, you can be easily sued for publishing inaccurate information.

If you are an Internet provider, things become more complicated, since you are hosting other companies' services, information, and products. In order to prevent your company from damage, it is necessary to create a disclaimer and rules that explicitly forbid certain material on your servers. Although most countries consider Internet providers to be in a similar position as telephone companies, in some cases they are considered to be responsible for the content of the servers.

In 1998, Felix Somm, who headed the CompuServe[13] operations in Germany until he was indicted in 1997, was convicted in Germany of violating local pornography laws. Somm had been accused of trafficking pornography and neo-Nazi propaganda, which are both prohibited by German law, and was blamed for not blocking access to pornographic pictures that were available on the Internet. By convicting Somm, the court appears to be saying that Internet service providers in Germany are responsible for Internet content and must take affirmative steps to block access to objectionable material. This verdict fortunately is based on the German legal system and does not affect the laws in the United States.

Although a judge who apparently did not understand how the Internet works made the decision, it is an indication that illegal content can be a problem for every party involved in providing the information.

The situation has changed dramatically in Germany, though. New regulations make it quite clear who is responsible for content. It is the person that uploads the content to a Web site, and not the ISP.

This does not mean that all judges now know what to do. In March 2000 a new case was brought against CompuServe. AOL provided a forum where people started to trade MIDI files. A court ruled that CompuServe was responsible for the forum and therefore for the copyright violations.

4.2.5 Intellectual Property on the Web

Copyright protection on the Internet has several fundamental limits, defined by international agreements. In many countries, an expression can be pro-

[13] http://www.compuserve.com/

tected, but ideas or facts cannot be. A work that is very similar to another work does not infringe copyright either. Before the Internet arrived, these rules were easy to handle, as copying in many cases was at least as much work as rewriting in one's own words. On the Internet, information is copied very easily and very fast. Just copy the information from a site and paste it into your Web page. This can be done in seconds—and even automatically by specialized programs.

Brad Templeton has written a very interesting article about intellectual property on the Web.[14] His article, titled "The Biggest Myths About Copyright," gives a good overview on the issues of copyright. Today, almost every piece of information is copyrighted, whether a copyright statement is visible or not. Using that material is a violation of the copyright, regardless of whether you charge money for it or not. This applies especially to the Internet. Although information is freely accessible, it does not mean that the information can be reused for commercial purposes.

Many companies have started suing people who are running fan sites on the Web if they use copyrighted material. In the beginning, everyone was setting up fan pages without thinking about copyright issues, as these fan pages were created mostly for fun, and not for making money. But as trading banner advertising became more popular, many fan pages started to make money, which was not in the interest of the copyright owners. One example is *Star Trek*.[15] The owner of the *Star Trek* logos and images asked all fan page owners to remove the copyrighted information from their pages, leaving most pages blank. The number of *Star Trek* fan pages has decreased since then. This has angered many of the fan groups, who started to protest against this decision on the Web.

Other copyright owners try to bundle the fan pages into a single site. Look at ACMEcity,[16] which allows fans of various comic figures to create their own Web pages on that particular server. The fans are able to use a set of a few thousand images, sound, and other media as long as the pages remain on that particular server.

In May 2000, the producers of the television show Big Brother[17] tried to admonish anyone who tried to set up an unofficial fan page. In this case it is questionable if intellectual property is involved since the whole concept was without content.

The awareness of copyright issues has increased over the last few years, but people still want information on the Web to be free. Web technology enables the free transfer of information, and restricting it is difficult. The major advantage of the Web is that copyright owners can use search engines to discover copyright breaches easily.

[14] http://www.templetons.com/brad/copymyths.html
[15] http://www.startrek.com/
[16] http://www.acmecity.com/
[17] http://www.bigbrother.de/

Interestingly, the biggest problem on the Web does not come from text-based content, but from copied images, sounds, and programs. Images are easily scanned in and put onto a Web site. Many images come from books or magazines. The JPEG image format allows images to be presented on every screen of any type. The images are compressed so they do not take a long time to download. The music business fears the MP3 format, which compresses in a manner similar to the JPEG format, with a ratio of 1:10 or even higher. It allows complete compact discs to be copied over the Internet in a reasonable time. The files can be downloaded onto a computer and from there copied onto a cassette or another compact disc. And now the movie industry fears the Dvix standard that made available all movies online in a highly compressed format.

Distributing pirated versions of software has been made much easier with the Internet, and many sites offer pirated software for download. This is also one of the reasons why more and more companies offer free software, as protecting the software would cost more than distributing it for free. Until a few years ago, copying software was not protected by law, and only very recently have laws been introduced to protect databases (in Germany, for example, in 1998). Many countries still do not have copyright laws.

Most Web sites today consist of a database that contains travel information, email directories, or product information. Copying databases over the Internet is just as easy as copying information or software. Copying the database of Yahoo! is easy (as it is publicly available on the Internet), and without the copyright protection of the database, we would see many replicate sites popping up on the Internet.

The law does not apply for all types of databases. In some countries, databases that contain all information about a certain topic without sorting them systematically and methodically are not included, as they do not contain any added value. But this again is not true for all countries; therefore, do not assume that you have the right to copy the database from a Web server. If you use only small parts of a database, this is considered fair use. Copying the complete database onto a private system is not allowed without the permission of the database owner.

4.2.6 Online Auctions

One of the most disputed areas in online business is the online auctions. Not only are they the most publicized cases, but also the most spectacular ones. And most surprising is the fact that different judges have ruled differently for the same matter. Although online auctions are described in more detail in Chapter 7, let's explore some very interesting cases of the past. Remember, almost anything is sold through the Internet. In online auctions houses, property on the moon, dead dogs, marijuana, human kidneys, and even undelivered babies have been on sale. While many items on sale seem illegal, the situation is not that clear. Although e-business has now been growing over the last few

years, online auctions have a very difficult status, as they are not really well defined. In most cases an online auction is a flea market or a promotional tool. But many fear those auctions that feature low prices and bad quality.

Let's look at some recent problems with online auctions. Hardware.de,[18] an online auction site in Germany, for example, was dragged into a lawsuit because a company tried to sell HP[19] toner cartridges to customers through an online auction. In one case the auction stopped at 15 dollar/euro and the seller refused to ship the cartridges as the street price for these particular cartridges was at about 25 dollar/euro. The seller tried to pull out of the auction after it finished, due to the low price. They claimed that offering a product online does not mean that they are willing to sell it. The court ruled against the seller and decided that it had to sell the cartridges at the cost of the highest bid. This sounds quite reasonable, but unfortunately other judges have other opinions.

In Münster, not far from Hamburg, a judge decided just the opposite. A Volkswagen dealer tried to sell a car in an online auction, but was disappointed with the low price it generated for a new car. The highest bid was only just above 10,000 dollar/euro. The dealer decided not to ship it to the customer, and refused to sell it at that price. The judges decided that the dealer was right, because no legal contract was signed over the Internet. In this case the dealer was lucky, as there had been no minimum price set.

In Italy all auctions online are forbidden by law, but it seems that nobody really cares. All big players in online auctions have an Italian Web site, and business seems to do quite well. In Germany several organization tried to prohibit online auctions, but failed.

There are many other cases around the world, where similar problems have occurred. The major inhibitor to online business is the changing interpretation of the laws in different countries.

4.3 Encryption Algorithms

4.3.1 Key Escrow

Discussions in many countries are going on about encryption algorithms and privacy issues. Encryption algorithms allow transmitting information using code that cannot be read by people who do not have the right key or password. Law enforcement agencies and governments all over the world discuss the possibility of disallowing encryption in order to keep up public safety. Many politicians think that criminals are the only ones using encryption technologies. But this is not true.

Encryption algorithms are essential for e-business. See Table 4.4 for a simple encryption algorithm. Without privacy protocols, every business transaction over the Internet could be made public and used against the participants in

[18] http://www.hardware.de/
[19] http://www.hp.com/

the transaction. Would you want to show your competitors how much business you are doing with your customers, or even let them know who your customers are? Of course not, but still many politicians think that it is better to ban encryption.

Some countries, like France, already allow the use of encryption only if a copy of the keys that are used for the encryption have been sent to a governmental agency. This concept, called key escrow, allows the government and the police to decipher encrypted messages. The idea behind it may be good, but it won't work. People and businesses won't trust encryption algorithms if they know that the government is able to read their information. And it won't keep criminals and terrorists from using it.

In most countries the possession of weapons is illegal, but criminals still use them. Making encryption illegal will be an even worse scenario. All business transactions over the Internet would become public, and this information would be used by other companies to ruin businesses. Even if encryption were to become illegal all over the world, it is likely criminals would still use it, since they clearly don't care about what politicians or the laws say. A detailed description of encryption technologies can be found in Chapter 11.

One of the simplest encryption algorithms is ROT13. With this algorithm, every letter is assigned a number. A becomes 1, B becomes 2, and so on. If you now write "HELLO," you assign each letter a number and add 13 to it, then replace the number with a letter again. If the number is larger than 26, subtract 26 in order to stay within the range of the alphabet. "HELLO" becomes 8, 5, 12, 12, and 15. Now add 13 to each of the numbers and you get 21, 18, 25, 25, and 28. Since 28 is larger than 26, we subtract 26 from 28 and get the following: 21, 18, 25, 25, 2. This becomes eventually "URYYB," which has no resemblance to "HELLO." This is an example of a very simple encryption algorithm. It is sufficient, if you are afraid that someone is scanning your mail in transit for keywords. Using this simple encryption, they won't find the keywords anymore. But even this won't be really secure; adding a little decryption algorithm to the scanner can be done without too much trouble.

Table 4.4. A Simple Encryption Algorithm—ROT13

4.3.2 Legal Issues on Export

Governments all over the world fear strong encryption. Originally developed for the military, it uses complex mathematical algorithms to encode text and binary code. In 1991, Phil Zimmermann wrote a 128-bit encryption program called PGP[20] (Pretty Good Privacy). The program was distributed over the Internet and suddenly people from all over the world were able to encrypt and protect their data.

In the United States, ammunition is treated as such and requires a special export license. As Zimmermann did not request such a license before releasing PGP over the Internet, he was arrested, as publishing on the Internet is the same as exporting it to other countries. Anybody throughout the world is able to download the application. After three difficult years in court, the government relaxed the restrictions on encryption algorithms.

In 1996 encryption algorithms were dropped off the list of controlled ammunition. Still, it is illegal to export any technology that uses encryption algorithms that are stronger than 40 bits without the written consent of the U.S. government. In order to export strong encryption algorithms, you need to leave the keys with the government. The only exception is the banking sector, which has a special regulation that allows exporting 128-bit keys for banking applications. But the laws on exporting encryption algorithms in the U.S. are not very logical at the moment.

In 1994, Phil Karn requested permission to export his book *Applied Cryptography*. The book discussed encryption algorithms and had a floppy disk that contained all of the source code. The book was approved for export, but the floppy disks were not. The export of encryption algorithms in digital form is forbidden, but exporting it in book form is not. Karn sued in order to find out what the difference was. Although the case is still pending, others are using this hole in export restrictions to get algorithms outside of the U.S.

For example, PGP was developed in the U.S. In order to ship it to international customers, the source code has been printed out. The resulting book of more than 5,000 pages has been exported to Finland, where some people scan in the source code and put the program back together. PGP supports key lengths of up to 4,096 bits in version 5.5. It is actually no problem to extend the number of bits to a higher number, but with each additional bit, encryption and decryption take longer to complete. Although 1,048,576 bits may be really safe, it is impractical, as it takes too long to encrypt. Not even your grandchildren would see the result of the encryption and decryption.

There are two types of encryption: symmetric and asymmetric. With symmetric encryption, it is legitimate to export 40-bit keys, and with asymmetric, it is possible to export 512-bit keys. Browsers use symmetric encryption and PGP uses asymmetric encryption algorithms. A more detailed discussion on

[20] http://www.pgp.com/

Using the brute force method, it is now possible to hack a 40-bit encrypted code in very little time. There are even screensavers that use the free time when a user is not working at a certain computer to hack 40-bit encryption algorithms. Just recently a text with 56-bit encryption was cracked in three days.

By adding a bit to the key, the strength of the key is doubled. If it takes three days to crack a 56-bit key, then it will take approximately six days for a 57-bit key. A key with 64-bits can be cracked in 768 days. Faster computers will eventually decrease the time to crack these keys; therefore, it is important to use keys with more bits. At the time of writing 128-bit keys are safe, but soon you will have to switch to 256-bit keys in order to be sure that nobody can break into your information.

Table 4.5. Breaking Encryption Algorithms

encryption algorithms can be found in Chapter 11.

As exporting encryption technologies in book form is very time-consuming and error-prone, encryption algorithms developed in other countries become more important for e-business transactions. Some of the most important companies are Baltimore Technologies[21] in Ireland, which develops public key infrastructure software; Brokat[22] in Germany, which creates online banking software; Softwinter[23] in Israel, which programs encryption software for Windows NT; and C2Net[24] in Australia, which develops the Stronghold Web server that allows SSL-enabled transactions at 128 bits. These companies offer encryption algorithms that use any bit rate your application requires, without any restrictions on export. They can also be imported into the U.S., as there is only a restriction on export.

The U.S. Congress is under pressure from the software industry to change this policy, as it destroys the encryption technology market for American companies. It hinders free trade and the development of new technology in the U.S. While American companies try to find a compromise with the government, companies in other countries move on to develop and introduce new technologies, giving them the leading edge over their competitors in the U.S.

[21] http://www.baltimore.ie/
[22] http://www.brokat.de/
[23] http://www.softwinter.com/
[24] http://www.c2.net/

4.3.3 National Encryption Laws

This subsection provides a brief overview on the national laws in different countries around the world. Governments have only recently realized that laws and regulations are needed. As knowledge and awareness are still being built up, laws are changing constantly and quickly. Just remember the former chancellor of Germany, Helmut Kohl, who, when asked a few years ago what he thought about the information highway, thought the questioner was talking about the German Autobahn. Since then, awareness has increased significantly within governments. But due to the global nature of the Internet, it is difficult for single governments to be able to solve legal issues on their own. National governments view the Internet as a threat to their power.

Remember that you should not count on the information given here as being valid at the time of reading, and policies and laws are changing rapidly. France, for example, has just recently abandoned its policy of disallowing the use of encryption. Great Britain, on the other hand, has been talking for a while about introducing regulations on encryption technologies. On this book's Web page[25] you will find up-to-date information on national encryption laws.

Table 4.6 has a list of some of the larger countries around the world with national regulations on the use of encryption, and how import and export are handled by these countries.

4.3.4 Digital Signatures

Not only can encryption technologies be used to ensure that nobody other than the authorized persons are able to read a certain message, it is also possible to ensure the authenticity of any given message through a digital signature. Internet services offering public key infrastructures (PKI) offer both functionalities as part of their service.

Contrary to public belief, it is possible to sign digital documents in a way similar to how traditional documents are signed. A digital signature is not a scanned image of a handwritten signature or a typed signature. The digital signature is an electronic substitute for a manual signature. Technically speaking, it is an identifier composed of a certain sequence of bits that is created through a hash function, and the result is encrypted with the sender's private key (which can be decrypted by anyone who is in possession of the public key). By adding the digital signature to the digital document, it can be easily verified who signed it, when it was sent off, and whether the document was altered during transit.

Once the encrypted message has been sent out, the recipients are able to decrypt the message using their private key. If a signature is found, the same hash function that the sender was using is invoked, and the message digest of the recipient is compared automatically with the result of the sender. If the two results match, the message was really sent by the sender. And it can be

[25] http://www.ebusinessrevolution.com/

Country	Use of Strong Encryption	Export of Strong Encryption
Australia	No restrictions on use.	Some restrictions on export.
China	Not allowed.	No information.
European Union	No restrictions on use.	No restrictions on import and export.
India	No restrictions on use.	No restrictions on export. License for import is required.
Israel	License is required, but almost always granted.	Regulations for import/export exist and are handled case-by-case.
Japan	No restrictions on use.	License for export is required. No export of encryption software is allowed.
Russia	A license to use encryption is required.	No restrictions on export. License for import is required.
Singapore	No restrictions on use.	No restrictions on import and export.
South Africa	No restrictions on use.	No restrictions on import and export.
South Korea	Not allowed.	Import/export of encryption is prohibited.
United States	No restrictions on use.	License for export is required for encryption software of more than 56 bits.

Table 4.6. National Encryption Regulations

verified that nothing has been changed in transit by checking the integrity of the message.

As digital certificates are difficult to forge, nonrepudiation has become possible on the Internet. If a person has sent out a certain message, it can be traced back easily through a PKI and the signatures. The PKI is used to store the time when a certain message has been sent out, which can be very important in some business cases.

Digital signatures form the basis for legally binding contracts in the course of electronic business, since they electronically provide the same forensic effect that a traditional paper document and a handwritten signature would. In order to use digital signatures legally, a framework needs to be created in all countries that defines exactly what a signature is and how it can be created. In the European Union, several initiatives have been started, both on a Union-wide level and on a nationwide level, such as the "Signaturgesetz" in Germany. But it is unlikely that national legislative initiatives can be used on the global Internet.

A prospective directive for establishing a legal framework for the use of electronic signatures[26] was presented in 1998 by the European Commission. By defining the minimum rules for security and liability, the proposal ensures that digital signatures are legally accepted throughout the European Union. It creates a framework for secure online transactions.

4.4 Developing a Dark Site

4.4.1 Reasons for Crisis Management

Products or services sold online may possibly be defective or have some sort of a problem. If there is more than a single incident, the manufacturer or retailer will get in trouble. If such a disaster happens to your company, you have two possibilities. Either cover it up and hope that nobody will notice or go public with all the information you have, warning people and giving them advice on how to resolve the problem.

The first choice is no longer an option with the wide use of the Internet. You just cannot keep something secret—normally, too many people are involved and someone will leak it to the Internet. So the only thing you can do is go public and let everybody know that you are aware of the problem and take the responsibility for that particular issue.

In order to be prepared for such a situation, you need to create a *dark site* that can go online in case of a problem or an emergency. A dark site is not a sort of voodoo site, but a site that is kept secret until it is necessary to use it. The dark site contains information on your product you would not have released, but may be helpful in case of defects.

[26] http://europa.eu.int/comm/dg15/en/media/infso/com297en.pdf

Product defects are not the only issues that can cause problems. Unhappy or angry online users are able to put up Web sites with negative information about your company, your product, or both. Due to its infrastructure, every Web page has the same priority on the Internet. If someone puts something up against you, you had better take it seriously. It takes only a few people with a Web site to set back the whole production of a company. But even worse than Web sites are emails, which are sent out to other Internet users at the speed of light. In the real world, one bad experience is relayed to fewer than 50 people in most cases. Bad experiences on the Internet are sent out to thousands of people with a single mouse-click.

4.4.2 Disaster Recovery

Ulrike Brandt, a financial journalist, has written a very informative article on Internet crisis management in the German financial magazine *Wirtschaftswoche*,[27] where she discusses the topic of disaster recovery and where you can get additional information. The topic is very important, but unfortunately, not many managers are aware of it.

Just look at the case of Intel.[28] In 1994, Thomas Koenig, a mathematician, found out that the newly released Pentium chip did not calculate correctly. Under certain conditions, divisions, remainders, and tangent and arctangent floating-point instructions produced results with reduced precision. He reported this error to the chip manufacturing company, but Intel put him off. First, it denied the existence of the bug, then stated that the problem affected only very few users. Then Intel wanted the users to prove that they needed that special calculation to certify for a replacement.

All this created a huge outcry on the Internet; Web sites were put up and heated discussion threads started in the Internet newsgroups. The result was a huge avalanche that landed on Intel. The media talked about the problem, users sent angry emails to Intel, wanting their chips replaced, and the chip sales dropped. As a result, Intel gave up in December 1994 and offered to replace all faulty Pentium chips[29] and had to stop the complete production of that particular chip, even though it was right that only very few were affected. But giving up production of that particular chip was not so difficult, as faster chips were already in the pipeline. The next generation of Pentium chips, without the error, was already designed and the roll-out phase began soon after.

Since then, Intel has changed its strategy. Even though it still cannot guarantee that their chips are error-free, it is now more open to customer issues and maintains an online database with known errors in the chips. With the introduction of the Pentium II, Intel also invented a way to update some parts of the microcode on their chips so bugs can be removed without replacing them.

[27] http://www.wirtschaftswoche.de/ "In Sekunden zerstört," *Wirtschaftswoche* 45/29.10.1998, pp. 157–160.

[28] http://www.intel.com/

[29] http://www.intel.com/procs/support/pentium/fdiv/

The first release of the Pentium did contain a bug in its floating point processor that returned a faulty result when performing a floating point division (FDIV). To see if your Pentium has the FDIV bug, enter the following formula in the Windows calculator:

$$x = \frac{4195835}{3145727} \times 3145727 - 4195835$$

The result should be $x = 0$. On faulty Pentiums, you will get $x = 256$ instead. In this case you are entitled to receive a free replacement for your faulty Pentium chip.

Table 4.7. The Pentium FDIV Bug

Its newer chip, the Pentium III, on the other hand, seems to be a marketing disaster. The Pentium III chip contains a digital ID that is unique for every processor. The reason for it was to provide a means to check the identity of a particular user for online transactions. Intel's serial number is appealing to corporate customers, because they can more easily track technology assets through the identifying serial code.

Although many online companies like the idea of identifying customers, privacy groups have called for consumer boycotts and legal action and created a Web site called "Big Brother Inside"[30] that resembles the Intel motto of "Intel Inside." Many people (hackers and software company employees) have started to crack the safeguards imposed by Intel to make the serial number secure. Although at the time of writing nobody was able to crack the highly secure ID number, the message that gets out to the customers is the wrong one, at least from Intel's point of view.

Other companies do not seem to be affected by angry users. Microsoft,[31] for example, does not seem to have this problem. Although there are many anti-Microsoft sites on the Internet, Microsoft is not losing market share because of them. Ford[32] had problems in 1995 similar to Intel's. Due to a technical problem, some Ford drivers claimed the car could go up in flames. The online activists, calling themselves the "Association of Flaming Ford Owners," decided to put up a Web page[33] with the image of a burnt-out Ford on the main page and flames in the background (see figure 4.1).

[30] http://www.privacy.org/bigbrotherinside/
[31] http://www.microsoft.com/
[32] http://www.ford.com/
[33] http://www.flamingfords.com/

Figure 4.1. Flaming Ford Owners' Homepage

In April 1996, Ford had to recall more than 8.7 million cars and trucks in the United States and Canada to have the ignition switches replaced (with potentially up to 26 million cars and trucks that may need a replacement). The action cost Ford more than 1.5 billion dollars. In this case it is not known if their claims were right or not, but that is not the point. The incident happened in 1995, but the Flaming Fords Web site is still up and running in 2001. Today more than 20,000 links exist to that particular Web site. People may stumble over it and decide not to buy a Ford.

In December 1998, Ford issued a short press release that it had to recall more than three million cars because of a possible corrosion problem. I found this snippet on Yahoo!'s *dailynews* site[34] (search for "Ford Recall Issued," December 23, 1998) and went then directly to Ford's home page to check if they have a press release with more information on the incident, but was not able to find anything. Ford's search engine gave me no more information, nor was there a link from its home page as one might have expected. Maybe there was information online, but I couldn't find anything within 10 minutes of searching. It may also be that because of the holiday season, no Webmaster was around to update the information. But not being there during holidays may ruin your business even faster, as more people have time to surf on the Internet.

The Internet enables consumers to talk more freely about their experience with a certain product or service, so it becomes vital for all companies to keep

[34]http://dailynews.yahoo.com/

an eye on the Web to track down people who are not happy with their products. If you think you can just shut down the Web site of that particular consumer, you do not understand how the Internet works. Once information has been put online, it is virtually impossible to get rid of the information. If you cut off somebody's Web site, they will find 50 others who will replicate their content immediately. The more pressure you put on people, the less effective it becomes, as more and more people join in to support them.

There is no way you can stop people from publishing their opinions on the Web, no matter how right or wrong they are. The only thing you can do is set up a Web site that tells consumers that you are aware of the allegations. If the allegations are true, you had better put some additional information online about how to solve the problem. If the claims are false, put some evidence online to prove you are right. In any case, respond quickly or you will lose out, no matter if you are right or not.

4.4.3 Negative Campaigning

In addition to angry consumers, negative campaigning can spell bankruptcy for your company. Negative campaigning by your competitors can also ruin your image with the public. Instead of showing the advantages of their own products, they will start to find all the disadvantages of your products.

In December 1998, Sun[35] launched a Web page with information on Hewlett-Packard's newly introduced UNIX Server HP V2500.[36] Depending on your point of view, the information presented on that particular Web page is either positive for Sun or negative for Hewlett-Packard. In the European Union, law prohibits, for example, negative campaigning and comparative advertisement. But on the Internet, national laws are not always applicable. Putting up the information on a Web server in another country is fairly simple. Countries like Bulgaria just recently introduced laws against software pirates, but there are still enough countries where the Internet is beyond the scope of the law. But in our example, merely putting the desired page onto an American Web server would resolve all legal issues regarding the content.

Another problem is the media. Due to the amount of information a magazine or newspaper receives each day, it is virtually impossible to check if all of the data is correct or incorrect. Especially in the U.S., we can see a tendency to print information without double-checking it. Together with negative campaigning, this can have a negative impact on your products and/or your company. Therefore, always keep an eye on the Internet. Look out for these tendencies within your user groups, keep in touch with them, seek dialogue, and in the case of an emergency, react quickly. In our interconnected world there is no way to avoid a disaster if you are not open to your customers. This is one of the reasons political dictators fear the power of the Internet. They

[35] http://www.sun.com/

[36] http://www.sun.com/realitycheck/headsup981215.html

just can't control information anymore, which is their only real power over the people.

In the event of an emergency your company needs to act quickly. Therefore, you have to take some steps before, during and after the crisis:

- **Risk audit**—Do a risk audit of your company on a regular basis.
- **Documentation**—Develop plans for documenting tasks and responsibilities for the emergency.
- **Keyword monitoring**—Constantly monitor the Internet (especially Web sites, mailing lists, newsgroups and chat areas) for special keywords.
- **Crisis manual**—Develop a crisis manual and put it on your intranet.
- **Dark site**—Design a dark site with all the necessary information.
- **Simulations**—Do simulations of emergency situations on a regular basis.
- **Up-to-date**—In case of emergency, always keep the dark site up-to-date.
- **Information**—Inform your target group and the media via e-mail about the emergency.

Table 4.8. Risk Management

4.4.4 Online Experience

In October 1996, a 16-month-old baby died from an infection of E-coli bacteria. The baby had ingested apple juice made by Odwalla,[37] a California-based juice company. The apple juice was suspected of being the source of the bacteria. Within 12 hours, the management of Odwalla recalled the apple juice from more than 4,500 shops and set up a Web site with information on the incident.

[37] http://www.odwalla.com/

It contained a statement by the management, and a frequently asked questions (FAQ) page on E-coli bacteria written by doctors, to help the victims. A team of experts was online to calm down the frightened consumers. The site also provided links to the Web site of the Food & Drug Administration (FDA)[38] that contained additional information on emergency situations. Although another 66 cases of E-coli infections were registered, a survey showed afterward that almost 90 percent of the customers were willing to drink Odwalla apple juice in the future. The investment in releasing all information and creating the dark site had been spent wisely.

After the horrible crash of the MD-11 off the Canadian coast in September 1998, Swiss Air[39] set up a first press release on its Web site within hours. Important phone numbers, a condolence Web page, and some other statements were available on the Internet the same day. In the following days, more information was released, including the radio chats between the tower and the pilots and the names of the deceased. The very efficient Webmaster rescued Swiss Air from losing its highly successful business as a result of this single, though extremely tragic, incident. It also helped the relatives of the victims to find out more on the incident without having to search for information all over the place, as often happens.

Figure 4.2. Swiss Air's Homepage

[38] http://www.fda.gov/
[39] http://www.swissair.ch/

The Deutsche Bahn,[40] the German rail service company, lost a large amount of credibility after the derailing of one of its high-speed trains in May 1998. Information was not available on the incident immediately after the accident (neither online nor offline), nor was the Bahn responding to the families of the customers in a sensible way. A general letter was sent out to each of the families with advertisements for rail journeys. The company was not prepared for handling such an incident. It seemed that they thought that it could never happen. *Der Spiegel*,[41] the most-read German news magazine, compared this accident to the tragic incident of the *Titanic* in 1912.

You need to start thinking about a strategy long before an emergency occurs. You should conduct a risk audit for your company, analyzing what could go wrong with your products. Develop plans where the tasks and responsibilities are documented for the emergency situation. In order to learn about emergencies in advance, you need to monitor the Internet seven days a week, 24 hours a day. First you need to create a list of keywords and then check Web sites, newsgroups, search engines, and databases on a regular basis. Mailing lists and chat areas should also be visited if your target group is using these types of media. This is the only way to find out about dissatisfied customers and aggressive competitors. Your emergency plan should be available on your intranet so that people know what to do whenever they need to, and a printed copy should also be available in case of a technological breakdown.

4.4.5 Digital Complaint Services

Another factor that needs to be taken into account are online complaint services, which are hoping to make money by resolving consumer disputes with Internet retailers. These services are able to bundle complaints against companies and create class-action suits in a very simple and effective way. Consumers will get access to a brand name and experience in linking up with major companies to make sure the complaint goes to the right person quickly.

Complain.com,[42] Fightback,[43] (see Figure 4.3) and Complain To Us[44] are three service companies that specialize in this area. These companies charge a flat fee if they get involved in writing a letter and following up complaints. Fightback, for example, charges $25, while Complain.com charges $19.95 for any case that is pursued personally, while all other complaint resolutions are free of charge.

Consumers can fill out a form with information about the product or service they purchased, what went wrong, the actions they have taken to resolve the dispute, and the resolution they are seeking. In order to qualify for the online

[40] http://www.bahn.de/
[41] http://www.spiegel.de/
[42] http://www.complain.com/
[43] http://www.fightback.com/
[44] http://www.complaintous.com/

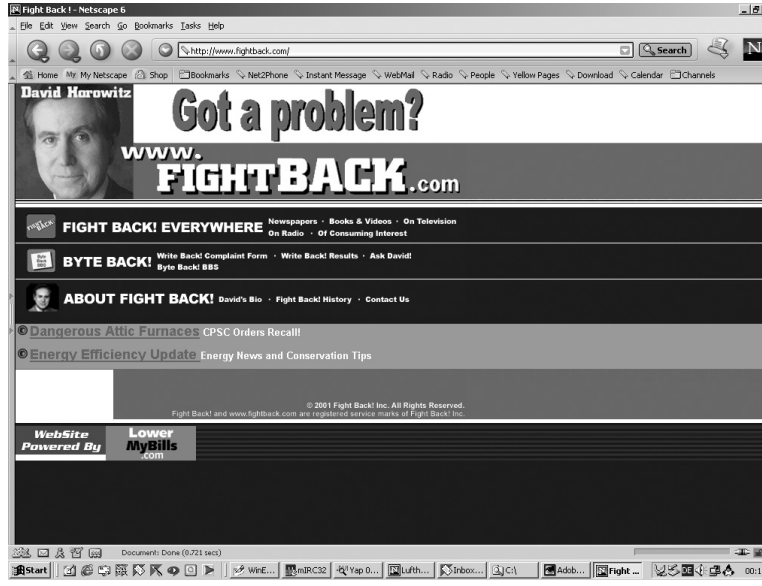

Figure 4.3. Fightback Homepage

complaint service, the customer must have tried to contact the customer care department themselves.

Complaint.com does send a letter of complaint to the company, and the consumer will receive a confirmation within four weeks if the issue has been resolved. If the problem persists, the letter will be sent once more to the company, but this time to the chief executive. If that does not help, consumers will be referred to partners such as law firms to pursue further action.

While single complaints won't be very effective, the aggregation of complaints and the publicity on the Web site will drive companies to respond to the issues of their customers. The above-mentioned companies also have plans to publish the contents of their complaint database on the Web, making it easy for customers to look up complaints from the past and find out how to resolve a particular issue.

4.4.6 Strategic Planning

As mentioned earlier, it is important to develop a dark site that contains basic information about your company and your products. It should inform your customers on security measures and should contain a list of experts they can contact in the case of an emergency. The dark site should replace your normal Web site within an hour, or better yet, within 30 minutes of a disaster. The management needs to be informed about the Internet presentation and to re-

lease statements as soon as possible. The Web site needs to be updated as soon as new information about the emergency is available.

The dark site should also be put on removable media, such as a CD-ROM or ZIP disk. Just in case your company gets cut off the Internet, you can send the information to an ISP that is able to quickly set up an emergency site. In this case, inform the public immediately via TV, radio, or newspapers about the incident and tell them about the emergency URL. Many of these steps need to be taken, even if your company is not presently on the Web. But with the Internet, you have to be even faster in your communication of the crisis. If you don't talk about it, then someone else will for sure. Remember, the competition on the Internet is extremely tough.

Doing all this is not cheap, but not doing anything is far more expensive, as we have learned from the examples presented here. Larger corporations have special task forces for emergency situations. While that would be overkill for small and medium-sized enterprises, they also need to keep an eye on the Internet.

Specialized search engines will monitor the Web for them. They only need to key in their desired keywords, and these search engines will monitor the Web day and night. As soon as something happens, an email will be sent off that triggers a beeper or other alarm to get the attention of the responsible person so that the company can react to the threat from the Internet. Two Web sites that offer this service are "The Informant"[45] and "Mind-It."[46]

Many small to medium-sized companies will most likely outsource the task of monitoring the Web. Specialized companies will take over the task. They will become the watchdogs over content, and they will also react in the case of a crisis. Investment in such a company is a good bet for Internet investors. These services are needed, and their revenues will increase quickly in the future.

Although dark sites and other means of prevention won't reduce the liability for an error in a product, these measures will certainly help to limit the financial damage that can ruin a company.

[45] http://informant.dartmouth.edu/
[46] http://minder.netmind.com/