Internet access continues to expand, with current estimates of 407.1 million Internet users worldwide\(^1\) and an estimated 165.2 million users in the United States alone.\(^2\) The explosive growth of Internet use for information access, file transfer, e-mail, collaborative work, banking, shopping, and performing countless other functions has brought about an escalation of concerns. The advantages of quick access to timely data and less restricted communications resulting from Internet connectivity have been accompanied by reduced consumer confidence in Internet-related business activities, the risks of financial loss, and legal liability from sources both external and internal to the organization.

Organizations have responded by creating the position of Chief Privacy Officer (CPO). The primary responsibility of the CPO is to protect online consumer privacy by developing an organization’s privacy policy and ensuring compliance with privacy laws and regulations. However, the explosive growth of Internet use for business has brought about an escalation of concerns, including reduced consumer confidence in Internet-related business activities, risk of financial loss, and legal liability from sources categorized as external and internal to the organization. This article discusses the far-reaching types of misconduct and risks organizations face, and concludes by proposing the strategic response of an expanded role for the CPO.

The effectiveness of this new role, in overseeing these responsibilities, would be determined by assessing current operations, implementing proactive measures to reduce potential misuse, and continuously keeping abreast of technological advances, legislative and regulatory initiatives, and new areas of vulnerability.
laws and regulations. There are currently about 350 CPOs in the United States according to Alan Westin, who founded the International Association of Corporate Privacy Officers. Westin projects that the number of CPOs will rise to between 500 to 1000 this year as organizations respond to new privacy-related laws and regulations. For example, three significant new laws and regulations imposing privacy standards in the United States went into effect November 1, 2000. Included among these are the Gramm–Leach–Bliley Financial Modernization Act, directed at consumer privacy in the financial services industry; the Health Insurance Portability and Accountability Act, which ensures patients' medical records are private; and the United States Department of Commerce's Safe Harbor list, intended to assist United States corporate compliance with the European Union Data Protection Directive. While appropriate for issues of consumer privacy, does the new CPO position provide adequate consideration of the increasing risks facing online organizations?

The first line of defense in responding to increasing risks resulting from inappropriate Internet activities is to raise the awareness and understanding of what the risks are and how they might arise. This article first discusses the various types of misconduct and the risks organizations face. The scope of considerations is far-reaching. Certainly, this discussion is not comprehensive. Any effort to address all possible threats is never-ending, as online activities are limited only by the imaginations of an increasingly Internet-savvy workforce and worldwide population. The article concludes by proposing the strategic response of an expanded role for the CPO. In addition to overseeing an organization's Internet privacy issues, the role of CPO should encompass Internet integrity. Thus, this individual's realm of responsibility would encompass not only privacy-related laws and regulations but also online content liability and the interpretation of laws and regulations as applied to the Internet.

ORGANIZATIONAL RISKS OF INTERNET USE IN BUSINESS

To promote an understanding of the types of misconduct and the risks to which organizations are subject, this section presents example threats to Internet use in business. As shown in Exhibit 1, the sources of these threats are categorized as external, both external and internal, and internal to an organization. Each of these categories is not exclusive, but rather there is overlap among them. The purpose of the categorization is to reveal the motivation and implications resulting from each source. A summary of the sources and corresponding threats is presented in Exhibit 2.

External Threats to Online Organizations

Online organizations are subject to a diversity of threats from the external environment. Each of these sources may have differing motives but may
nonetheless cause financial loss or reduced confidence in Internet-related business activities of the targeted organization.

**Competitors.** Competitors and industry spies may seek to gain access to copyrights, intellectual property, trade secrets, and other proprietary information. Intelligence gathering has occurred for decades, including traditional spying methods such as browsing at a competitor's store, posing as a customer, searching obscure public records, or counting deliveries at the loading dock. In what Microsoft Corp. called a deplorable act of corporate espionage, hackers gained access to its computer network by using an e-mail account in Russia to steal passwords to the network. At a minimum, the hackers were able to view source code to recent versions of the Windows operating system and portions of its Office suite. Organizations must be on the alert to recognize the corresponding e-methods for spying.

**Consumers.** The major concern of consumers focuses on privacy. Online businesses have increasingly sought to tailor Web site interaction and target promotional activities to individual consumers. This requires the collection of various types of data, preferably identified with a specific individual.
The use of cookies enables personal information to be easily obtained from Web users, often without their knowledge. In addition to click-stream data, cookies can collect the user’s IP address, the number and dates of prior visits, the type and version of browser and operating system, among other types of information. Further, users may be asked to provide registration information when visiting a Web site which, when combined with data collected through tracking technology, can be used to create an individual user profile. Subsequently, this information may be used to send unsolicited bulk e-mail, or spam. While primarily utilized for commercial purposes, spam may also promote political, malicious, or illegal schemes.

Consumer reaction has ranged from outrage to filing lawsuits against major Internet companies for failure to disclose data collection practices or to comply with their own published privacy policy. Among the companies named in claims are Amazon.com, RealNetworks, and Yahoo!. In addition to the special regulations that recently went into effect, the Federal Trade Commission recently asserted its authority by bringing enforcement actions against Web sites for questionable data collection practices.

---

**EXHIBIT 2 — Sources and Example Threats to Internet Content and Use in Business**

<table>
<thead>
<tr>
<th>External Sources</th>
<th>Both External and Internal Sources</th>
<th>Internal Sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competitors</td>
<td>Business Partners</td>
<td>Employees and Consultants</td>
</tr>
<tr>
<td>Copyright infringement</td>
<td>Regulations violations</td>
<td>Employer Liability</td>
</tr>
<tr>
<td>Intellectual property loss</td>
<td>Cookie sharing</td>
<td>Copyright infringement</td>
</tr>
<tr>
<td>Trade secret loss</td>
<td>Technical failures</td>
<td>Defamation and libel</td>
</tr>
<tr>
<td>Consumers</td>
<td>Device defects</td>
<td>Discrimination</td>
</tr>
<tr>
<td>Invasion of privacy Criminals</td>
<td>Loss of network</td>
<td>Harassment</td>
</tr>
<tr>
<td>Defaced Web sites</td>
<td>Misdelivery</td>
<td>Hostile work environment</td>
</tr>
<tr>
<td>DDoS attacks</td>
<td>Password loopholes</td>
<td>Obscenity</td>
</tr>
<tr>
<td>Hacking and cracking</td>
<td></td>
<td>Pornography</td>
</tr>
<tr>
<td>Malicious code</td>
<td></td>
<td>Invasion of privacy</td>
</tr>
<tr>
<td>Theft</td>
<td></td>
<td>Securities violations</td>
</tr>
<tr>
<td>Government</td>
<td></td>
<td>Trademark and trade secret violations</td>
</tr>
<tr>
<td>Discovery (subpeona)</td>
<td></td>
<td>Loss of employee productivity</td>
</tr>
<tr>
<td>Law enforcement (search warrant)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intruders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
**Criminals: Hackers and Crackers.** Legal commentators are divided over how Internet crime, or cybercrime, should be addressed. Cybercrime can either be viewed as traditional crime committed with computer resources or as a new category with unique considerations requiring a new legal framework. Emerging technologies are accompanied by emerging challenges such as perpetrator identification, intent and motivation, jurisdiction, and international cooperation. Although acting from outside of an organization, disgruntled insiders are the primary perpetrators of Internet crime. The perpetrators, generally referred to as hackers or crackers, have cost United States businesses an estimated $10 billion annually according to the FBI, from various activities ranging from simple criminal trespass to sophisticated Web site defacing, distributed denial of service (DDoS) attacks, hacking and cracking, malicious code, and theft of proprietary information, resources, and services.

Web site defacing entails unauthorized access to either a user’s account or the webmaster’s password to download, alter, and upload a Web page. Perhaps the most brazen of Web site defacing was directed against the Federal Bureau of Investigation, which investigates this criminal violation of federal law.

DoS attacks direct numerous computers to send service requests to a targeted Web site. A rash of DoS attacks against prominent Web sites, including Amazon.com, eBay, and Yahoo!, occurred in February, 2000. The servers at these targeted sites were so overwhelmed that the sites were unable to respond to legitimate requests, causing more than $1.2 billion in total losses. The estimated losses are based on each company’s lost revenues for site downtime, lost market capitalization due to plunging stock prices, and the cost for systems security upgrades. Future losses may result from a reduction of consumer confidence in E-commerce. Additionally, organizations and Internet service providers could be held liable for unwittingly allowing their computers to partake in the attacks.

Hacking and cracking entails trespass for the challenge or thrill of gaining illegal entry, illicit financial gain, or malicious activities. According to a survey by the FBI, 55 percent of respondents reported malicious activity by disgruntled insiders. A former employee of Forbes, Inc. used a co-worker’s account to vengefully cause five network servers to crash and erased the server volume on each. A two-day shutdown of Forbes’ New York operations resulted in losses exceeding $100,000.

Malicious code is devised to cause damage or to steal information. There are an estimated 30,000 viruses in existence, with approximately 300 new viruses created each month. The most common forms are viruses, worms, and Trojan programs, designed to spread from one computer to others via executable code in e-mail or infected disks. The resulting damage can be quite costly. For example, the Melissa Macro virus caused an estimated $80 million damage; and the “ILOVEYOU” virus cost an estimated $10 billion in damage worldwide.
**Government.** The government may gain access to Internet content through law enforcement activities or discovery processes. Law enforcement agencies investigating illegal activities may present a search warrant to search files or e-mail messages in transit, stored on disk or in paper form, backed up to tape, or even those which have been deleted and overwritten. Similarly, through discovery, a subpoena may be issued. For example, e-mail messages written by Bill Gates were retrieved and used as evidence to support the Department of Justice’s antitrust lawsuit alleging that Microsoft used its Windows monopoly to unfairly crush Netscape Navigator. Antitrust experts commented that the messages constituted some of the most damaging evidence against Microsoft.

**Intruders.** Organizations are subject to intrusions that are not illegal but may certainly be disruptive. Unlike criminals who gain illegal unauthorized entry, marketers and advertisers are able to intrude upon the privacy of employees through cookies and spam. Organizations may question the methods and types of information collection and the use of that information. Further, spam can overload a company’s server and cause it to slow or crash.

**Both External and Internal Threats to Online Organizations**

Threats to Internet content may straddle the external and internal environment through sources such as business partners and technical failure. Business partnering may include formal and informal alliances established for a joint project. Technological glitches can expose organizational content to perusal by unintended sources.

**Business Partners.** Organizations are less likely to view business partners as a threat, in contrast to other sources such as competitors. However, the interests of a partner organization lie primarily with furthering its own goals. An organization may be liable not only for the actions of its own employees, but also for those of partner employees. The risks from a source that is both external and internal can become more complicated. Global partnering, for example, requires compliance with a multitude of trade laws worldwide. Web sites must comply with the European Union’s privacy laws, which restrict the collection of personal data. Other areas of global restrictions include consumer protection laws, advertising restrictions, and the international equivalents of the United States Food and Drug Administration.

A risk unique to Web site partnering is cookie sharing — the practice of collecting and consolidating information gathered from various Web sites. Another form of cookie sharing is achieved by multiple cookie creators partnering to share one Web site. Cookies can be sent to a user from a domain other than the site the user visited. For example, an advertising
agency could post its clients’ banner ads from a central server and include cookies to track the activities of users receiving the ad. The user is unlikely to know what site created the cookie and therefore less likely to know the intended use of the user profile obtained.

**Technical Failure.** Internet content may be at risk due to technical failure including device defects, loss of network integrity and availability, misdelivery of e-mail messages or files, and password protection loopholes. In managing resources, an internal system administrator can, for example, monitor employees’ files or e-mail, as was the case at Epson America, Inc. This interception was by an internal employee, but the content examined could be outside of the employee’s realm of responsibility. Similarly, an ISP can intercept communications without liability as long as it is necessary to provide services or to protect property — again relinquishing content, but this time to someone external to the organization. Message delivery misdirection resulting from a technical glitch may also reveal content to unintended recipients.

**Internal Threats to Online Organizations**
Those within an organization, including consultants and employees, may inadvertently or intentionally cause their employer shared liability for their actions. The most common concerns for liability on the Internet are copyright infringement, pornography, and defamation. We consider a wider array including copyright infringement; defamation and libel; discrimination; harassment; hostile work environment; obscenity; pornography; invasion of privacy; violations of securities laws; and violations of trademark and trade secret laws. Although these areas illustrate potential liability on the part of employers for employee Internet activities in the workplace, the legal precedents regulating this arena are still evolving.

**Copyright Infringement.** The copyright laws of the United States, intended to balance the rights of users and creators, include protection of the various materials found on the Internet. The ease with which electronic material can be copied has resulted in a rapid increase in copyright infringement on the Internet. Copyright infringement committed by an employee may result in employer liability, even if the employer did not perform the copying or distributing.

Employer liability can result from what may seem to be innocent activities. An employee may have brought in an individually licensed copy of software from home, copied software from the Web, or cut and pasted clipart from other Web sites. For example, the webmaster of the National Association of Fire Equipment Distributors used copyrighted clipart, obtained from three CD-ROM volumes, to decorate the trade organization’s Web site. In the ensuing lawsuit, *Marobie–Fl. Inc. d/b/a Galactic*
Software v. National Association of Fire Equipment Distributors et al., the trade organization was held liable for copyright infringement. The bottom line is that if an employer has possession of improperly obtained materials for which valid purchase receipts cannot be provided, it may be charged with copyright infringement.

**Defamation and Libel.** The various forms of Internet communication have given rise to employee cybersmearing or cyberventing, the virtual equivalent of casual conversations around the water cooler. Unwitting or disgruntled employees have utilized bulletin boards, chat rooms, e-mail, and Web sites to anonymously vent opinions, concerns, frustration, or anger about the workplace. For most large companies, at least one Web site is available; while for others, such as Microsoft, there are several.

The common law tort of defamation is intended to protect an individual’s interest in his own reputation. Defamation can be difficult to prove for a public company. Postings must contain false statements, not only an opinion, must be made knowingly and recklessly, and must hurt the company. In what has been described as a case of cyberventing gone too far, a former engineer of Intel Corp. created a Web site as a critical forum for a group called Former and Current Employees of Intel. Intel has not filed a defamation charge for the site. Rather, a restraining order was placed against the former employee in response to unsolicited mass e-mails sent to as many as 30,000 Intel employees. Intel chose to effectively cease the offender’s activities rather than pursue a lengthy case, drawing more attention to that which they sought to stop.

Frequently, the intent of a lawsuit is not about defamation, but rather to reveal the names of anonymous detractors. For example, the Raytheon Co. suspected that postings to a Yahoo! finance message board were made by an employee. In the ensuing lawsuit, Raytheon obtained subpoenas against Yahoo! and other Internet services to learn the identity of all 21 aliases, most of whom were employees, and then dismissed the suit. Four employees subsequently resigned; others entered corporate counseling.

**Discrimination, Harassment, Hostile Work Environment, Obscenity, and Pornography.** According to the Communications Decency Act of 1996, employers are not liable for obscene or harassing use of electronic telecommunications by their employees unless the conduct is within the scope of employment and the employer (1) had knowledge of, and authorized, the conduct or (2) recklessly disregarded the conduct. Under harassment law, an employee may sue for damages based on a “hostile environment,” a vague term including an array of offensive elements, such as jokes, chat, pinups, images, and even co-workers gathered around a screen making sexist or racially insensitive remarks.

Unfortunately, instances of such Internet abuse abound in the workplace. For example, two African-American employees of Morgan Stanley
Dean Witter filed a $36 million class action suit, later settled, claiming they suffered emotional and physical stress from e-mail messages containing racist jokes. Four female employees received a settlement of $2.2 million from Chevron Corporation for sexually harassing e-mail. Compaq Computer Corp. fired 20 employees after they downloaded sexually explicit images from Web sites, logging over 1000 hits apiece, and distributed the images via e-mail. The New York Times Co. fired 23 employees for distributing pornographic images through e-mail.

**Invasion of Employee Privacy.** Employers bear the responsibility for managing organizational resources appropriately. In response, increasing numbers of organizations are monitoring Internet activities. Among the reasons for monitoring are reduced employee productivity, decreased bandwidth, corporate espionage, and legal liability. Nearly three quarters of major United States companies responding to a survey review some form of their employees’ communications including Internet connections, e-mail, computer files, or telephone calls. Of all surveillance methods, Internet and e-mail monitoring have seen the most explosive growth, with 54.1 percent of companies now monitoring employees’ Internet connections and 38.1 percent reviewing e-mail messages. However, these actions may conflict with legitimate employee privacy expectations in the workplace.

**Violations of Securities Laws.** Provisions of the Securities Exchange Act (SEC) of 1934 prohibit the manipulation of stock prices through false or misleading communications. With respect to the Internet, the SEC has taken action in cases of phony Internet message board postings. One incident was perpetrated anonymously by an employee of a publicly traded company, PairGain, targeted in his hyperlink posted to a Yahoo! finance message board. The link, which stated, “BUYOUT NEWS!!! ECILF is buying PAIR ... Just found it on Bloomberg ...”, presented an authentic-looking spoof of Bloomberg L.P.’s news site. The stock price of PairGain rose nearly 31 percent before the markets settled. PairGain cooperated fully during the investigation and was never implicated. Nonetheless, the company was subjected to the disruption of the investigation and was undoubtedly concerned about potential liabilities.

Additional concerns include inaccurate disclosures made unwittingly by employees of public companies participating in Internet-based discussions. Such statements, albeit inadvertent, violate the general antifraud provisions of the Securities Exchange Act.

**Violations of Trademark and Trade Secret Laws.** Similar to copyright infringement, employers may also be held liable for its employees’ violations of trademark and trade secret laws. If an employee were to post the trademark of another organization on his employer’s Web site and,
when informed, the employer did not take action to correct the infringement, the employer may be held liable. The same rationale applies to an employee’s misuse of trade secrets. If an employee used the employer’s resources to obtain another organization’s proprietary information, such as a customer list or software code, the employer may be liable.

**Loss of Employee Productivity and Internet Resource Use.** For some companies, the concern is not what their employees are doing on the Internet, but rather the time they spend. For example, at Xerox-PARC, 40 employees were fired for spending as much as eight hours a day visiting inappropriate Web sites. Ernst & Young reported some firms calculated that more than 80 percent of their Internet capacity was used to access non-business-related Web sites. To gain insight into workplace surfing, a survey revealed only 9.6 percent of respondents never surf non-work-related sites, while 12.6 percent admitted surfing over two hours. Employee Web surfing can represent lost productivity, especially when coupled with non-work-related e-mails. About half (51.5 percent) of respondents to the same survey reported receiving 1–5 non-work-related e-mails, on average, during the workday. Over half (56.3 percent) send 1–5 e-mails. Together, these activities could represent an estimated cost of $9,600 per employee per year, as shown in Exhibit 3.

### Exhibit 3 — Potential Losses Resulting from Decreased Employee Productivity

<table>
<thead>
<tr>
<th>Factors</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of hours per day each employee spends on personal business</td>
<td>1</td>
</tr>
<tr>
<td>Number of work days per year</td>
<td>240</td>
</tr>
<tr>
<td>Average hourly rate including overhead expenses</td>
<td>$40</td>
</tr>
<tr>
<td>Annual cost of lost productivity per employee</td>
<td>$9,600</td>
</tr>
</tbody>
</table>


**STRATEGIC RESPONSE: THE EXPANDED ROLE OF CHIEF PRIVACY AND INTEGRITY OFFICER**

It is evident that as more people gain access to the Internet, the numerous potential cyberliabilities confronting online organizations will continue to increase. The burden of repercussions from misuse is placed squarely on organizations, which hold the ultimate responsibility for use of organizational resources by their employees. Interestingly, liability may even extend to inadequate site security, resulting in unwitting participation in Internet abuses such as DDoS attacks as previously discussed.
In response, organizations may place the responsibility of overseeing Internet activity on the existing legal department or on one or more chosen individuals, depending on the responsibilities to be assumed. A survey of 66 Fortune 500 companies with CPOs, conducted by PriceWaterhouseCoopers, found the CPO to be part of the legal department in 50 percent of the surveyed companies. Only 8 percent reported the formation of a separate privacy department headed by the CPO.

In order to effectively coordinate proactive and reactive organization-wide action to potential consequences, we recommend expanding the role of the existing CPO to include Internet integrity. Responsibilities would be expanded from focusing on consumer privacy to ensuring the integrity of (1) Internet content, including Web sites, files, e-mail, and communications, and (2) Internet use, including the direct activities of internal sources and the consequences of external sources. Thus, this emergent role would more appropriately be titled Chief Privacy and Integrity Officer (CPIO) to protect organizational resources while maximizing the use of the Internet. Based on the reported areas of responsibility of existing CPOs, none currently include this proposed expansion of responsibilities from a focus on privacy issues to the broadened perspective of Internet integrity. Certainly this expanded set of responsibilities should be accompanied by an expanded set of qualifications. A legal specialization in consumer privacy would be necessary to ensure organizational adherence to government regulations, industry self-regulation, and organizational initiatives associated with consumer privacy. Proactively attending to the broad spectrum of Internet activities and potential unintended consequences requires both an expanded legal background, including online content liability and the interpretation of laws and regulations as applied to the Internet, and an extensive technical understanding to minimize the occurrence of threatening Internet activities.

Specifically, the newly defined CPIO would be responsible for formulating or reformulating an expressed Internet use policy, undertaking ongoing training and other means to maintain awareness of issues, monitoring internal sources, implementing defenses against external sources, and securing adequate liability insurance. The effectiveness of this new role in overseeing these responsibilities would be determined by assessing current operations, implementing proactive measures to reduce potential misuse, and continuously keeping abreast of technological advances, legislative and regulatory initiatives, and new areas of vulnerability.

Internet Use Policy
The Internet use policy should clearly state what is acceptable and unacceptable use of specific Internet technologies, by whom, at what times, for what duration, and for what purposes. Details about personal use, prohibited use, and access to prohibited materials should be comprehensively
stated. Privacy rights, if any, for allowable personal use should be defined to clarify employee expectations. The various types of use prohibited under all circumstances should be enumerated, such as criminal, disruptive, offensive, harassing, or otherwise unethical use. Access to prohibited materials such as that which is copyrighted, licensed, other intellectual property, sensitive company materials, or otherwise illegal should be explicitly condemned. Procedures for identifying violations must be communicated. The consequences of policy violations should be stated.

Training
The development of a formal Internet use policy can promote improved use, especially if reinforced by communicating that policy and conducting education, training, and retraining sessions. Other means to maintain awareness of issues may be employed, such as presenting the Internet use policy each time an employee logs in or presenting a pop-up reminder when certain system facilities are accessed. Employee awareness of appropriate Internet use could thereby be kept up to date, even as technological advances and associated new means of abuse occur.

Monitoring Internal Sources
Since it is the employer who is held responsible for employee abuse of the Internet, monitoring or reserving the right to monitor is a necessary means to appropriately manage resources. Generally, United States federal law allows employee monitoring for business purposes if the employees have been made aware of the extent of monitoring. However, in implementing monitoring programs, applicable statutory, regulatory, and common law requirements intended to protect employees’ privacy interests must be considered. If undertaken, such monitoring may reveal the need for filtering software to block employee access to inappropriate Web sites, chat rooms, message boards, and Usenet news groups.

Defenses against External Sources
Automated defenses should be employed against external sources, such as intrusion detection systems, firewalls, virus protection programs, security patches for operating systems, and encryption and authentication products. Procedures to update these defenses should be established to minimize the adverse effect of technological advances rendering current versions obsolete.

Liability Insurance
Organizations may reduce financial exposure of liability by purchasing insurance. Among the most costly and common risks to online organizations are business interruptions caused by hackers, viruses, and internal
CONCLUSION

With the increase in Internet-related business activities, organizations are confronted with a multitude of new risks resulting from both external and internal sources of threats. In light of the potential for adverse impacts on companies, it is imperative that a coordinated and comprehensive response be formulated. The creation of the CPO has already been done within major organizations. However, the organizational risks extend well beyond privacy concerns. The scope of responsibilities must be broadened to include Internet integrity issues. Therefore, we propose that the CPO position should be expanded, becoming the Chief Privacy and Integrity Officer. Organizations will thereby be enabled to more comprehensively protect themselves, their customers, and their business partners as the use and reliance on the Internet continues to grow.

References