
Table of Contents

Introduction	1
Chapter 1	Hiring Employees to Support Technology 5
	Wanted: Technology Guru Willing to Work Long Hours for Low Pay 5
	Filling Regular Staff Positions 6
	Retaining Information Age Talent 6
	Considering Contractors 7
	Keep a Backup 8
Chapter 2	Managing Employment Practices in a Wired World 9
	Preventing Employee Misuse of Technology 11
	Employer Responsibility for Online Communication 12
	Employer Responsibility for Illegal Conduct 13
	Employer Responsibility for Costly Telephone Use 13
	Monitoring Employee Communications 16
	Telecommuting: Balancing Risk and Reward 17
	Suggested Components of a Telework Policy 19
	Goals for a Technology Policy 22
	Technology Policy Elements 22
Chapter 3	Securing Shifting Sands 25
	The Day the Computers Died: Managing Equipment Vulnerability 25
	The Technology Security Toolbox 26
	“It Was Here a Minute Ago” 34
	Disaster Drills 35
Chapter 4	Making Net Gains 37
	Web Functionality and Security 37
	Web Content 41
	Fundraising on the Web 48
	Web-based Advertising 52
	Protecting Your Reputation in Cyberspace 55
	Web Accessibility 56
Chapter 5	Clarifying Privacy and Confidentiality 59
	Employees 60
	Clients 60
	Web Privacy 61
	Web Cookies 65
Chapter 6	Managing Change in a Technological Setting 67
	Technological Changes 70
	Business Process Changes 72
	Human and Cultural Changes 74
Chapter 7	Tracking Software Ownership 75
	Staying Legal – Using Software Appropriately 75
	Big Brother, Big Business 76

Chapter 8	Selecting and Managing Vendors	79
	Choosing With Whom to Do Business and How	79
	Managing Vendor Contracts	81
Chapter 9	Protecting Children on the Internet	85
	Tools for Managing the Risks of Internet Access	86
	If Your Web Site Attracts Young Visitors	88
	Developing an Acceptable Use Policy for Clients	88
Chapter 10	Insuring Bits and Bytes	91
	Property Coverage	91
	Liability Coverage	96
Epilogue	107
A Short Glossary	109
Bibliography	113
Resources	117

Sample Policies

Wireless Communications Device Policy, Sample #1	14
Wireless Communications Device Policy, Sample #2	15
Office Technology and Privacy Policy	24
Web Site Disclaimer and Notice of Proprietary Information	43
Policy Concerning Web Links	47
Web Links Disclaimer	48
Statement on Web Security	63
Web Site Privacy Statement	64
Tips for Internet Safety and Good Manners	87
Norfolk Public Schools - Internet Access Agreement	90

Sidebars

The 10 Commandments of Computer Ethics	3
Tap Recent Grads	6
Netiquette: Be Nice on the Net	12
Danger in the Rough Surf: Cyberpiracy	40
Web Content Accessibility Guidelines	58
Developing a Web Privacy Policy	63
Should I Upgrade?	68
Software Licenses	76

Introduction

The nonprofit sector has come a long way technologically speaking in what seems like a matter of minutes. It wasn't long ago that nonprofit executive directors were coveting laser printers and Pentium-class personal computers and bemoaning the lack of Zip drives and the inability to view some sites on the Web due to antiquated systems. The CPUs we routinely see discarded in office hallways or on city sidewalks were once workhorse computer components we depended on to generate mail-merge fund-raising letters and other essential by-products of charitable business.

The days when a typewriter with a built-in correcting ribbon was considered the "most valuable piece of equipment" in a nonprofit office are a distant memory. In fact, the youngest generation of nonprofit employees has never had the opportunity to use these antiques. They have been using computers — in the classroom and at home — since childhood. The focus has turned to the nuances of e-commerce functions on a nonprofit's Web site, electronic filing of informational tax returns, and achieving a 21st century nirvana: the automated nonprofit office.

Nonprofits are harnessing technology in creative ways that, not surprisingly, mirror uses in the business world. They are creating new products and charitable services delivered entirely online and using technology to improve efficiency and the overall management of precious resources. For their private sector counterparts, both uses would logically lead to the creation of wealth for individuals. In the nonprofit sector, these activities have the potential to create stronger communities — the very environs served by a nonprofit's beneficial mission-focused programming.

The lure of new and emerging business technology is intoxicating. The ability to send an e-mail announcement or fund-raising appeal in a matter of seconds to thousands of prospective supporters opens new opportunities for productivity and redistribution of scarce resources in the development office. The willingness of private businesses to donate equipment — from high speed PCs to handheld personal digital assistants or PDAs — puts technology within the reach of even the smallest charity. But along with the tremendous benefits of technology — time saved, content enhanced, and greater efficiency — comes an array of risks. Given technology's nature and the speed with which new

technology can be integrated in a nonprofit, many related risks may go unnoticed by the individuals involved in identifying and managing more traditional risks, such as the risk of child abuse in a youth-serving organization. While managers in a nonprofit might easily envision the risk of a child suffering an injury on a camping trip, they might have greater difficulty recognizing the risk of destruction of the office file server or inadvertent release of computer-stored confidential client information. Not enough attention has been paid to the legal and operational risks associated with technology, such as the risks of losing technology access altogether, liability for unrelated business income tax from advertisements on a Web site or responsibility for harm caused by employee misuse of equipment.

Just as there appears to be no limit as to how technology will change our daily lives, there may be no visible ceiling on the range of risks facing an organization that relies on technology. Ironically, as computer technology complexity accelerates at lightning speed, eclipsed only by the charitable world's increasing dependence on computers, the average user's understanding of exactly how these vital systems work has been left in the dust. The need for a specialist or two to guide the use and management of technological resources can only grow over the next decades. These specialists must master the technology that arrived yesterday and stay attuned to changes, opportunities and risks that may be barely visible on tomorrow's horizon.

The Nonprofit Risk Management Center advocates a thoughtful, methodical approach to managing technology risks. Every organization should take the time to consider how technology risks could prevent the nonprofit from achieving its mission. The ultimate goal of risk management in a nonprofit is to free up resources for mission-critical activities. Rather than shying away from technology due to fear about the associated risks, we urge nonprofit leaders to embrace risk-taking on the technological frontier. But before you blast off, take some time to review available road maps, consider what dangers may lie ahead, and take advantage of the tools and expertise available to increase the odds your venture will be successful.

To assist with this process, we have identified and organized our road map into ten categories of activity or concern. We begin with the topic of employment practices in the information age. In Chapter 1 we explore the topic of recruiting and retaining staff for the information age. For some organizations, the untimely departure of the only person who knows how to back-up the file server and update the Web site is a serious risk. In Chapter 2 we discuss the importance of managing employee use of technology. Although some readers may believe that the most serious or likely threat to the security of a nonprofit's technology comes from outside the organization, the opposite is true. The vast majority of data losses and other risks facing your network and peripherals are from intentional and accidental actions by your employees. In Chapter 3 we delve into the topic of system security. Most readers will have some familiarity with the security features and measures discussed here. Our

intent is to clarify the importance and value of these tools and help you decide how and if they should be integrated into your organization. Chapter 4 addresses the issue of Web sites, covering both Web functionality and Web content concerns. In Chapter 5, we cover the topic of privacy in the information age, in an attempt to help the reader begin to get a handle on the questions — if not the answers — that must be considered as part of an overall effort to manage technology risks. The book continues with chapters on Change Management, Tracking Software Ownership, Managing Technology Vendors and Protecting Children on the Internet. The final chapter of the book covers Insuring Bits and Bytes.

We expect that some readers who are anxious for information on the intersecting issues of risk management and technology will choose to digest this book in the format presented. Other readers will use this text as a reference, reading only those sections of interest at a particular moment.

Our intent is to help you develop a fuller perspective on the range of risks associated with the use and misuse of technology. We also intend to provide practical suggestions for managing a whole host of risks that will help you put your organization on a stronger foundation without consuming vast, or even significant, human or financial resources. In the chapters that follow, we categorize technology risks and opportunities, describe the nature of the risks and suggest an array of practical strategies any nonprofit can adapt to meet its needs.

For information on any of the topics addressed in this book, or technology risks beyond the scope of this book, contact the Nonprofit Risk Management Center at (202) 785-3891 or visit www.nonprofitrisk.org.

The 10 Commandments of Computer Ethics

by the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that insure consideration and respect for your fellow humans.

Computer Ethics Institute
A project of the Brookings Institution

http://www.brook.edu/its/cei/cei_hp.htm