

The Surprising Risks of Counterfeit Software in Business

White Paper

Microsoft Corporation
2009

Summary

In 2006, international market research firm IDC published a paper sponsored by Microsoft about the risks of obtaining and using counterfeit software¹. That study presented the results of IDC's investigation about the security risks associated with obtaining and using pirated software. This White Paper continues that story with the results of a more recent study conducted by Microsoft, explores the prevalence of counterfeit software within midsize business environments, and describes the risks that go hand-in-hand with counterfeit software and other forms of software piracy.

The Business Software Alliance (BSA), a respected industry trade organization, defines software piracy as the unauthorized copying or distribution of copyrighted software. This can be done by copying, downloading, sharing, selling, or installing multiple copies onto personal or work computers. Counterfeit software, also as defined by the BSA, is the illegal duplication and sale of copyrighted material with the intent of directly imitating the copyrighted product. In the case of packaged software, it is common to find counterfeit copies of the CDs or diskettes incorporating the software programs, as well as related packaging, manuals, license agreements, labels, registration cards and security features².

Counterfeit and pirated software is often routinely found in the business environment during licensing reviews. Because software licensing is so important to businesses, they commonly engage in reviews to ensure that licensing remains current and procurement practices are being properly followed. These licensing reviews can be internal or as part of a broader engagement with a software asset management (SAM) partner.

Similarly, when businesses engage with Microsoft for licensing reviews, third-party SAM partners are engaged to facilitate better understanding of Microsoft licensing and to help businesses ensure they have the necessary processes in place to manage software like other fixed assets.

¹ *The Risks of Obtaining and Using Counterfeit Software*, IDC, October 2006

² *Business Software Alliance Web site*, <http://www.bsa.org/>.

Because counterfeit software is so often found in licensing reviews worldwide, Microsoft decided to research a smaller sample and get a more detailed analysis of what was going on in one specific area. In 2007, a study was conducted based on the results of Microsoft license reviews that had occurred with mid-sized business customers in the United Kingdom. The extent of high-quality counterfeit software found within these business environments during the study led to a closer examination of the results, as presented in this White Paper.

The study yielded three primary findings:

1. Of the midsize businesses reviewed during the study, counterfeit software was discovered within a significant portion (37%).
2. All of the counterfeit software found was high-quality, which also points to an increase in sophistication on the part of counterfeiters. Because the businesses had purchased the software in good faith, they were surprised to find that the software was not genuine.
3. Each midsize business found to have counterfeit software in the study spent an average of £7,185 GBP (\$10,222 USD) on these purchases, which in turn provided them with software that was neither licensed nor genuine.

Legal Notice

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft, ActiveX, Internet Explorer, SQL Server, Windows, Windows NT, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Summary	1
Legal Notice.....	3
Introduction.....	5
The Study	7
Review methodology	7
Study findings.....	8
The risks of counterfeit software.....	10
How can businesses protect themselves?	11
Additional resources to help.....	12
Conclusion	12
Appendix A: Previous research and exploring the risks	13
Risks of seeking counterfeit software and ways to bypass product activation.....	13
Risk of identity and information theft	15
Counterfeit software and computer stability.....	15
Appendix B: Examples	17

Introduction

Counterfeit software and other forms of piracy present ever-increasing challenges to consumers and businesses alike which go beyond concerns about licensing compliance. Software piracy is not a new development, but the availability of pirated software over the Internet has its own increased level of risk to consumers and businesses. Because of this, using the Internet to actively seek out ways to download pirated software and then circumvent software activation is inherently more dangerous. Businesses and IT departments that centralize procurement or have standard software asset management (SAM) practices in place can help protect themselves from the risks of counterfeit software.

Microsoft is committed to fighting piracy and reducing the risks of counterfeit software. To do this, Microsoft organizes its investments to fight piracy of Microsoft software within the Genuine Software Initiative (GSI), which focuses on three strategic areas of education, engineering, and enforcement. This includes sponsoring research, assessing the breadth of the impact of software piracy, and working with customers and partners as part of Microsoft's commitment to fight piracy. Additionally, GSI supports third-party research that helps customers to understand the risks that they face from counterfeit software and other forms of piracy.

In 2006, the GSI team worked with IDC to present the results of a study which concluded:

1. The cost of recovering from a single incident of malicious software on a computer was greater than the initial perceived cost savings of using pirated software.
2. Given the security risks, the cost of obtaining and using a pirated or counterfeit copy of Microsoft Windows® or Microsoft® Office can include the cost of one or more service calls to clean the affected computer(s), the loss of data or information on an infected computer that needs to have its hard drive reformatted, and the potentially much larger cost of identity theft.
3. Obtaining and using pirated software can pose a serious IT security risk.

While this IDC study focused mostly on the ways that consumers and small businesses obtain software, the risks of counterfeit software are not limited just to these groups. Midsize businesses, as well as larger businesses or organizations with managed IT resources, need to be vigilant about the findings from the 2006 IDC study because the risks are certainly applicable to businesses of all sizes. In addition, midsize businesses can be exposed to even greater risks, as detailed in Figure 4 of this White Paper.

To research this further, Microsoft recently worked with a number of midsize business customers to determine the extent of counterfeit software in their environments and the impact of using counterfeit software might have on their businesses. This work resulted in three key findings:

1. Of the midsize businesses reviewed during the study, counterfeit software was discovered within a significant portion (37%).
2. All of the counterfeit software found was high-quality, which also points to an increase in sophistication on the part of counterfeiters. Because the businesses had purchased the software in good faith, they were surprised to find that the software was not genuine.
3. Each midsize business found to have counterfeit software in the study spent an average of £7,185 GBP (\$10,222 USD) on these purchases, which in turn provided them with software that was neither licensed nor genuine.

Across all of the midsize businesses surveyed, one consistent theme emerged: When the environments in question were examined for the existence of unlicensed and counterfeit software, the number of environments that had unlicensed or counterfeit software was high, and customers were very surprised to learn the results.

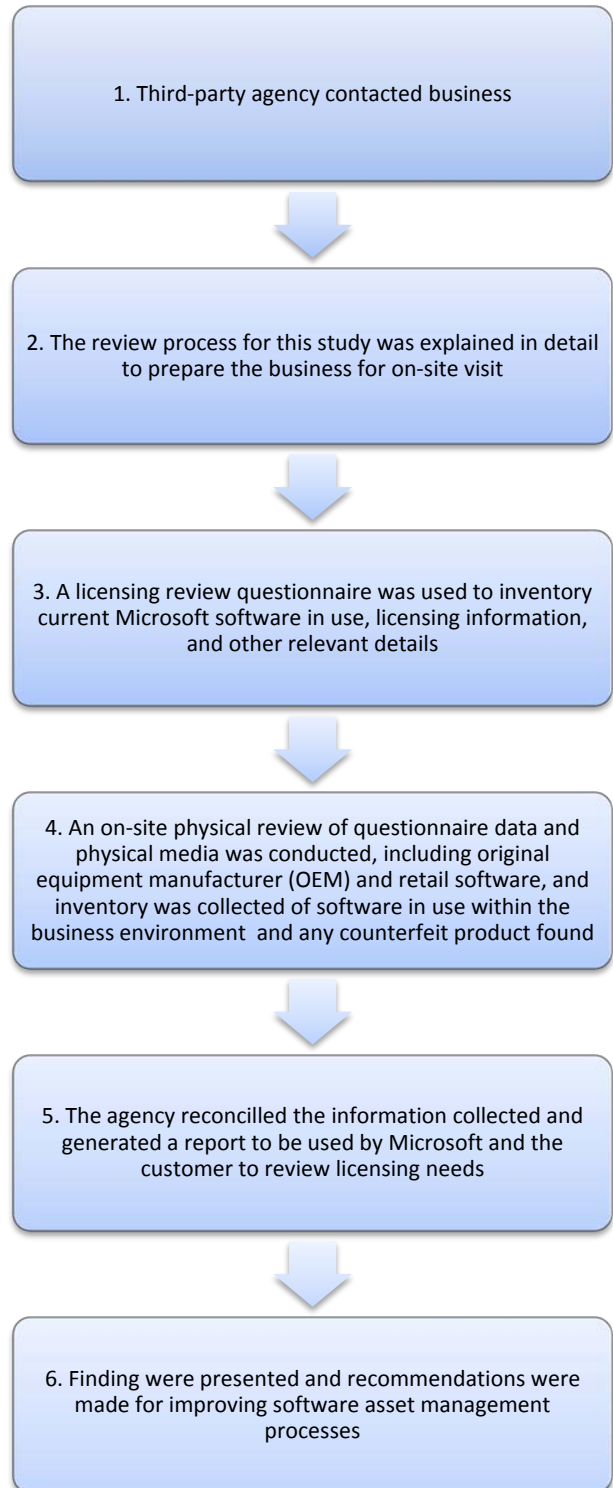
The Study

The goal of the study, which was conducted in the United Kingdom in 2007, was to determine the possible presence and impact of counterfeit software within midsize business computing environments. Each year, thousands of Microsoft-initiated license reviews worldwide are performed by third-party agencies. This particular study was conducted by utilizing existing license reviews within the United Kingdom. Microsoft ensured that the sample used in this study was randomly selected and was comprised of 30 midsize business customers' licensing reviews, including on-site assessments of physical product and licensing information in accordance with the methodology shown in Figure 1. All of the third-party review teams that performed license reviews used in the study have received training from Microsoft for identification of counterfeit software and received assistance in confirming suspected counterfeit directly from Microsoft product identification teams.

Review methodology

During this study, the 30 midsize business customers that underwent on-site reviews of their software inventory and computer environments also were subject to a closer analysis of any counterfeit product found during the review. The study review methodology described in Figure 1 and the resulting reports from the on-site visits formed the foundation of the data gathered as part of this study.

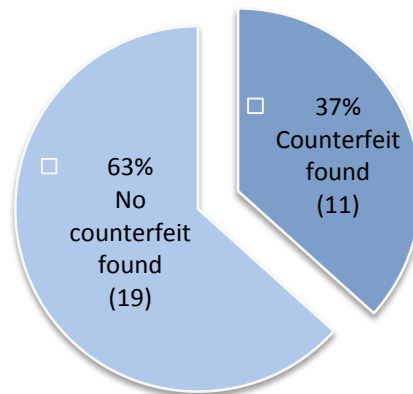
Figure 1 – Study Review Methodology



Study findings

Of the 30 companies reviewed, 11 (37%) were found to have unknowingly purchased counterfeit software, including both Windows and Office. While the sample size was relatively small, the number of individual instances of counterfeit suggests that it's likely high among midsize businesses. This suggests that further research is warranted, and is especially noteworthy as midsize companies with a dedicated IT department often have policies governing procurement of software. Appendix B of this White Paper contains some detailed examples of customer licensing reviews that were not included in this study but further highlight the extent and circumstances of counterfeit software found within midsize business environments.

Figure 2 - Counterfeit Software Found in Random Study Sample



Another study finding is that of the counterfeit software found during the reviews, all of it was high-quality packaged product. Unlike low-quality counterfeit software, which makes no attempt to appear professionally produced or genuine and often consists of a product key and product name written in permanent marker on a CD or DVD, high-quality counterfeit software is software that appears to be professionally produced and attempts to include the piracy prevention features of genuine Microsoft software, such as embedded holograms or interwoven threads.

Information about Microsoft's software piracy prevention features and examples of counterfeit software can be found at Microsoft's [How to Tell](http://www.microsoft.com/howtotell) Web site³, which contains an extensive gallery featuring high-quality, mid-quality, and low-quality counterfeit software and counterfeit

³ Visit <http://www.microsoft.com/howtotell> to learn more about identifying the piracy prevention features of genuine Microsoft software.

packaging examples. In the example shown in Figure 3, a holographic sticker is used in place of the embedded edge-to-edge holograms on the installation media.

Figure 3 – Piracy Prevention Features in Genuine Microsoft Software



In fact, over £79,030 GBP (\$112,439 USD) was spent by midsize businesses on software that was ultimately found to be counterfeit. This means that each of the 11 midsize businesses found to have high-quality counterfeit software in this study spent an average of £7,185 GBP (\$10,222 USD) for non-genuine, unlicensed software, even though they thought they'd already purchased properly-licensed, genuine software. As a result, these businesses ended up having to spend additional money to properly license the software they had purchased.

What the Microsoft study shows is that even professionals can be misled by high-quality counterfeit software. As high-quality counterfeit software continues to become more readily available, the potential for it to enter business environments unintentionally increases. Therefore, it is imperative for IT departments to continually communicate and review the process by which software is procured and deployed within their business computing environments to help protect against the risks of counterfeit.

In addition, Appendix B of this White Paper contains four examples of additional customer license reviews not included in the random selection within the study, including background, history, and more information on counterfeit software found within the specific business environments.

The risks of counterfeit software

As previous research has indicated, counterfeit software poses increasing dangers to customers, including the consequences of non-compliance and software audits for not having proper licensing in place. More importantly, research shows that there are additional risks to business customers, as shown in Figure 4 below.

Figure 4 – Risks of Counterfeit Software

Risk	Description
<i>Data loss and/or increased system instability</i>	In a recent Harrison Group study investigating the impact of unlicensed software on midsize companies ⁴ , it was found that companies using unlicensed and/or counterfeit software were 73% more likely to have loss or damage of sensitive data, and 73% more likely to have critical computer failures lasting 24 hours or more, than those using fully and properly licensed genuine software. In addition, further information is available in Appendix A of this White Paper regarding system instability that can be attributed to the use of non-genuine software.
<i>Identity theft</i>	As outlined in Appendix A of this White Paper, counterfeit software poses a risk of identity theft to private customer and employee information.
<i>Risk to reputation</i>	Companies face potential risks to their reputation from the use of counterfeit software, especially if there is a resulting loss of sensitive customer or employee data.
<i>Financial consequences</i>	Businesses can potentially suffer financial consequences due to data loss and/or system downtime, including any resulting impact to production.
<i>Penalties resulting from under-licensing and/or counterfeit software</i>	In addition to the potential financial consequences listed above, individuals responsible for software procurement, including directors and senior management, can potentially be held liable for penalties resulting from under-licensing if counterfeit or unlicensed software is found. One example of this is the Sarbanes-Oxley Act in the United States ⁵ , which governs the implementation of internal control reporting provisions for businesses.

⁴ [Impact of Unlicensed Software on Mid-Market Companies](#), Harrison Group, September 2008.

⁵ [Sarbanes-Oxley Act of 2002](#), United States Securities and Exchange Commission.

Appendix A of this White Paper also contains more detailed information on the study findings from the 2006 IDC research study, more information on computer instabilities that have been recorded since the initial research, and methods counterfeiters use in an attempt to circumvent product activation (which, in turn, carry additional risks).

How can businesses protect themselves?

As reflected in this study as well as the other past studies referenced, both counterfeit and unlicensed software is a risk to any business' computing environment. Unfortunately, most businesses don't know where to start addressing the problem.

To help protect themselves from the risks of counterfeit software, businesses should:

- 1. Buy genuine software from trustworthy sources.** The best way to purchase software is from an authorized reseller who sells only genuine software. To locate a reputable reseller, businesses can use local resources such as a Chamber of Commerce, the Better Business Bureau, and consumer publications, or find local Microsoft reseller contact information online at Microsoft's [Midsize Business Center](#), [Small Business Center](#), or the [Business & Industry](#) Web sites.
- 2. Learn how to identify counterfeit software.** Microsoft's [How to Tell](#) Web site contains a wealth of information about how to determine whether Microsoft software is genuine, including pre-purchase checklists, product information, and visual examples of Certificates of Authenticity (COAs), installation media, and product packaging, including piracy prevention features.
- 3. Centralize software procurement.** Centralized procurement can help protect an organization's software and help businesses to recognize what they have, where it's running, and any licensing overlap. International financial and reporting requirements, such as Sarbanes-Oxley in the United States, are requiring more stringent requirements in the area of fiscal reporting. Improving the way that licensing information is managed and software is procured, can help businesses know exactly what's in their computing environments, creates the opportunity to regularly review that information to help protect against risk and liability, and increases opportunity for cost-savings. One example of improving software procurement and licensing information management is conducted through Software Asset Management (SAM), as discussed earlier in this White Paper. [Learn more](#) about the top 10 reasons to implement a SAM program.

Additional resources to help

The following Web sites also provide additional useful information:

- [Genuine Microsoft Software](#): By using genuine Microsoft software, businesses can be confident that their software is legitimate and fully supported by Microsoft.
- [Piracy](#): Businesses can help protect themselves from the risks of software piracy with helpful tips on how to identify counterfeit software or other misuse of software.
- [Microsoft SAM](#). The Microsoft SAM site contains an overview of SAM, its benefits, and a listing of partners that are available to help implement best practices.
- [Microsoft Software Assurance \(SA\)](#): SA combines the latest software with phone support available 24 hours a day, partner services, training, and IT tools that help businesses deploy, manage, and migrate software.

Conclusion

As evidenced during this study, as well as from previous research, counterfeit software and other forms of software piracy can be found in and pose serious risks to businesses of all sizes. Because counterfeit software was found in one in three businesses in this study, and because all of the counterfeit software found was of high-quality, it's understandable that the study participants were surprised by the findings. In addition, the businesses involved in the study that were found to have purchased high-quality counterfeit software had to spend additional money in order to properly license their software.

As counterfeiting increases in sophistication, the likelihood for it to enter business environments unintentionally increases. Therefore, businesses must remain vigilant to help protect their computing environments from the risks of counterfeit software by purchasing genuine software from trustworthy sources, understanding how to identify counterfeit software and implementing procurement practices. By taking advantage of Microsoft's anti-piracy resources and increasing awareness of what's entering their business environments, businesses can help to eliminate any surprises during the procurement process, and, more importantly, help to protect themselves from the risks associated with counterfeit software.

Appendix A: Previous research and exploring the risks

In the initial 2006 study to assess the risks of obtaining and using pirated software, IDC investigated whether visiting the Web sites offering tools and techniques for using pirated software and downloading and using key generators and activation exploits would expose users to malicious or potentially unwanted software. IDC set up a testing lab within its own IT department and ran tests on Web sites offering pirated or counterfeit software, key generators, or activation exploits for two weeks in August 2006. The latest versions of commercially available anti-malware software were used to identify malicious and potentially unwanted software. The security team at Microsoft then added to the research by actually downloading key generators and activation exploits from both the Web sites IDC analyzed and from peer-to-peer networks.

Risks of seeking counterfeit software and ways to bypass product activation

In addition to the risks of using counterfeit software within a business environment, there is additional danger in the act of finding pirated software to install. This is especially true for activation exploits, which are programs used to circumvent or bypass product activation.

During the 2006 research study, IDC found and tested 98 unique Web sites offering access to counterfeit product keys, pirated software, key generators, and other activation exploits for Windows XP and Office; about one-fourth of these sites hosted malicious or potentially unwanted software. In some cases, the Web sites visited tried to install the unwanted software automatically upon visiting the site. In other cases, the user was required to take manual action, such as receiving a prompt to install an ActiveX® control that ultimately resulted in the installation of malicious or unwanted software.

Following the initial IDC research, we have continued to see more activation exploits, and some have been discovered to contain malicious code. When a user installs an activation exploit, any code that might be within that program is installed, including viruses, malware, adware, and Trojans. Some examples of how this can happen are listed in Figure 5.

Figure 5 – Malicious Software and Activation Exploits

1 - Downloaded software containing malware

- **What is it?** This is downloaded software that claims to circumvent or bypass product activation. It is a backdoor application that does not even try to bypass activation, but opens the user's computer to attacks from remote computers.
- **What does it do?** The download contains three files. One is an mp3 file, one is a text readme file that advises users to ignore anti-virus program warnings which say the program is malware, and another executable file that purportedly bypasses activation of Windows. In actuality, the program does not even attempt to bypass activation or touch any activation-related files or registry keys. Instead, the malware modifies the system state by adding registry keys and injecting code in the system processes, thereby opening up the computer to access by remote attackers. This access could potentially allow an attacker to manipulate files or registry data, log keystrokes, capture screens, or manage running processes on an affected machine.

2 - Downloaded software containing adware

- **What is it?** This is downloaded software that claims to circumvent or bypass product activation. It also contains adware, which is software that displays advertising or downloads advertisements to a computer after it is downloaded.
- **What does it do?** Even though this particular activation exploit is advertised to circumvent or bypass product activation for Windows Vista®, it doesn't. Instead, this is simply adware that advertises itself as a popular activation exploit. Once downloaded and executed, the program advertises a download site and creates files within a system directory, but does not circumvent or bypass activation of the software.

3 - CDs/DVDs containing malware

- **What is it?** Some installation CDs or DVDs for software programs that are counterfeit contain activation exploits but also include Trojans, malware, spyware, or worms.
- **What does it do?** One example in particular has an application within the DVD that claims to activate Windows Vista. However, instead of activating the product, it attempts to steal personal data and send the information to an FTP server.

4 - Downloaded software containing a Trojan

- **What is it?** In a recently publicized incident, an anti-virus software maker issued an alert to warn Mac users not to download Apple iWork '09 installers from sites offering pirated software. Although the software in this particular package is complete and functional, the installer contains an additional installation package with a type of malware called a Trojan.
- **What does it do?** After the user begins the installation of the software, the installer for the Trojan is launched and eventually connects to a remote server over the Internet. Because the user is asked to enter an administrator password during installation, this means that a remote user or users will have the ability to connect to the infected computer and access data or perform remote actions on that computer.

Although the software found during this recent Microsoft study was found to be free of malicious code including malware, we have seen an alarming level of sophistication on the part of counterfeiters. This sophistication results in repackaged counterfeit versions of software that are made to look genuine and can easily fool those who are unfamiliar with how to tell the difference. Because we have seen many examples of low- and mid-quality counterfeit with malware, it is reasonable to expect that counterfeiters will eventually start to distribute high-quality product containing malicious software.

Risk of identity and information theft

During acquisition of counterfeit or pirated software (which includes activation exploits), users can be exposed to critical security threats and identity theft. We have also seen examples of credit card theft following online software purchases that later turned out to be counterfeit.

In one recent United States Department of Justice (USDOJ) case⁶, an Oregon man was sentenced to four years in prison for selling counterfeit software with a retail value of more than \$1 million USD, aggravated identity theft, and mail fraud. During a two-year span, the man used thousands of online auctions to sell copies of counterfeit software. He further admitted to stealing individuals' personal information through the use of a computer keystroke logger program, which was bundled within the counterfeit software, installed itself on victims' computers, recorded the victim's name and bank account information, and sent it over the Internet to be used in setting up online payment accounts.

Because of increased use of the Internet by employees while at the office, businesses' critical information may also be at risk from the act of seeking out pirated or counterfeit software, including financial and banking data, confidential product information, and employees' personal information. Counterfeit software and piracy in the business environment also has the potential to cause losses in revenue and customer base as a result.

Counterfeit software and computer stability

Since the launch of Windows Vista®, we have seen a variety of potentially damaging activation exploits that are a direct result of efforts by counterfeiters. Attempts to circumvent product activation for Windows Vista have resulted in more than one million reported crashes since the launch of the product. Because activation exploits attempt to modify key system components of Windows, and because crashes from counterfeit software often go unreported, the total number of crashes from activation exploits is likely much higher.

One important aspect of computer crashes relative to the business environment is data loss. Counterfeit software is likely to cause computer performance problems and crashes, which may result in data loss. Other related problems include downtime, lost revenue, and customer

⁶ [United States Department of Justice Press Release](#), July 23, 2008

dissatisfaction. In the Harrison Group study, it was found that companies using unlicensed software have failures more frequently, which could lead to lost critical data and employee downtime. In addition to the increased likelihood of critical computer failures mentioned earlier in this paper, it was also found that businesses were 28% more likely to experience a loss of sensitive data, including customers' personal information, from the use of unlicensed and/or counterfeit software.

Appendix B: Examples

Microsoft's account teams work with customers on a daily basis to help them better understand their software licensing and purchasing options. A key part of this understanding is an evaluation of their current environment, including an inventory of existing software licenses. The customers in the examples below each had their environments evaluated in order to better understand their software licensing and business computing environment. Several license reviews of midsize businesses that were not part of the random selection used in the study were included as individual examples, in order to further highlight the extent and circumstances of counterfeit software found within midsize business environments.

The total valuation of counterfeit discovered within these four examples was in excess of £1,174,000 GBP (\$1,669,434 USD).

Example 1 – Professional Services Firm

The Microsoft team, working with an independent third-party, helped a large UK professional services firm analyze the extent of counterfeit software within their environment. The company has an established network of over 100 offices covering the entire UK; with in excess of 1300 desktops, 150 Windows servers and 140 SQL servers.

In total, over 2000 units of high-quality counterfeit product were identified, including End User License Agreements (EULAs), License Paks, Client Access Licenses (CALs), and COA labels for Office Professional Edition, Windows NT® Server 4.0, SQL Server® 2000, Windows Server ®2000, Windows 2000 Professional Edition, and Windows XP Professional Edition. These items were valued at over £600,000 GBP (\$853,293 USD).

Example 2 – Telecommunications Company

A third-party licensing review was conducted for an established telecommunications company in the UK. The company's business computing environment contains over 600 desktops.

During the license review, over 550 units of high-quality counterfeit product were identified, including copies of Office 2000 Professional Edition, Windows 98 Second Edition, Windows 2000 Professional Edition, Windows XP Professional Edition, and Windows Server 2000. These items were valued at over £130,000 GBP (\$184,880 USD).

Example 3 – Legal Firm

A third-party license review was conducted for a large legal services firm with offices across the UK and more than 750 employees.

During the license review process, the team uncovered over 600 counterfeit units, including Office Professional Edition EULAs and Office 97 Professional Edition License Paks. These items were valued at over £260,000 GBP (\$369,789 USD).

Example 4 – Manufacturing Industry

The Microsoft team assisted a customer from the manufacturing sector who had independently chosen to undergo a licensing review using a SAM partner of their choice. The company is a subsidiary of a multi-national corporation.

During the initial stages of the SAM review process, the customer contacted Microsoft for assistance after concerns about authenticity were raised by their SAM partner. With the onsite support of the Microsoft Product Identification Team, over 400 counterfeit units were uncovered, including copies of Office 2000 Professional Edition and Office 97 Professional Edition. These items were valued at over £184,000 GBP (\$261,697 USD).