Information Systems Misuse - Threats & Countermeasures

By Vijay Gawde, CISSP, NCSA, CCNA, MCSE

In today's world, use of information systems has become mandatory for businesses to perform the day to day functions efficiently. Use of Desktop PC's, Laptops, network connectivity including Internet, email is as essential as telephone at workplace. The employees and networked information systems are most valuable assets for any organization. The misuse of Information Systems by employees however poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Organizations need effective countermeasures to enforce its appropriate usage policies and minimize its losses & increase productivity. This paper discusses some of the issues related to Information System misuse, resulting threats and countermeasures

Desktop Dangers

The shift of corporate computing focus from centralized to decentralized, distributed, network computing coupled with drop in hardware prices has empowered the desktop computers with fast processors, more memory, high capacity disks and peripherals such as CD-ROM/Writers. Significant amount of organization's intellectual property now resides on employee's computers. With highly user friendly operating systems such as Microsoft Windows, employees can now easily install software on their office computers from CDs, listen to music, watch videos, play games, store personal data, execute applications that may be inappropriate for business. The paradigm shift to powerful networked desktops necessitates organizations to enforce policy based controls such as defining organizational standard configurations for these workstations that are restrictive enough to curb risk while non-restrictive enough to support vital business functions.

Few years back, web browser was the only tool available to access internet. Today employees can use new breed of applications such as real-time streaming media players, instant messaging (IM) clients and peer-to-peer (P2P) networks over the internet. The use of applications like P2P can have a very little, if any business justification. Chat, Online Purchase, interactive games, gambling, pornography, surfing non business related sites such as sports, entertainment, web based personal email and even searching another job etc. are major contributors to losses organizations suffer due to misuse of corporate desktops. In addition to being potential productivity drainer, corporate desktops can relay company confidential information through instant messaging or emails rapidly over the Internet exposing organizations to legal liabilities.

Following calculation depicts a conservative example of productivity loss suffered by typical organization

Hourly Employee Cost	Daily Misuse (Hours)	Daily Loss Per Employee	Weekly Loss Per Employee	Annual Loss Per Employee
$25	1	1x$25=$25	5x$25=$125	52x$125=$6500

- *It takes only about 150 employees for a company to loose a million dollars annually.*

Security Breaches

Information systems and networks are often inherently insecure because they are designed with functionality not security as its primary goal. Most organizations view security threats as inbound i.e. from outside to inside. However there are major threats to security that are not introduced from external sources but by employees themselves. It is important that organizations understand the inside threats and extend perimeter security controls to local desktops with security measures such as host based intrusion detection system, personal firewall, Antivirus software. With easy availability of hacking tools, motivated employees can find ingenious ways of unauthorized access to corporate confidential data. Security breaches can even happen due to accidental risk of attaching wrong files in email attachment or sending email to wrong recipient. Social engineering attacks can trick legitimate, though naïve users into providing them with access to corporate systems. Sharing folders on a PC, choosing weak passwords, sharing passwords, leaving important printouts on desk, not locking the screens are some of the examples of lack of sense of security, due care and diligence. Whether incidents are due to malicious intent or inadvertent employee error, the result is the same; loss of revenue, productivity and potential liability.

Bandwidth Bandwagon:

Bandwidth is never enough! Banner advertisements, streaming media, MP3 downloads; P2P file sharing are bandwidth guzzlers that place increasing demands on organization’s network resources. While some of the network traffic is easy to classify as non-critical to business much of it including streaming media may or may not be work-related. Internet management policies that block all bandwidth intensive applications at corporate firewall may be counter productive. Organizations need a tool to manage the available bandwidth to be distributed according to organizational preferences and policies, optimize network performance for business applications or else it could lead to a situation where few of the employees watching streaming videos and listening to online music while its CEO is struggling to access critical business webcast.

Legal Battle:

Transfer or display of sexually explicit content via office computer can create hostile work environment. Companies can be held accountable when their employees use the Internet appropriately such as forwarding offensive message. Most employees don’t know that their employers are legally liable for damages related to the electronic distribution of offensive material in the workplace. Internet threats such as malicious code, Trojans, spyware, could make desktop vulnerable to leakage of important corporate information. Installation and use of illegal software by an employee can make corporate pay legal damages. Privacy Laws in many countries make it essential that organization control employee behavior and misuse of its information assets.

Table 1.0 – Internet Misuse Statistics

Misuse	Description
General	• 30% of web surfing is not work related. (*IDC Study*)
Hacking	• 75% of the companies cited employee as a likely source of hacking attacks. While 45% of business had reported unauthorized access by insiders. *(CSI/FBI Computer Crime and Security Survey, 2003)*
IM	• There are more than 43 million users misuse IM at workplace *(IDC, 2003)*
P2P	• 45% of the executable files downloaded through popular P2P network Kazaa contain malicious code *(TrueSecure, 2004)*
Legal	• A company can be liable to $150k per pirated work for allowing employees to use company network to download copyrighted material *(RIAA, 2003)* • 27% of fortune 500 companies have battled sexual harassment claims stemming from employee misuse. *(American Management Association)*
Porn	• 70% of the pornography is downloaded between 9am to 5pm *(SexTracker)*
Spyware	• 30% of the companies have detected spyware on their network *(Websense UK survey, 2003)*
Streaming Media	• 77% of online listening to Internet Radio on week days takes place between 9am to 5pm, pacific time *(Arbitron, 2004)* • 44% of corporate employees actively use streaming media. *(NielsenNetRatings)*

COUNTERMEASURES:

First Step - Acceptable Use Policy

Organizations need to develop acceptable use policy for desktop usage that must emphasize on what is appropriate and what is inappropriate usage like what kind of applications users can run, what kind of data they can store, what can they surf on Internet, what type of activity is strictly forbidden, what consequences will result if the policy is violated. Employers must make sure that their staff understands not only the rules,, but also the rationale behind the Acceptable Use Policy. As the new avenues for misuse emerge, organizations must review the policy and announce the amendments and communicate among all the employees using IT resources.

Organizations should consider deployment of automated client desktop policy enforcement tools which can provide them centralized monitoring, control and audits in a decentralized, distributed computing environment.

Desktop Controls

Organizations should implement comprehensive desktop security and controls to mitigate risks due to misuse and in appropriate use. Organization should consider enterprise wide standard build desktop roll out that locks down and baselines system capabilities, implementation of role based access control, centralized automated antivirus solution, patch and update management system, software metering, monitoring system, and enterprise backup solution that covers the desktops. The desktop control initiatives should be pro active rather than reactive with the blend of preventive, detective and corrective.

Training and awareness program

Training and awareness is main preventive control. Employees should be made aware of the emerging threats and how to mitigate the risks, rational of company's NDA policy, legal exposures arising out of employee misuse and how to protect the sensitive data. Appropriate media controls should be in place to handle sensitive computer printouts, floppies and CDs. Employees should be trained to protect their workstations by locking the screens while away from desk, use of screen savers, prevent shoulder surfing etc.

Content Filtering

Content filtering is primarily divided into 2 categories; *Web filtering* and *Email filtering*.

Web filtering helps organizations enforce corporate Internet usage policies; allow control of access to non-business related websites, protects organization, staff and network assets and provides tools to monitor web usage. Filtering out non-business content leads to increased employee productivity, increase network efficiency, minimizes bandwidth costs, avoids workplace issues caused by objectionable content and helps to protect the organization from legal liabilities. The web filtering solution typically has categorized database of various website categories, self-learning capability to catch the new websites and usually comes with granular policy manager with real-time monitoring and managing controls.

Email filtering solution filter the content based on the organizational policies and preferences. Email filtering allows organization to limit the bandwidth consumption, spam control, antivirus, worm control, and enforce the appropriate email usage policies. Email filtering protects organizations from leakage of company confidential information. Limiting the size and type of email attachments prevents serious attacks such as denial of service.

Mobile Workers

Prevalence of laptops and Internet has only compounded the control problems for organizations. Those mobile workers using laptops at homes without appropriate controls may introduce viruses, worms or offensive content into the corporate network when they connect their laptops at workplace. Use of laptops also pose significant exposure of company confidential information walk out of corporate network,. Organizations must have complimentary mobile computing policies in place to protect their information assets.

Conclusion

One of the most overlooked threats in a corporate security program is the threat posed by employee behavior. As much as 80% of the security compromises are the result of the actions by an inside. Prevention of the misuse of Information Systems by employees has direct business value. Benefits of misuse controls are increased productivity, maximization of corporate assets, compliance with privacy regulations, protection from legal liabilities, preserving network bandwidth and resources. Organizations should deploy comprehensive countermeasures to defend against misuse of its IT resources.

Vijay Gawde, *CISSP, NCSA, CCNA, MCSE*
is Senior IS Security consultant at Riyad Bank, Saudi Arabia. He has more than 20 years of IT experience including product development, networking, e-business and information systems security. He can be reached at *vgawde@riyadbank.com*