MICROSOFT AUSTRALIA

Inquiry into the Management and Integrity of Electronic Information in the Commonwealth

Submission to the Joint Committee of Public Accounts and Audit

December 2002

CONTENTS

INTRODUCTION

Microsoft Australia welcomes the opportunity to make a submission to this inquiry, and commends the Government for opening public discussion of this important issue. As a global leader in the information technology business, Microsoft is heavily involved with numerous national and international forums concerning information integrity and security issues. Microsoft products are used extensively by Australian government agencies, businesses and consumers.

In the information security field, Microsoft is already engaged as an industry representative for many leading international organisations and meetings, including:

- The U.S.-Australian Cybercrime Bilateral;
- the United Nations Working Group on Information Technologies;
- the OECD Group of Experts on Information Security and Privacy;
- the G8 (Group of Eight) Nations Subcommittee on Cybercrime, and;
- various NATO initiatives concerning computer and network security.

Microsoft has also been involved with the Council of Europe's draft Convention on Cybercrime and the European Commission's recent Communication on Cybercrime.

THE STATE OF PLAY

The relevance of security

Issues of electronic information integrity and security have been a concern for business and government alike ever since the widespread adoption of computing technologies for information processing. In recent years, the rise in popularity of the Internet has led to increased expectations for information delivery and a whole new set of challenges.

Information security in the online world is now a tremendously complex and wide-reaching issue. Ensuring a secure computing environment requires different strategies at different levels; governments and other large organisations, mid-sized businesses and individual users all have different and unique security requirements. Government agencies and other large companies must contend with massive and diverse computing environments that encompass a mix of different software platforms, commercial and custom-built applications and services.

Global concerns over terrorism in the wake of events such as the September 11 attacks in the USA and the Bali bombings have also increased concerns over information security. Since our world has become dependent upon IT, electronic information repositories held by both public and private organisations are now widely viewed as potential targets for attack, requiring a new emphasis on both physical and digital security.

Despite these concerns, governments around the world remain committed to providing the benefits of electronic information maintenance and delivery to their constituents.

Achieving this goal in balance with the security concerns requires commitment to a clear set of policies designed to create an effective, secure yet useable environment.

An Evolving Security Environment

The tremendous progress computing has made in the past fifty years is the product of a vast "ecosystem" of commercial software companies, government and academic researchers each playing a unique and critical role in advancing the state of the art.

So too, as recent world events have made clear, this immense ecosystem is dynamic and constantly changing. Clearly, industry, government and the public all have an interest in keeping pace with these changes as they evolve and ideally, staying ahead of the threats and breaches of security before they occur. These evolving threats have one thing in common: in the past only dedicated IT professionals used to worry about security– today, it is a concern of everyone.

While we will not be able to address all of these issues in-depth in this submission, we believe that the various "fronts" in the battle for security can be outlined as follows:

- *Technology:* The software itself, whether an operating system, library or development tool, stand-alone application or network service, must be fundamentally secure.
- *Implementation:* The software must be implemented and used in a way that is resistant to attack and misuse, while maintaining the ability to further update and modify it as threat models evolve.
- *Procedures:* Software providers must have mechanisms in place to accept customer feedback and respond to security issues, while organizations and individuals must be able to effectively implement needed changes.
- *People:* While technology is capable of ensuring a very high level of security, its users must still be aware of, and vigilant against, potential issues.
- *Policy:* Strong policies must exist, both at the organizational and governmental levels, to govern how software is used and to deal appropriately with individuals and organizations that maliciously exploit or misuse the software.

Existing policies

Microsoft recognises that many existing government initiatives and policies have been put in place to ensure the integrity of electronic information, including NOIE's work on the E-Security National Agenda and the Defence Signals Directorate Information Security Group's Electronic Security Instructions initiative. Other general security policies, such as the Protective Security Coordination Centre, will also have an ongoing impact on electronic information security.

Ongoing policy development will be critical to the continuing evolution of a secure and authenticated environment for the exchange of electronic information. While the IT industry as a whole works to make its products more secure, security does not occur in a vacuum. Government can continue to play a critical leadership role in creating best practice models for information security, setting an example for businesses and other organisations to emulate.

Perceptions of cybercrime

To date, the potentially devastating effects of cyber-crime and other information violations have not been widely recognised. This is reflected both in the sentences typically handed down to those convicted of electronic fraud and in the general attitude of the public towards ‘white collar’ information-related crimes.

In many segments of the media, attention is focused on minor flaws within software or hardware. Frequently, insufficient recognition is given to the fact that all hacking crimes begin because an individual sets out with the deliberate intent to gain unauthorised access to information.

As a market leader that provides global products, Microsoft and our customers have served as a target for criminal attack. In response, we are directly committed to protecting and confronting the challenges of online security for probably more customers’ information around the world than any other single organisation, .

As more information is moved into electronic formats and the exchange of this information becomes an everyday occurrence, the potential for damage by hackers or terrorists is also going to increase dramatically. Microsoft supports the notion that the legal framework should reflect the very real threat posed by cyber-criminals, and that punishments should be allocated in accordance with this fact.

Microsoft’s view of security issues

In considering issues of information integrity and security, it is important to recognise that it is not possible to create ‘100 per cent secure’ or impenetrable software that is also accessible and useful. Software development, like virtually all fields of human interest, is an imperfect science, and as a result all software has bugs. Some of them can be exploited to cause security breaches until the bugs are overcome. For instance, virus writers are constantly coming up with new code variants, adding to the challenge of maintaining a secure system.

It is also important to recognise that even if software could be made perfect, it would not solve the problem entirely. Most attacks involve, to one degree or another, some manipulation of human nature. If users deliberately choose to execute an infected file attachment without virus-checking it first, problems will arise. If IT managers fail to regularly patch their systems, vulnerabilities will continue to exist even when they have been recognised by the original software developer. If systems administrators choose an obvious password, then hackers will find it easier to break into their networks.

It is therefore vital that the public understands its role in maintaining solid security because there is a strong degree of personal responsibility involved in maintaining the integrity of any system.

Finally, all information security systems involve a trade-off between ease of access and ease of use. A bank vault concealed in the middle of an isolated mountain range is highly secure, but extremely difficult to access on a day-to-day basis, lessening its usefulness. Likewise, a system which forces users to learn a new password every day is highly secure, but also highly inconvenient.

These concerns are reflected in Microsoft's 10 Immutable Laws of Security, which are widely used for internal and end user education and training on security issues.

Microsoft's 10 Immutable Laws of Security

Law #1: If a bad guy can persuade you to run his programme on your computer, it's not your computer anymore.
Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.
Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
Law #4: If you allow a bad guy to upload programmes to your website, it's not your website any more.
Law #5: Weak passwords trump strong security.
Law #6: A machine is only as secure as the administrator is trustworthy.
Law #7: Encrypted data is only as secure as the decryption key.
Law #8: An out of date virus scanner is only marginally better than no virus scanner at all.
Law #9: Absolute anonymity isn't practical, in real-life or on the web.
Law #10: Technology is not a panacea.

IMPROVING MANAGEMENT AND INTEGRITY

Trustworthy Computing Environment

As part of its efforts to take a leadership role in improving information security, Microsoft has been working on the creation of the Trustworthy Computing Environment which addresses the technical, policy and social issues involved in creating a secure system for information exchange.

The Trustworthy Computing Environment framework recognises that for truly widespread adoption of information technology which can be relied upon as we do other major infrastructure networks, current approaches to software development and deployment will need to change rapidly, without requiring all existing systems to be eliminated. The notion of trust needs to be addressed from three perspectives: the goals of those who use it, the means available to meet those goals, and the identity of all elements working within these systems. Key goals identified by Microsoft include availability, suitability, integrity, privacy and reputation. Each of these interacts with each other, and are impacted in turn by government policies, technological developments and other issues.

Addressing these complex issues is a challenging task. Microsoft believes that it may take a decade or more to fully create such an environment. (The Trustworthy Computing Initiative is discussed in detail in the Appendix to this submission.)

Underscoring its commitment to helping create the Trustworthy Computing Environment, Microsoft has devoted substantial resources to developing technology tools and trusted systems that enable users to protect their online data easily and effectively. These include:

Anti-virus technologies – A range of technologies to help users detect and protect against software viruses and to ensure that viruses do not spread.

Secure online identification – Various tools to help users verify the identity of other online users and to protect the integrity of their own identity online.

Encryption-based solutions – Platforms and tools that support a range of powerful encryption solutions.

Security evaluation and product certification – Regular and rigorous product evaluation and certification by third-party security testing bodies.

Update facilities – online, real-time software update tools which install the very latest software enhancements and bug fixes.

As further part of our commitment to delivery on the Trustworthy Computing Initiative, approximately 8,500 of our Windows developers stopped developing new code for two months. earlier this year and instead devoted their full-time efforts to extensively reviewing our existing stocks of code for security vulnerabilities, threat modelling and re-coding. We estimate that this unprecedented initiative has cost Microsoft, to date, over one hundred seventy six million dollars (A$176,000,000). We are now conducting security reviews of other products as well, and this pioneering commitment is based upon our senior executives' decision that security is paramount in an age of new and shifting threats. It also recognizes our responsibility as an industry leader to constantly create ever more secure technology.

The role of standards

All technology projects require a commitment to standards, and this is especially true in the field of information integrity and security. For instance, policies which incorporate encryption of sensitive information (such as the Government's Gatekeeper initiative) will generally specify the key length for encryption, amongst other details.

Providing such definitions helps provide a basis for high levels of interoperability. However, it is crucial to recognise that standards should not be set in stone and forgotten, or wedded exclusively to a particular technology or set of technologies. As trials occur, requirements change and technologies evolve, standards will need to be flexible enough to account for these changes without requiring extensive revision.

Microsoft advocates an approach of outlining broad goals for information integrity and security, allowing the details of implementation to be determined on a case-by-case basis, using the best and most appropriate technology for the particular set of circumstances. Within its own operations and software development activities, Microsoft is fully committed to open extensible standards – most notably XML (Extensible Markup Language), which forms the basis of the .NET Framework and allows information interchange across a wide variety of computing platforms – to ensure ongoing interoperability into the future.

To this end, Microsoft has developed a framework called Gov.NET that outlines a series of foundation pieces needed for the online world while integrating those pieces into the existing business applications already in existence. This is important because as Australian government agencies increasingly use the Internet to exchange information between agencies, with other governments or to deliver services to constituents online, there are a range of "technology foundation pieces" that are being considered to better enable this capability.

Government certification

Over the past decade, government information assurance programs have taken on a critical role in the development of IT policies and infrastructures, both for government purchases and as a role model for industry to follow. Throughout the 1990s, a number of security evaluation programs from the United States, Canada and Europe came together to form a guideline known as the Common Criteria, which is now adopted by the governments of 15 countries, including Australia.

These guidelines carry significant requirements for documentation, evaluation, design and test reviews – a rigorous and expensive process for anyone who creates software. Commercial software vendors have a clear incentive to satisfy their government customers, and are thus devoting tremendous resources to attaining this certification.

In 2002, Microsoft achieved Common Criteria certification, underscoring our commitment to creating secure and usable software. As very few businesses can afford to carry out detailed analysis on a wide range of products for themselves, Common Criteria is likely to be an important basis for many advances in the field of information security and integrity.

Free Software and the Government Security Program

In recent years, the concept of free software (FS) or 'open source software' (OSS) has gained increasing visibility. In an open source software environment, the original source code used to develop a program is made freely available, and users are free to alter this as they see fit. In contrast, most commercial software providers do not make their source code available as it represents their key intellectual property and the basis for their commercial life.

Many open source advocates argue that the free software model provides for a higher level of security and integrity than would otherwise be available. Microsoft believes that this is an overly simplistic view, and that the very real security risks associated with the open source development model are often ignored. There are important issues around security that should be examined in this context.

Simply making source code available does not guarantee comprehensive, expert security review. The core argument behind OSS security is the "many eyes" theory, which holds that the more people who review the source code, the more likely bugs and security problems will be found and fixed. However, source code availability aids finding security flaws only if the code is actually examined, and the testers who examine the code have security expertise.

Through our Government Security Program (GSP), Microsoft is actively seeking to facilitate this opportunity for government. In short, GSP is a technology sharing program which Microsoft has offered to selected national governments around the world, including Australia. Through GSP, the national government participating in the program gains access to Microsoft's core intellectual property -- the source code of Microsoft Windows. Microsoft makes this code available primarily to allow governments to assure themselves of the high level of security inherent within the Windows product sets. As a supplement to this access Microsoft has also made available the ability for technical teams from Australia to utilise its Redmond-based high secure facilities and work closely with its software developers on national security projects. Entry into the Government Security Program is free.

As the GSP as well as our participation in government certification programs attests, Microsoft welcomes the opportunity to open its code up to expert scrutiny and review. There is no guarantee of such expertise in the open source development process, and there is no ongoing commitment to maintaining the product.

This is particularly relevant in the context of government certification programs such as Common Criteria. Very few community-driven software development efforts would have the logistical and monetary capabilities required to participate in such a program. Even if a large commercial entity were to assume the responsibility and costs for certifying an OSS project, the path to certification would be arduous due to the distributed nature of code contributions in OSS projects and the lack of uniform documentation and testing processes across all contributing developers and sub-components.

The task would be made even more difficult given the fact that the certification process must include any additional features and sub-components that are added to the evaluated configurations as the product continues to mature and respond to customer and competitive demands. This is a difficult task to manage unless the certification process is handled by skilled professionals.

Open source software also has negative implications for industry development. Companies have little incentive to invest funds in research and development if their work can be freely appropriated by others.

FUTURE ISSUES

Device proliferation

It is widely recognised that in the future, access to electronic information will be carried out not just from personal computers, but from a wide range of other devices. These include (but are not limited to) mobile phones, personal digital assistants (PDAs), handheld and portable computers, digital televisions and even games consoles. The networks which are used to exchange information will also expand, with wireless access via either telephone networks or local wireless systems taking on an increasingly central role.

One important result of this switch to a network-enabled, device-independent model will be a need to rethink approaches to information security. Systems which have proved effective with PCs will need to be adjusted for other devices, and the introduction of new networks will pose challenges independent of the software which runs across them.

Web Services

Web Services is a general label used to describe the creation of individual software services that can be accessed over the Internet and other networks, and can be combined by individuals and businesses to meet their specific needs. For instance, a company which wants to authenticate the identity of visitors to its site would simply access a widespread commercial service such as Microsoft Passport, rather than writing its own proprietary code.

Virtually all major software development companies are now working within a Web Services model. Microsoft has taken a leadership role in the creation of Web Services through its development of the .NET Framework, which uses the open standards of XML to allow different software components to interact with each other.

In a Web Services environment, issues of information integrity and security take on a new and central importance. Users will not wish to access software services from providers unless they have already established a trust relationship with them.

At the same time, the combination of multiple services from different providers will create new security challenges for each implementation, and these will need to be addressed with appropriate widely adopted policies and standards. Importantly, the adoption of Web Services will reduce the complexity of current software development, allowing administrators to spend more time concentrating on security issues.

Evolving policies

Extra devices and the emergence of Web Services are just two examples of how changes in the technology industry will also require changes in information security policies. Other changes – some of which have not been envisaged by technology developers themselves – will continue to appear on a regular basis.

This rapid rate of change requires an ongoing dialogue between the technology industry and its customers, and this dialogue is especially important within the government arena because of the leadership role which government (especially in Australia) plays with respect to technology policies and adoption.

More generally, security policies should be formulated in such a way that they can be readily adapted to new circumstances without requiring continuous revision. This is an essential requirement, as ongoing competition means that software will continue to develop faster than policies. Even the most proactive government body is unlikely to keep pace with the rapid rate of change, especially in the software field.

CONCLUSION

Information security and integrity are now recognised as critical elements of any information technology plan. Perfect information security is a myth, both because of the nature of software development and because of the ever-present possibility of human error. A sensible information security policy must recognise these factors, and balance the need to protect information against the requirements of those who use that information. It must also balance the need to certify security standards with the important of protecting intellectual property.

Information security is a goal rather than a destination. The rapid rate that technology continues to evolve, and the new uses which are made of electronic communications, mean that an ongoing dialogue between business, the IT industry and government will be needed to ensure that a proper standard of security is maintained. Microsoft would welcome the opportunity to be part of this dialogue and to contribute its expertise to ensure that the full benefits of electronic information are realised for all Australians.

APPENDIX

Microsoft Australia Trustworthy Computing Environment Whitepaper.

CONTACT INFORMATION:

For questions or further information, please contact:

Julie Inman
Corporate Affairs Manager
Microsoft Australia
1 Epping Road
North Ryde, NSW 2113
(Ph) (02)9870-2656
juliei@microsoft.com