Microsoft

Achieving resilience against modern cyberthreats

Protect

Detect

Respond

Microsoft is a reliable partner helping to protect valuable information in an era of constant targeted attacks and determined adversaries.

New technologies – new opportunities – new threats

The world of information technology is complex, and is being transformed by key business drivers – mobile, social media, cloud services and big data – that are reshaping markets, business models, and the way people access information. However, in addition to offering new business opportunities, these large-scale technology trends are also bringing security challenges and even new threats.

From passive protection to active resilience

Passive protection is no longer sufficient to ensure the security of information and IT infrastructures. The more thoroughly information technology permeates business processes, the more organizations will be exposed to complex, advanced attacks by criminals who aim to strike where organizations are most vulnerable and the criminal return on investment is highest.

This means that organizations need to rethink their approach towards security, and create a holistic security strategy built on risk management to achieve resilience against modern cyberthreats. It's similar to team sports. In ice hockey, for example, the goaltender is the last bastion, protected by defenders out of the defensive zone. To effectively protect the goal, the whole team must have situational awareness to read the game. The underlying risk management approach is the work of the coach, who is responsible for defining efficient tactics and plays based on the strengths and weaknesses of the team and their opponents.

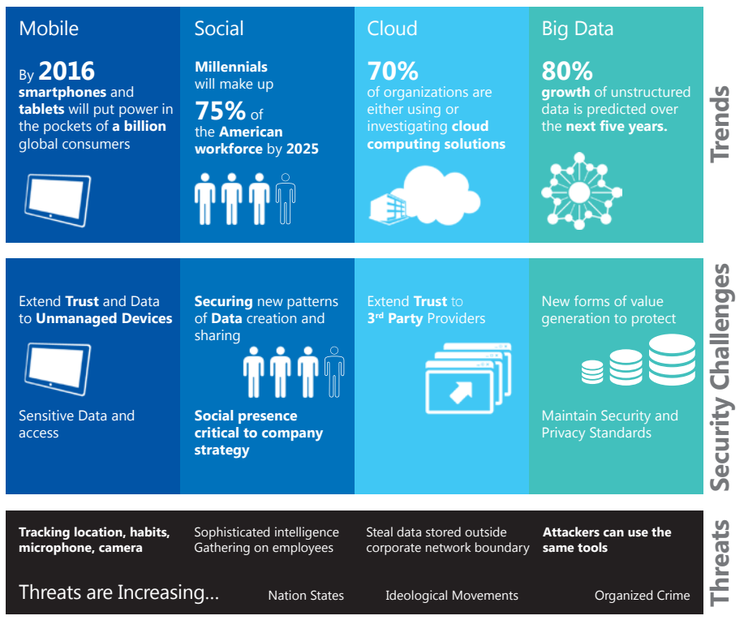
New security approach

Providing holistic protection for an IT infrastructure and ultimately for the information it contains means building on a modern security framework. Microsoft's pillars of security comprise proactive strategies built on a "Protect – Detect – Respond" approach to protecting infrastructure, managing the identity of users and devices, detecting concrete threats, and responding robustly if security breaches occur. In essence this is similar to the team effort described in the hockey analogy, where it is not a single security technology or process that provides resilience against modern cyberthreats, but a systematic, agile and risk-based security strategy. As the world's leading manufacturer of platforms and applications, Microsoft is the ideal partner for organizations seeking a business-oriented security strategy.

Information and communications technology has long permeated the majority of business processes, with mobility technologies, social media functions, cloud services and big data all helping drive economic and societal development. By allowing easier access to information, people and know-how, IT makes business processes more cost-efficient and

Large Scale Technology Trends

Transforming access to people and information



enables services to be customized.

While the majority of businesses and individuals conduct their transactions safely every day, information technology is also subject to permanent and increasing threats. This means that organizational data in the private and public sectors, as well as consumer data, are in significantly more danger than only a few years ago. Any device connected to a network is exposed to a multitude of threats, regardless of the operating system or whether the device is a smartphone, tablet, PC, router or Internet TV.

Risk-based rather than absolute security

There is no absolute security – but for any device there is such a thing as optimal security in light of the anticipated risks and the need to maintain productivity. Achieving this optimal security requires a comprehensive evaluation of the risks as the basis for developing measures designed to safeguard the achievement of business objectives. Risk-based security of this type has two components: basic protection against the common, undirected threats to which any infrastructure is exposed, plus advanced security technologies and services designed with a deep understanding of the infrastructure technology and architecture to help protect against targeted attacks by determined adversaries. This risk-based security approach means that an organization has to understand its assets (information, services, applications, devices and users) and apply appropriate prevention, detection and response technologies, resources and processes to align investments with risks.

Platforms and applications developed by Microsoft are installed on a large number of computers worldwide. With such profound knowledge of the blueprint of the software, we also have a special responsibility. Microsoft takes this responsibility seriously: it has set the baseline for basic protection very high, and provides advanced solutions and services to help protect against attacks by determined adversaries.

Businesses under threat

The more heavily dependent on information a business is, the more seriously its business processes – and even its very business models – are under threat. Organizations are facing the task of building optimal security in an environment of shrinking budgets where they have to combine data privacy and information and infrastructure security. In addition they find themselves confronted with a range of different technology delivery models, myriad providers, and short innovation cycles. In short, the development of technologies is dynamic, and organizations have to cope with an increasingly complex infrastructure.

But they also have to contend with a "dark force": a multibillion dollar industry populated by criminals, state sponsored attackers, hactivists, organized crime and others with wildly differing motives. These attackers are becoming increasingly professional, using the latest technologies and sophisticated methods to break into systems and achieve their aims. They target their victims on the basis of the perceived value of what they want to achieve. This perceived value may be different from the value the company puts on information or research results, as to a large extent it's a demand driven market.

Microsoft's Pillars of Security

Information systems security based solely on protective measures does not provide adequate protection from attacks by determined adversaries. A more agile security framework, however, can provide holistic protection for an IT infrastructure and ultimately for the information contained therein. Microsoft's security pillars include proactive strategies built on a "Protect – Detect – Respond" methodology for protecting infrastructure, detecting concrete threats, and enabling robust responses if security breaches occur.

Cyberthreats: a serious danger to business and society

Data networks have long served as the hub for devices of all types. Whether it's an organization's own network or the public Internet, network-based threats affect all users, businesses and organizations.

The evolution of cyberthreats

The organized crime ecosystem exploits weaknesses in the information technology infrastructures of organizations in the public and private sector.

Attacks are targeted, hidden, and often combine multiple, automated attack vectors. Sophisticated attacks no longer just threaten desktop computers, but mobile devices as well. Even cloud infrastructures are attacked on a daily basis, although these infrastructures are generally protected by the highest security standards, so attackers face a much greater challenge.

No longer are attackers just targeting large corporations with important data. Any organization willing to pay a "ransom" for "kidnapped" data is a potential victim. In such cases, attackers will typically block access to the victim's systems or encrypt the data until the money is transferred. In other cases, hijacked systems are being used not just to send spam, but to attack system owners directly through extortion, data theft, or data destruction, as seen in the recent outbreaks of ransomware attacks.

What's at risk?

Devices and systems of all types are at risk: individual smartphones and tablets used at home or brought to work, computers certified for business use, servers, cameras, sensors, as well as entire datacenters. Not only are each of these individual targets, but it is possible to attack many different targets at once.

There are a number of different ways that networked systems can be attacked, both through known and unknown vulnerabilities, which are then exploited by malicious attackers to achieve their various goals. A complicated physical break-in isn't required, but the endless variations of increasingly sophisticated attack vectors, often combined with sophisticated social engineering attacks, make it complicated to protect information technology systems.

Public sector infrastructure and industrial systems are also increasingly at risk. More and more electricity installations, water utilities, rail infrastructures and building technology systems – to name just a few examples – are connected with the Internet and set up for remote control. The 'bring your own device' trend also increases risks, as it enhances the value to the attacker. If adversaries attack private systems, with no additional effort they can potentially gain access to company data as well as private information like e-banking credentials. The fact that control over private devices is limited means that in effect, a company's data may be less protected than assumed.

Origin of Data Breaches

Who is behind data breaches?		How do breaches occur?	
98%	stemmed from external agents (+6%)	81%	utilized some form of hacking (+31%)
4%	implicated internal employees (–13%)	69%	incorporated malware (+20%)
<1%	committed by business partners (<>)	10%	involved physical attacks (–19%)
58%	of all data theft tied to activist groups	7%	employed social tactics (–4%)
		5%	resulted from privilege misuse (–12%)

Source: Verizon 2012 Data Breach investigations Report

How you can gain greater agility and boost resilience

Threats to information on IT infrastructures will keep increasing. All the security in the world can't make these threats disappear completely. But it is possible to significantly reduce the risk by acting far-sightedly and opting for a platform from a manufacturer that is aware of its responsibility. Microsoft offers a wide range of support technologies and services to help secure its customers' systems. The focus is on increasing information technology resilience against threats – in effect boosting the IT immune system.

The key principles for organizations

Organizations can adopt a security strategy that bridges today's technology trends with security principles designed to increase the overall resilience of the whole organization's IT ecosystem. This approach is based on the following main elements:

a) Using trustworthy cloud services that harbor the organization's data in an infrastructure that is already resilient;
b) Increasing the resilience of the organization's own IT systems by enforcing good IT hygiene and enabling policy-based access to information.

A combination of these two elements creates a hybrid approach to building overall resilience. The following sections describe these two building blocks and how they can be used as part of an IT security strategy that boosts resilience while allowing a great deal of agility.

Use of trustworthy cloud services

The use of cloud services as a pillar of security is an often underestimated tool in today's information technology strategy. The cloud offers at least four significant security advantages over a purely on-premises model. First, the world has a significant shortage of computer security professionals, a problem that is not likely to be solved in the short term. Indeed, many small organizations may have little or no IT staff, let alone security experts. Cloud providers enable a centralization of security expertise, and adhere to emerging international standards of operational security, so organizations don't need to invest in the same level of security resources as they do for purely on-premises solutions. Second, the centralization of data, combined with industry standard accreditations, may permit better information protection than exists in today's massively distributed world, where monitoring and correlating of security information may be difficult. Third,

Pillars of Security
The hockey analogy: the goaltender

Protect

Protection focuses on defense-in-depth using architectural as well as operational activities and provides additional protections so that even products with vulnerabilities are harder to exploit. The analogy in ice hockey is the goalkeeper with all his protective equipment that catches the pucks that the opponents manage to get through the team's defenses.

much like on-premises software and systems, Microsoft's cloud services are created using secure development practices, thus helping ensure better security code quality. Fourth, as cloud services are always "up to date," we don't have to work with any legacy software, technologies or applications, which means it's possible to always have current and well protected cloud services.

Secure your own IT infrastructure

In addition to using trustworthy cloud services, your IT infrastructure needs to be protected through enforcement of good IT hygiene practices, including the following four activities:

Stay current (upgrade), and do patch management: The two most important things for organizations are still patch management, and upgrading operating systems and applications to the latest version. Other main elements also include deploying secured devices with policy-based information access, and not assigning administrator rights to users. Organizations should make sure that relevant patches are installed as soon as possible, as the window of opportunity before exploits become possible is only a matter of days or sometimes even hours. Organizations should also switch as quickly as possible to the latest version of the platform to ensure the most recent security functionality is in place. It's important to realize that the latest version of a platform is usually subject to significantly fewer attacks, as attackers tend to focus on platforms with fewer security controls in place.

Align Active Directory to threat environment: Active Directory in Windows Server manages users, computers, servers and applications across all levels of the information technology infrastructure, and in most organizations is also responsible for the majority of authentication and authorizations to data, services and devices. This means that it is a central element that particularly needs to be configured correctly and secured in line with an analysis of the risks. Special attention also needs to be paid to the correct operation and administration of Active Directory to protect, for example, against "pass the hash" attacks. The threats related to Active Directory also include users being able to access information and services that they are not cleared for because of a lack of control and management of identities. In the wake of mobility and cloud trends there is an increased need to have a well-managed Active Directory so that identities of users and devices can be trusted.

Assess threats and countermeasures: Information technology infrastructures and processes should be assessed thoroughly to gain an understanding of the current threat environment based on the enterprise's technical maturity, risks and requirements. This means also taking account of the fact that users want to work from anywhere on certain devices, and that the business needs to collaborate with external parties or leverage cloud-based services.

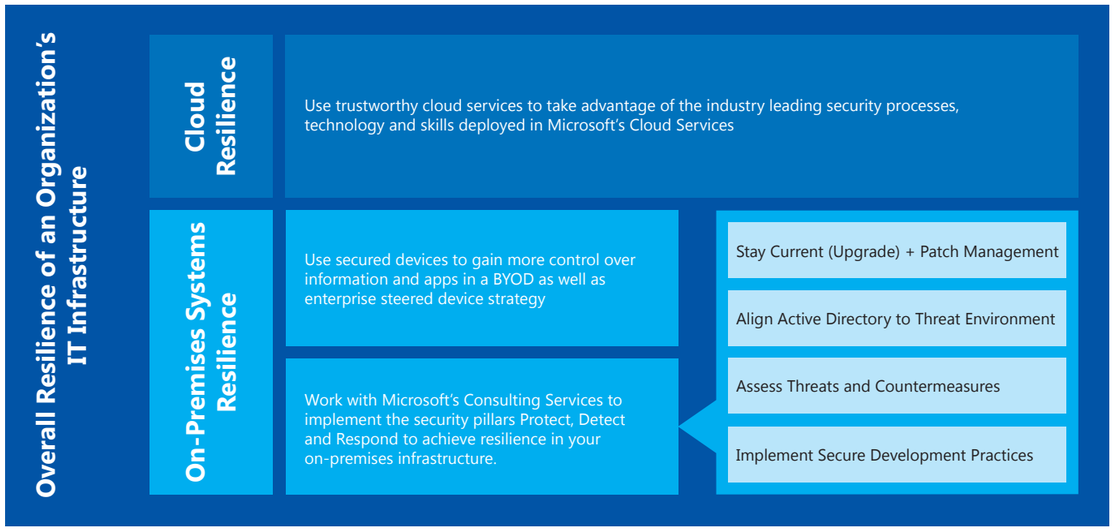
Implement secure software development: Organizations with their own software developers should take account of security right from the conceptual phase, and implement secure development processes. Microsoft's Security Development Lifecycle (SDL) is available free of charge and can be used for developing business line applications. SDL includes the following central principles: secure by design (security is planned); secure by default (the standard configuration contains as few privileges as possible and rarely used functions are deactivated); secure in deployment (documentation and tools are available to enable the software to be rolled out securely by administrators); and institutionalized communications (there is transparent communication, and patches or workarounds are rapidly available).

Deploy Newer Products

Security Features Added over Time

2004	2007	2009	2012
Key Threats • Code Red and Nimda (2001), Blaster (2003), Slammer (2003) • 9/11 • Mainly exploiting buffer overflows • Script kiddies • Time from patch to exploit: Several days to weeks	**Key Threats** • Zotob (2005) • Attacks "moving up the stack" (Summer of Office 0-day) • Rootkits • Exploitation of Buffer Overflows • Script Kiddies • Raise of Phishing • User running as Admin	**Key Threats** • Organized Crime • Botnets • Identity Theft • Conficker (2008) • Time from patch to exploit: days	**Key Threats** • Organized Crime, potential state actors • Sophisticated Targeted Attacks • Operation Aurora (2009) • Stuxnet (2010)
Windows XP SP2 • Address Space Layout Randomization (ASLR) • Data Execution Prevention (DEP) • Security Development Lifecycle (SDL) • Auto Update on by Default • Firewall on by Default • Windows Security Center • WPA Support	**Windows Vista** • Bitlocker • Patchguard • Improved ASLR and DEP • Full SDL • User Account Control • Internet Explorer Smart Screen Filter • Digital Right Management • Firewall improvements • Signed Device Driver Requirements • TPM Support • Windows Integrity Levels • Secure "by default" configuration (Windows features and IE)	**Windows 7** • Improved ASLR and DEP • Full SDL • Improved IPSec stack • Managed Service Accounts • Improved User Account Control • Enhanced Auditing • Internet Explorer Smart Screen Filter • AppLocker • BitLocker to Go • Windows Biometric Service • Windows Action Center • Windows Defender	**Windows 8** • UEFI (Secure Boot) • Firmware Based TPM • Trusted Boot (w/ELAM) • Measured Boot and Remote Attestation Support • Significant Improvements to ASLR and DEP • AppContainer • Windows Store • Internet Explorer 10 (Plugin-less and Enhanced Protected Modes) • Application Reputation moved into Core OS • BitLocker: Encrypted Hard Drive and Used Disk Space Only Encryption Support • Virtual Smartcard • Picture Password, PIN • Dynamic Access Control • Built-in Anti-Virus

Overview: Elements of an Agile and Resilient Infrastructure



How Microsoft can help

Security has been a core consideration for Microsoft for over ten years. On January 15, 2002, Bill Gates sent a memorandum to all Microsoft employees announcing the Trustworthy Computing (TwC) Initiative. In that memorandum, he noted the importance of providing computing that was as "reliable and secure as electricity, water services and telephony," and noted that the key aspects of a trustworthy platform included availability, security, and privacy. He also made clear that the initiative was not just about technology: "There are many changes Microsoft needs to make as a company to ensure and keep our customers' trust at every level – from the way we develop software, to our support efforts, to our operational and business practices."

From that date on, security, privacy, reliability and the commitment to customer-centric interoperability has been at the core of Microsoft's solutions. The TWC group has taken responsibility for trustworthy computing (efforts to help ensure a secure, private, and reliable experience for computer users) and engineering excellence (propagating engineering best practices across the company and into the IT ecosystem). As a result, Microsoft has developed various solutions designed to reduce the burden on information technology officers and enable them to concentrate on their core business. These solutions increase the resilience of Microsoft's customer's IT systems on the basis of the priorities of today's CIOs, and contain an assessment of common risks. Based on this foundation, Microsoft's customers can take advantage of the following products and consulting services to ensure the overall resilience of their infrastructure:

Microsoft cloud services and products

Trustworthy cloud services

Microsoft is committed to delivering trustworthy cloud services, and given its experience, investments, and history of commitment over the past ten or more years to the creation and delivery of security-enhanced, private, and reliable computing experiences, it is in a unique position to do so. Microsoft applies its resources to online services in ways that extend beyond traditional standards and methodology to deliver industry-leading capabilities.

Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape. OSA combines this knowledge with the experience of running hundreds of thousands of servers in data centers around the world that deliver more than 200 online services to more than 1 billion customers and 20 million businesses in 88 countries.

Microsoft uses OSA to minimize risk by ensuring that ongoing operational activities follow rigorous security guidelines and by validating that guidelines are actually being followed effectively. When issues arise, a feedback loop helps ensure that future revisions of OSA contain mitigations to address them.

OSA helps make Microsoft cloud-based services' infrastructure more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to real and potential Internet-based security threats, thereby increasing the security of those services for customers while aligning to industry-standard certifications that customers recognize and trust.

More secure operating systems and software

The security functionality of Windows and Windows Server platforms, and Microsoft's system management platforms, are the product of years of endeavor on Microsoft's part to make its technical platform for applications and business processes more resilient to threats. Among other things, these functions provide:

- Groundbreaking resilience to malware (managing threats and providing protection from them)
- Comprehensive device encryption (protecting sensitive data)
- Highly secured access control mechanisms for flexible workstyles
- End-to-end security and management for any kind of mobile device (various platforms)

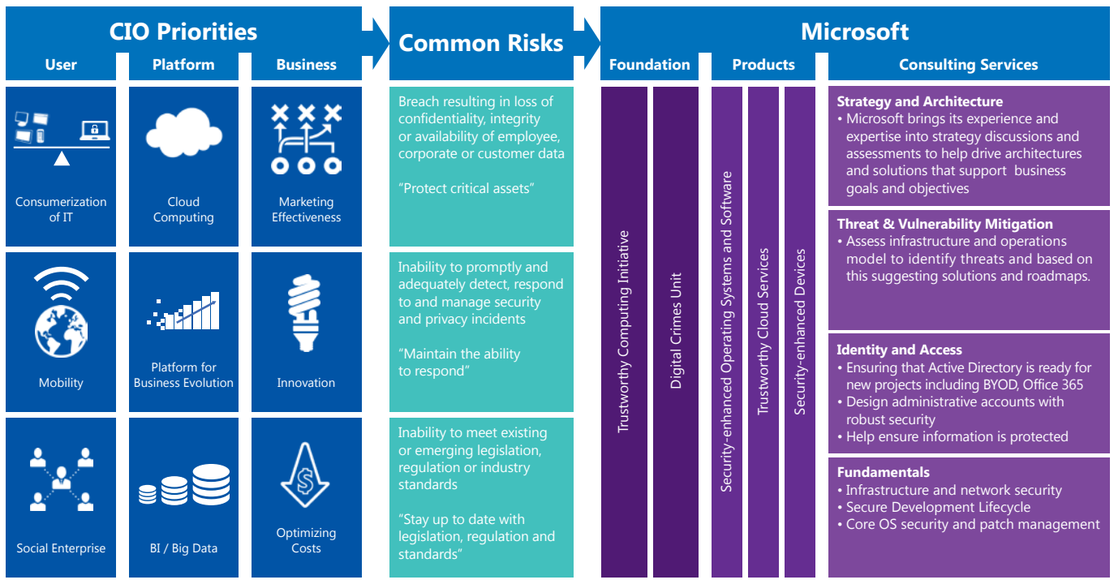
Security-enhanced devices

These days device security and management is a central element of an IT security strategy. It can enable any device and allow information access from anywhere based on policy and classification of information and devices. Security features are built into Microsoft devices from the start, which opens up new mobility and bring your own device (BYOD) scenarios, with Windows enterprise devices fully manageable and capable of accessing the most sensitive data with robust security. Information on a device is only as secure as the device permits, and built-in security components like a Trustworthy Platform Module (TPM) chip help enable the secure storage of certificates and thus the safeguarding of data.

Microsoft services

Microsoft's experts can offer an entire bundle of services tailored to organizations of different sizes in different industries and with different needs, helping make private and public organizations' systems and services resilient to modern cyber-threats, and providing IT with the platform for a security-enhanced infrastructure that enables users to access services and applications from different types of devices.

Microsoft Solutions for IT Security Risks



Pillars of Security
The hockey analogy: awareness

Detect

Detection parallels the situational awareness in a hockey game that is required to act and react according to the opponent's game. Security strategies focus on capturing, correlating and analyzing audit events from across the enterprise to detect anomalies that belie attacker movements. High value data and systems should profit from tools that can also detect 0-day attacks.

Premier Support Services
Dedicated support teams are on call around the clock to make sure basic protection against routine threats is in place. They can draw on an in-depth understanding of business processes to provide solutions to urgent challenges, and offer proactive services which can assess the security configuration of servers and Active Directory, as well as provide tools and training for the IT departments of the organizations they serve. The supporters are backed by a global network of experts in Microsoft technologies. Premier Support Services are provided on a customized basis for each specific product group. Proactive services include various different programs designed to help organizations assess their information technology risks and take the right security-minded steps.

Global Business Support
Microsoft's security experts cover all aspects of data security, and support customers when responding to incidents. They have a profound knowledge of Microsoft technologies and software development geared to security – thanks not least to the Microsoft Security Development Lifecycle. The know-how provided by the Global Business Support team includes rich experience in role-based access control, and a holistic approach to creating a seamless chain of innovative security features across all levels of the information technology infrastructure. In addition, experienced incident response teams support customers remotely or on-site if they suspect that systems have been compromised.

Consulting Services
Microsoft Services consultants work on site with IT departments to help deploy and adopt Microsoft technologies securely, efficiently, and cost-effectively. They help shorten the time it takes for organizations to see value from their investments, as well as minimizing the risks from the outset. Microsoft consultants can draw on a global network of experts.

Advanced Cybersecurity Services
Microsoft's experts specialize in detecting complex threats such as attacks by determined adversaries, and coming up with the right response. They analyze the threat landscape, implement advanced systems for detecting advanced attacks (including zero day attacks), and use forensic methods to proactively or reactively investigate IT systems for previously undetected attacks and their origins. They advise software developers on the customer side on how to take account of security from the outset, and provide their expertise to businesses and public sector organizations.

Addressing cybercrime at its roots

Digital Crimes Unit
Each year, cybercrime takes a personal and financial toll on millions of consumers. To address this growing problem, Microsoft has created a center of excellence for advancing the global fight against cybercrime. The Cybercrime Center combines legal and technical expertise as well as cutting-edge tools and technology, marking a new era in fighting crime on the Internet. Through cooperative efforts with customers, industry, academic and criminal law enforcement organizations and other industry partners, the Microsoft Cybercrime Center aims to protect consumers online and make the Internet safer.

Pillars of Security
The hockey analogy: defense

Respond

The ability to respond to threats with incident response teams is essential to actively counter cyberthreats and get systems working again. It resembles the defensive roles in ice hockey that aim at restricting the movement of opponent players before the goal and make a successful shot on goal impossible.

Way ahead – first steps for achieving resilience with Microsoft

Today's trends and challenges are changing the risk landscape rapidly, and existing controls and processes will have to evolve. To take advantage of Microsoft's capabilities for making your information technology systems resilient, and to help protect your valuable information, we suggest that you contact your local Microsoft representative to discuss how the approach and capabilities discussed in this white paper can support your organization's business goals. While specific needs may vary and your Microsoft representative will adapt the method to your needs, the following overall steps will provide customers with a concrete suggestion for the way ahead:

Pillars of Security
The hockey analogy: the team

Resilience

Resilience against modern cyberthreats cannot be achieved by one single component. It means improving basic IT hygiene to counter the opportunistic threats and make even persistent and determined adversaries work harder. In addition it requires managing risks effectively and deploying strategies against advanced adversaries. This compares to an ice hockey team which is put together by an experienced coach depending on its own and the opponent's strengths and weaknesses and that plays together for optimal impact and resilience.

For More Information Please Visit:

Guidance, tools and tips from the experts at Microsoft:
http://www.microsoft.com/security/

Microsoft Trustworthy Computing
http://www.microsoft.com/twc

Microsoft Services
http://www.microsoft.com/services

Microsoft Security Development Lifecyle
http://www.microsoft.com/security/sdl/default.aspx

Microsoft Security Intelligence Report
http://www.microsoft.com/security/sir/

Microsoft Security Response Center
http://technet.microsoft.com/en-US/security/dn440717

Microsoft security for IT professionals
http://technet.microsoft.com/en-us/security/

Microsoft Digital Crimes Unit
http://www.microsoft.com/DCU