



White Paper

Trusted Enterprise Security

How the Trusted Computing Group (TCG) Will Advance
Enterprise Security

By:

Jon Oltsik
Enterprise Strategy Group

January 2006

Table of Contents

Table of Contents	i
List of Figures	i
Executive Summary	2
Technology and Business Realities	2
Technology Benefits Depend Upon Strong Security	3
Most Organizations Have a Long Way to Go.....	3
Why Are Things This Bad?	6
Enterprise Security Needs a New Model	7
The Trusted Computing Group (TCG) and Enterprise Security	8
How TCG Will Enable a Trusted Enterprise Model and Improve Security.....	10
Large Organizations Should Embrace TCG	10
Bottom Line.	12

List of Figures

Figure 1. The Growing Security Gap	4
Figure 2. Worm Penetration.....	5
Figure 3. Users Blame Worm Propagation on PCs	5
Figure 4. Impact of Insider Attacks	6
Figure 5. The Perpetual Security Cycle.....	7
Figure 6. TCG as the Foundation for Enterprise Security	9
Figure 7. A TCG-based Security Infrastructure Can Eliminate Security Attacks.....	11

Executive Summary

In today's globally connected world, businesses depend upon IT more than ever. Ironically, sophisticated and frequent attacks threaten IT assets - and confidential data - more today than ever before. This report concludes:

- **Security issues are universal.** Companies large and small spend billions each year on security yet attacks and their associated damages continue unabated.
- **Large organizations need a new security model.** Today's layered security based upon a "black list" (i.e. keep bad stuff from happening) is under tremendous pressure due to scaling problems and operational overhead. ESG believes that obsolete process must be replaced with a "Trusted Enterprise Model" based upon identity, trusted relationships, confidentiality, and integrity.
- **Users should base their security on a Trusted Computing Group foundation.** Rather than 'rip and replace' their current infrastructure, large organizations can build a trusted enterprise model over time by moving to technologies that support TCG standards. In this way, CIOs can take a grassroots approach, address high-risk areas on a tactical basis, and plan for a strategic architecture that encompasses the entire enterprise.

Technology and Business Realities

Few people would debate the profound business impact associated with technology innovation over the past decade. Compute power is ubiquitous, bandwidth is cheap, and the standards-based Internet simplifies system connectivity and integration regardless of physical location.

As a result of these overwhelming advances, business activities are firmly anchored by IT in order to improve productivity and lower costs. This relationship can be seen in areas like:

- **Real-time data sharing.** In an effort to accelerate and improve decision-making, many large organizations are exploring ways to gather internal and cross-company information in real-time. For example, in response to the global terrorist threat, the United States Federal Bureau of Investigation's (FBI) "Sentinel" electronic information management system is an ambitious effort to link multiple systems and provide global data sharing. The bureau plans to use the Sentinel infrastructure to replace legacy applications like its Automated Case Management System. The FBI example is not unique; private and public organizations are engaged in similar efforts around the globe.
- **Business Process Outsourcing (BPO).** Fueled by global connectivity and inexpensive off-shore skills, ESG estimates that the global market for BPO is approximately \$150 billion (USD) today and growing at approximately 17% per year. The most popular BPO services include customer care, finance administration, content development, payment services, and human resources.
- **Employee mobility.** Mobility is now reality. 15 million tele-workers depend upon remote access of network assets to get their jobs done each day. In total, 40% of employees at enterprise companies log onto corporate assets from remote systems like laptops, home computers or Internet cafes. This mobility is also moving beyond the PC alone. Mobile devices are growing at approximately 35% per year with converged devices (phone/calendar/e-mail) increasing at 50% per year. As network bandwidth continues to proliferate, user location and device type will become more and more irrelevant.

Several studies have concluded that the link between IT and business processes is responsible for a significant boost in productivity. A Federal Reserve Bank Analysis found that annual labor productivity growth for the U.S. non-farm business sector averaged 2.8% over the 1995-2000 period, double its average annual rate of growth for 1973-95. The 1995-2000 timeframe was also highlighted by roughly \$2 trillion in IT investment.

Technology Benefits Depend Upon Strong Security

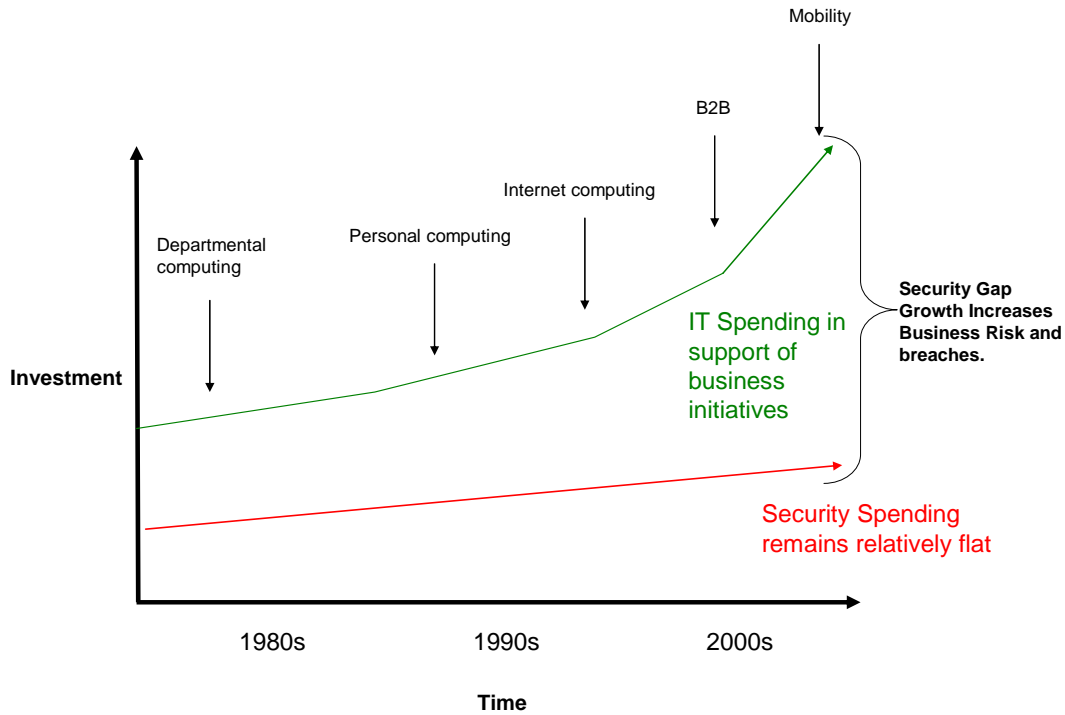
The technology industry has been quick to trumpet these compelling stories about the productivity, efficiency and cost savings derived from the technology boom but there is an ugly side to this expansion. Technology benefits depend upon a foundation of strong security protection and policy enforcement. Large organizations must have the tools to guard against security issues such as:

- **Compromised systems.** This is critical for several reasons. A single PC infected with an Internet worm can quickly impact devices and systems across an enterprise network while a computer compromised by a well-placed "back door" can be used to gather intelligence, attack other systems, or steal confidential data. Alleviating these risks depends upon the ability to inspect systems upfront, before it gains access to critical IT assets. This model is similar to searching airline passengers for weapons BEFORE they actually board airplanes.
- **Rogue devices and services.** To support new users and initiatives, large organizations constantly alter their technology infrastructure by adding new devices, systems, and services. If these persistent changes aren't carefully monitored, an intruder can introduce an unauthorized device, system, or service that can greatly increase the risk of a security breach. A marketing manager who installs a wireless access point to free her workgroup from their desktops may unknowingly open an attack vector for "war driving" (i.e. War driving is defined as the act of locating and possibly exploiting connections to wireless networks while driving around a city or elsewhere). This type of attack was used to break into the network of Lowe's, a U.S.-based chain of hardware stores.
- **Lost or stolen data.** In spite of the best security efforts, sometimes confidential data is simply lost or stolen. Government regulations like the California Database Breach Act (CA SB1386), the EU Privacy Act, or Canada's Personal Information Protection and Electronics Document Act (PIPEDA) mandate that these types of events must be disclosed whether from accidental loss or an electronic attack. This is precisely what happened to Citibank (lost backup tapes), Bank of America (lost back tapes), and Boeing (stolen laptop) (note: other prominent examples include notebook PC theft Wells Fargo with loan data, Los Alamos hard drives, Univ Calif. Berkeley notebook PCs with alumni information). These incidents proved extremely costly to the affected organizations.

Most Organizations Have a Long Way to Go

At least 130 reported breaches have exposed more than 55 million Americans to potential ID theft this year. This frightening situation exemplifies a growing gap between business-focused IT initiatives and the adequate level of security protection (see Figure 1). Just how bad is this situation? Data from several 2005 Research Reports demonstrates that companies large and small are overwhelmed by security issues that lead to damaging attacks.

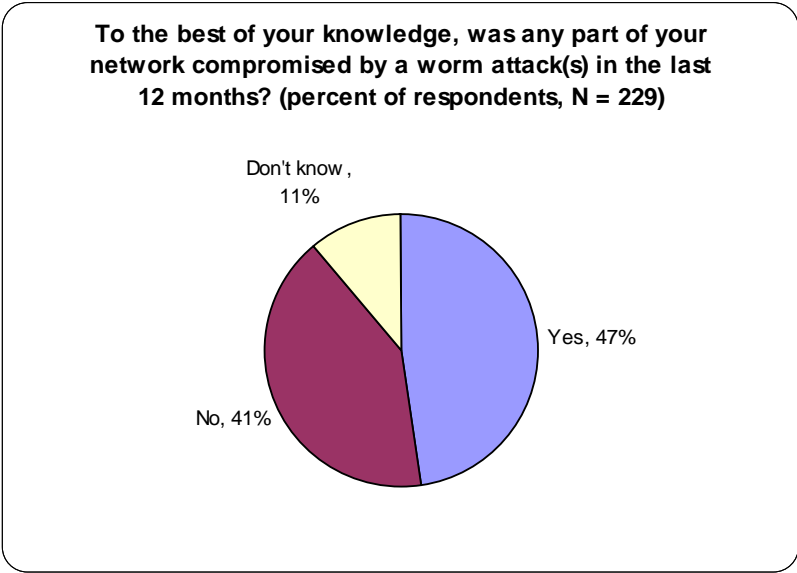
Figure 1. The Growing Security Gap



Source: Enterprise Strategy Group

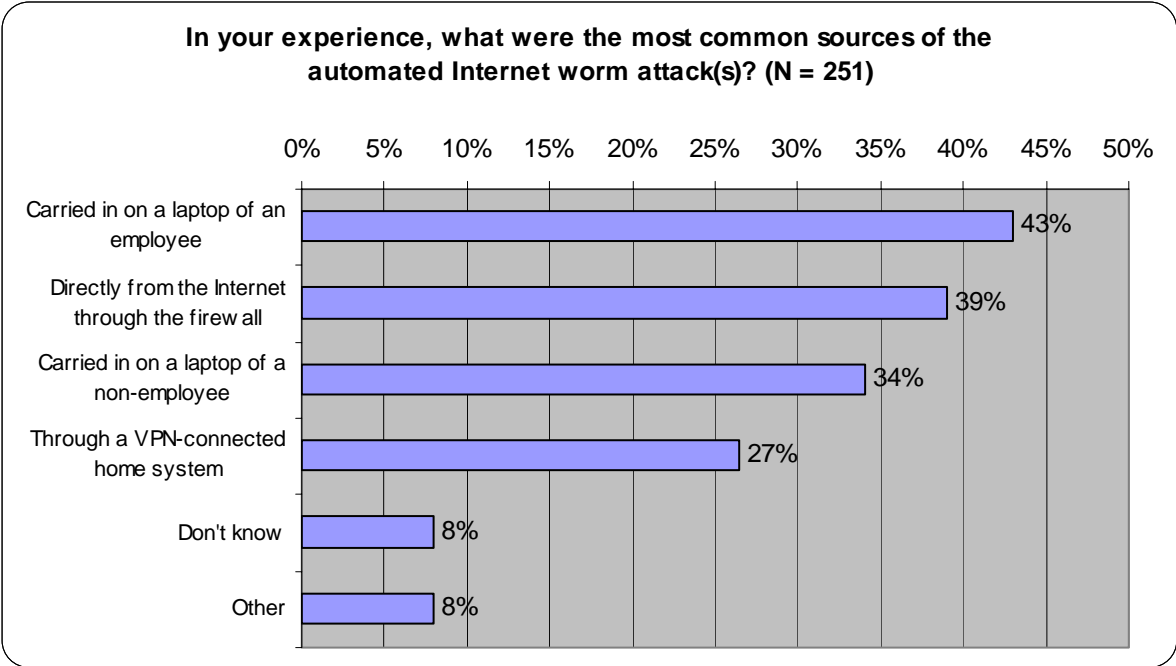
As explained above, compromised systems can disrupt IT activities, interrupt business operations, or lead to data theft. In spite of these devastating consequences, an ESG Research project found that 47% of companies said that a worm attack compromised some part of their network, while 23% of users said that their organization had suffered an internal security breach (see Figure 2).

Figure 2. Worm Penetration



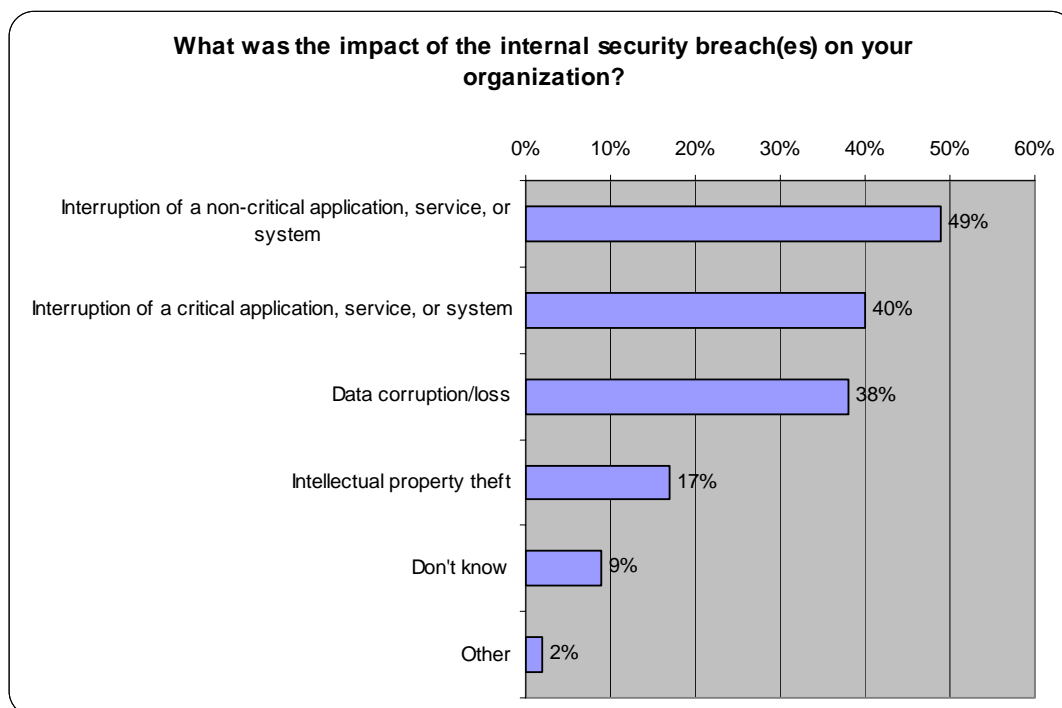
Where do these types of attacks begin? In terms of worm propagation, users believe that the primary source is an infected PC gaining access to the network (see Figure 3). This scenario is all too common for a simple reason; most PCs are not subject to any type of inspection before being granted network access. Again, this is analogous to providing passengers direct access from airport terminals on to airplanes with no security checkpoints.

Figure 3. Users Blame Worm Propagation on PCs



Security breaches like the ones described here can have a severe financial impact. For example, users claimed that insider attacks led to ramifications like the interruption of a critical business system and/or data corruption and loss (see Figure 4).

Figure 4. Impact of Insider Attacks

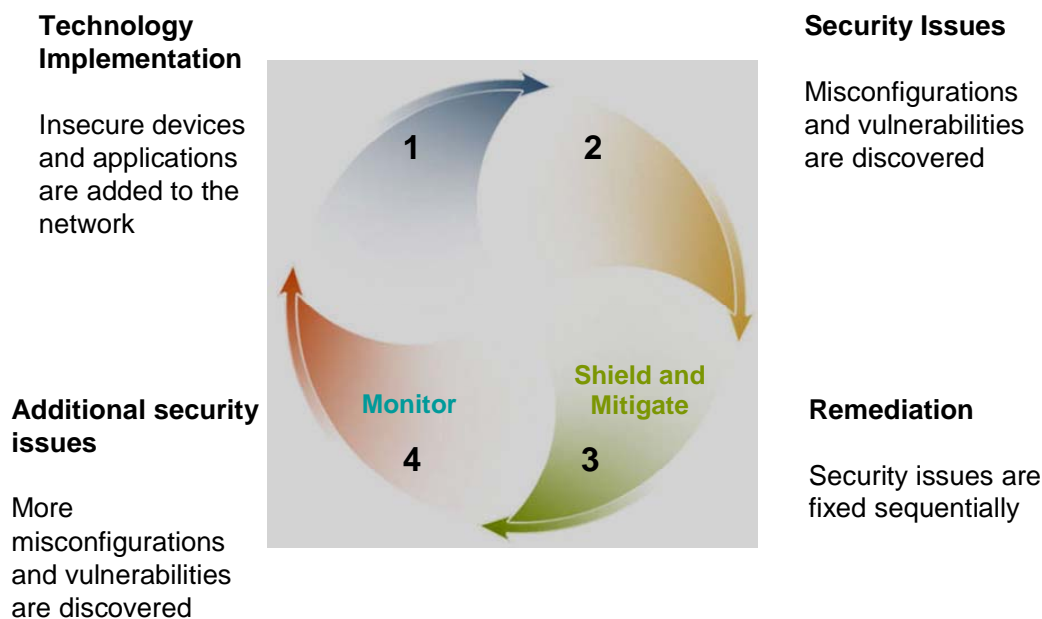


Why Are Things This Bad?

Large and small organizations spend billions and billions of dollars annually on security technology so why do they still suffer from damaging attacks? While an exhaustive study about security failures is beyond the scope of this paper, ESG believes that poor security is the result of a typical IT lifecycle pattern that goes something like this (see Figure 5):

1. **Insecure technology is deployed.** Historically, new technologies were deployed to address a specific issue and included little to no security protection.
2. **Security issues arise.** After the new technology is in place, someone realizes that it can be manipulated into doing something it shouldn't thus introducing a security risk. This could be a vulnerability like a software bug that allows outsiders to compromise a system a configuration error that allows users to access a critical system or service that they shouldn't, or a malicious code attack that forces a system to perform some type of malicious act.
3. **Security issues are addressed on a one-off basis.** High risk vulnerabilities tend to make alarms sound so they are generally fixed as soon as possible. Fixes can take the form of software patches from vendors, Access Control Lists (ACLs) that limit who can see what, or new security "signatures" written to identify and block specific types of attacks.

Figure 5. The Perpetual Security Cycle



Source: Enterprise Strategy Group

4. **More security issues arise with existing infrastructure while new technologies are deployed.** Inevitably, fixing mis-configurations and software vulnerabilities with existing technologies is a constant process. At the same time, large enterprises also deploy new insecure technologies. This cycle means that the security burden is constantly growing while remediation depends upon fixed resources and time. In other words, a bad situation grows constantly worse.

The model described here is sometimes also referred to as a "black list" approach to security. A "black list" is meant to identify and fix security problems as they arise. The more security problems there are, the longer the black list becomes. This method is fine if threats are relatively limited but it runs into scaling problems in a complex IT infrastructure with a multitude of attack vectors. A common security saying is that the security chain is only as strong as its weakest link. In a "black list" security model, a single missed vulnerability, configuration error, or "back door" can mitigate years of strong security efforts.

Enterprise Security Needs a New Model

The ESG data indicates that today's security complexity may be overwhelming traditional "black list" security models and it is likely that things will get worse - not better - over time.

One way to address this ever-growing issue is to turn the model upside down. Rather than base security on a "black list" approach that tries to identify and block things that should happen, why not utilize a "white list" model that defines the behavior that actually is allowed and blocks everything else? ESG believes that a "white list" or trusted enterprise model is far more compelling given IT complexity and constant flux. "Trusted" security has

been used effectively on a limited basis but to extend this model and make it a foundation for enterprise security, IT technologies must:

- **Include the concept of identity.** To prevent IT components from gaining malicious or accidental access to restricted areas, all technology piece parts need an identity - a unique and standard name proving that they are who they say they are. In the physical world, U.S. citizens have a unique Social Security number that has been used as a form of individual identity (author's note: the issues around Social Security Number theft and fraud are intentionally avoided in this analogy). IT devices, systems, and applications need this same type of system based upon unique identities.
- **Build upon identity with strong authentication.** To make identity a building block of security, it must be supported with a failsafe method of authentication where one entity can identify another entity with absolute certainty. This kind of authentication must be tamperproof to ensure that identities cannot be stolen, copied, or falsified.
- **Allow organizations to create trust relationships.** Once technologies have unique secure identities that can be authenticated, large companies must have the ability to map technology entities together to form trust relationships. For example, entity A and B could be grouped into an exclusive trust relationship based upon their identities. In this example, no other identity is trusted by either A or B and are therefore restricted from communicating with both. By defining who can participate in an activity, trust relationships preclude malicious outsider from gaining access to an IT asset and thus lower the risk of an accidental or intentional compromise.
- **Guarantee information confidentiality and integrity.** Once a trust relationship between entities is established, all subsequent communication passed back and forth must be protected against prying eyes. In addition, a receiver must have assurance that the information received actually came from the sending party and was not altered in any way while in transmission.

This security model is not new; this type of infrastructure is based upon security technologies like Private Key Infrastructure (PKI), digital certificates, encryption and hashing.

The Trusted Computing Group (TCG) and Enterprise Security

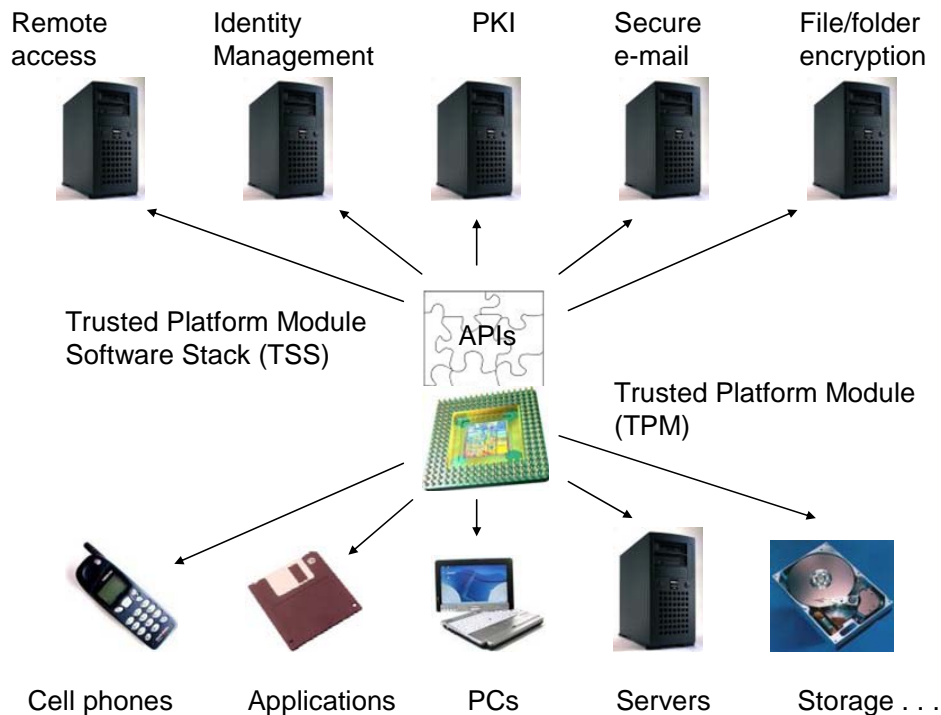
The technologies described above are readily available but they can be difficult and expensive to implement and operate limiting them to ultra-secure organizations like law enforcement, intelligence, and defense agencies. Why? Since technologies were never "instrumented" for security, establishing individual identities would require IT to retrofit every device, system, and application - a daunting if not impossible task.

Fortunately, there may be a solution to this untenable situation on the horizon from an unlikely source, an industry standards body. Enter the Trusted Computing Group, an industry standards body formed in 2003 to develop, define, and promote open standards for robust security technologies and trusted computing across multiple platforms.

The TCG model is based upon standards such as the Trusted Platform Module (TPM) and the Trusted Computing Module Software Stack (TSS, see Figure 6). TPM/TSS will not be layered on top of existing systems like most of today's security solutions. Rather, these standards will be added directly into IT assets as they are instrumented into Integrated Circuits (ICs), systems, and applications. TPMs from a number of semiconductor vendors are included today on new PCs and laptops, integrated into the motherboards of virtually all enterprisesystems from leading companies like Acer, Dell, Fujitsu, Hewlett-Packard, Lenovo, Toshiba and others.. As of the beginning of 2006, approximately 50 million TPM-based PCs have been shipped.

Just what does TPM/TSS do? Simply stated, TPM instruments hardware and software with core security technologies that can generate and store keys securely for use in digital certificates and encryption. These operations are accessed and controlled through standard TSS interfaces and readily available to security

Figure 6. TCG as the Foundation for Enterprise Security



management software for file/folder encryption, secure e-mail, identity and access management, and remote access.

TPM is inherently more secure than current software-based key management because the keys are stored in hardware in an encrypted format. In a PKI environment, private keys are never exposed to anyone. In this way, TPM's are virtually tamperproof. Compromising a TPM would require expert knowledge of microprocessors and a brute force attack on a sophisticated encryption algorithm. Even in this unlikely scenario, the world's most powerful supercomputers would require thousands of years to "guess" the value of an actual key.

TPM also supports the concept of "attestation" a method for measuring or fingerprinting the state of a system (i.e. describing the hardware and software that is or isn't installed on the system). Through attestation, one system can check the health of another to make sure that it conforms to security policy and does not contain any suspicious or unknown code.

There are a few other points worth noting about the work and philosophy surrounding TCG:

1. **TCG standards allow organizations to build a trusted enterprise model incrementally.** Since TCG standards will come free with new devices, CIOs can focus on tactical security areas in the short term and plan for more strategic enterprise efforts over time. For example, TPM/TSS could be used to address an individual area like laptop encryption to ensure that stolen systems won't lead to data

breaches and public disclosure. More strategic defenses like strong authentication and PKI can be added later without impacting existing security applications. In this way, a trusted model can be built as a phased project without the need for forklift upgrades.

2. **TCG is an opt-in model.** TPM/TSS must be turned on in order to work. In PCs, this is done through a pre-boot BIOS setup utility. The TCG standards mandate this on-site user implementation model in order to let individuals establish control, enable the chip and set up a baseline technology profile for attestation. This also ensures that no rogue application can compromise the TPM and that private keys are not actually generated until the user initiates this process.
3. **Third-parties cannot access TPM identities.** To avoid any privacy issues, the TPM 1.2 chip specification demands that manufacturers destroy their copies of TPM identities. This is done to ensure that identities remain secret and key sharing is controlled by the device owner. TPM compliance can be determined in an anonymous fashion through "zero knowledge" cryptography (i.e. a method of proving identity without disclosing confidential information).
4. **Encryption keys can be backed up.** Public/private key pairs are generated by TPMs and private keys remain secret forever as they are stored securely within the TPM itself. This is fine for PKI but if encryption keys are lost, critical information may become unreadable. To overcome this obstacle, TPM-based encryption keys can be backed up to a separate TPM for protection.

How TCG Will Enable a Trusted Enterprise Model and Improve Security

While TPM/TSS is available today on new PCs, the TCG has working groups established in order to extend this functionality to servers, peripherals, PDAs, digital phones, and storage devices. What's more, the TCG is also moving forward with its Trusted Network Connect (TNC) initiative, an open solutions architecture that enables network operators to enforce end-point security policies in order to either grant or deny network access.

Ubiquitous TCG devices will soon provide the foundation for trusted enterprise infrastructures built from the ground up for security. This could provide significantly better protection against a number of common attacks seen today (see Figure 7).

In this way, the TCG standards may act as the building blocks that change the way large organizations secure their critical assets and IT infrastructure. ESG believes that this trusted enterprise model can finally advance Information Security beyond today's inefficient layered and reactive approach.

Large Organizations Should Embrace TCG

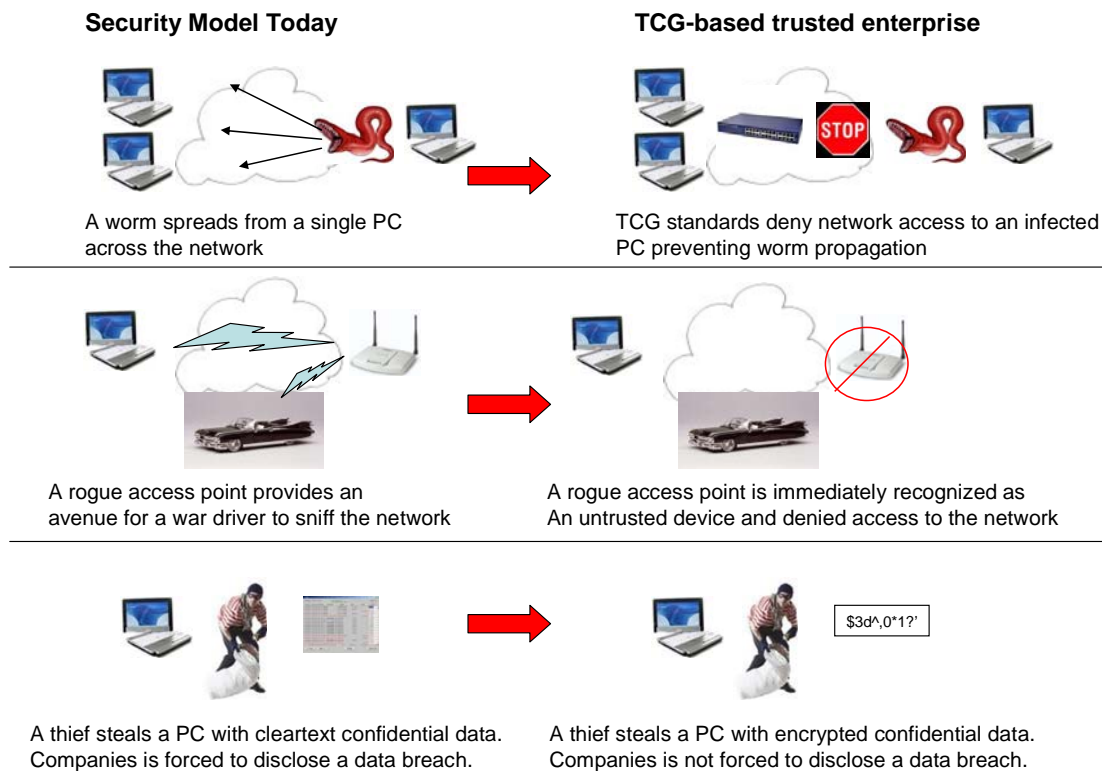
Today's security defenses are broken and it would take a massive effort to fix them. Rather than re-invent the wheel, ESG believes that CIOs would be far better off by embracing the TCG standards in their strategic plans in order to improve security organically over time. Business and technology executives should compile a TCG "to-do" that:

- **Mandates TCG standards in new purchases.** To plant the seeds for trusted enterprise IT, CIOs should make sure that any new technology purchases come instrumented with TCG standards. All RFIs and RFPs should mandate this requirement for starters. This is an easy step with PCs as all of the leading vendors already ship their systems with a TPM chip on-board. To cover other IT areas, technology managers should meet with their vendors to understand where TCG standards fit in their roadmaps.
- **Educate key personnel on TCG.** This requirement has broad ramifications across the organization. Obviously, IT, security and purchasing staff must understand TCG in order to purchase the right equipment, map out strategic security initiatives, and configure new products. Savvy companies will

also make sure to train legal and human resource professionals who can assess the impact of a trusted enterprise on privacy policies, workers rights, and International laws.

- **Offer a carrot and stick to vendors as they plan for TCG.** CIOs should share their strategic plans with key technology vendors to help them understand where TCG integration fits into their product roadmaps. As vendors hear more and more plans for TCG they will dedicate the right resources and place TCG standards in their product plans. Cooperative vendors should be rewarded with deals while laggards should be shown the door.
- **Explore TCG management options.** Embedded TCG standards depend upon management software that tells them what to do and how to do it. As such, smart CIOs should also base management software decisions of TCG support for activities like desktop encryption, network access, and authentication. There may also be a play to use TCG standards with other management activities like

Figure 7. A TCG-based Security Infrastructure Can Eliminate Security Attacks



software distribution, patch management, and asset management.

- **Assess and alter business processes for trust.** Informal but insecure business processes need to be addressed but doing so by introducing technology hurdles may alienate workers and slow productivity. Business managers should be included in the process here to examine where and how a trusted enterprise should be implemented while users need encouragement and training, not draconian impediments.

Bottom Line.

It's time that large organizations face the fact that today's layered security has outgrown its usefulness. This should not be cause for panic. CIOs should use this fact as an opportunity to engage business managers in an effort to develop a strategic security plan that protects business operations and critical assets.

ESG believes that future security will be based upon a trusted enterprise model and its key attributes of identity, defined trust relationships, confidentiality, and integrity.

While this is a fundamental shift that requires extensive planning, it does not translate into rebuilding the IT infrastructure to support security. A trusted enterprise model can be built over time by implementing new technologies instrumented for security. Large organizations can accomplish this organically by embracing the work of the Trusted Computing Group and implementing products with embedded TCG standards. As TCG-compliant technologies come on-line, CIOs can use the standards as a foundation for implementing tactical security solutions that reduce risk today while planning for strategic implementations that address security threats across the enterprise.