White Paper

The Trusted Computing Group (TCG) Storage Specification: Securing Storage and Information Lifecycle Management

By:

Jon Oltsik
Enterprise Strategy Group

January 2007

Table of Contents

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

Executive Summary

Confidential information is everywhere – spread from desktop to data center. Too often, this data is breached leading to expensive disclosures, embarrassing headlines, or costly intellectual property theft. Will this situation improve? The paper concludes:

- **Problems are widespread.** Large organizations provide confidential data access to lots of employees with mobile laptops so risks of a data breach are extremely high. At the same time, security professionals lack the right tools needed to monitor and enforce data privacy policies.

- **A new model is needed.** Layering tactical security products on top of IT infrastructure is expensive and ineffective. What's needed is a new model that instruments the IT infrastructure with fundamental security services. This will enable IT to provide user access and data confidentiality protection based upon trust relationships. ESG calls this model a trust-based architecture.

- **Storage can act as the "root of trust" for confidential data security.** Since confidential data resides on hard drives, storage should play a pivotal role in its protection. This can be accomplished by making storage devices the "root of trust" for systems, applications, and users. This fundamental step can help lock down access control, prevent tampering, and log all storage related activities.

- **The Trusted Computing Group (TCG) can provide the basic security plumbing.** The TCG has already successfully instrumented PCs with the Trusted Platform Module (TPM) providing functionality for identity, privacy, and system integrity. Now it is extending this support to storage devices. ESG believes that this could be a giant step forward for storage vendors and users in their quest to protect the storage infrastructure and implement secure Information Lifecycle Management (ILM).

Confidential Business Information

Over the past few years, IT spending rebounded from its low point after 9/11. Growth in IT spending is around 6% to 8% and should remain in this range through the end of the decade. While overall IT growth prospects seem to be on a slow and steady trajectory, enterprise storage capacity growth continues to demonstrate a much more robust increase. According to ESG Research, most enterprise organizations experience data capacity growth of at least 30% to 50% per year with no let up in sight.

Enterprise information growth isn't simply a function of capturing more and more digital junk like pictures, digital images, and mp3 files. In fact, ESG Research indicates an opposite trend – a large percentage of the total capacity of corporate data is actually considered confidential. In a recent ESG survey of 217 North American-based security professionals working for organizations with over 1,000 employees, respondents were asked to estimate how much of their organization's total data capacity would be classified as confidential. Nearly half of the respondents claimed that at least 50% of their data was confidential (see Figure 1).

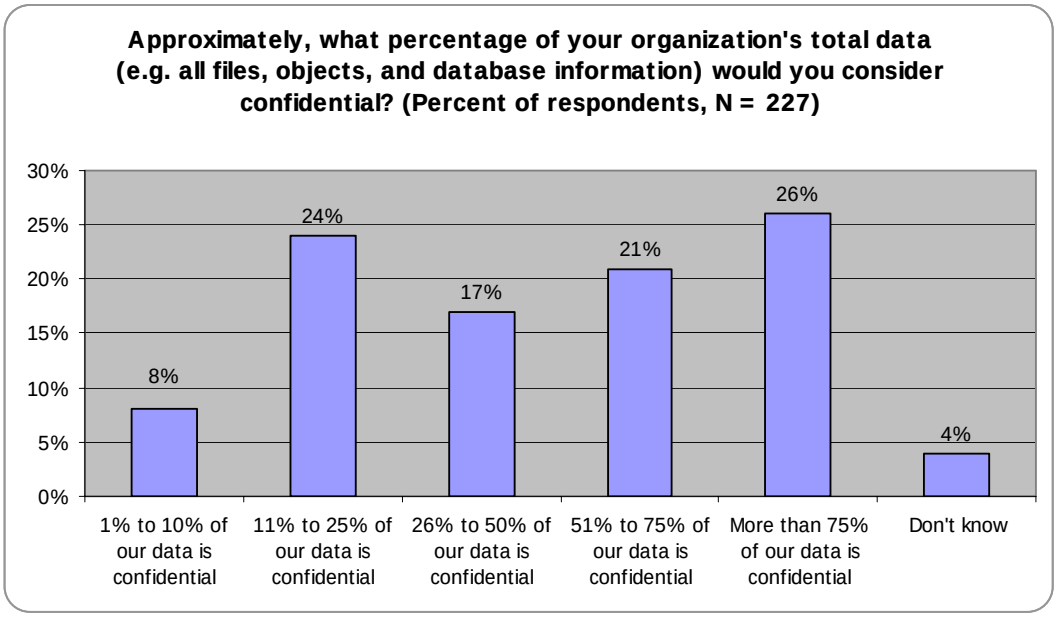
What's behind this high percentage of confidential information? Global organizations collect and use an ever-growing mountain of data for business-critical activities such as analyzing customer behavior, measuring business processes, and preparing for regulatory audits. Much of this data could be considered private (i.e. customer records, healthcare information, employee data), non-public private information (i.e. company confidential) or intellectual property.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

Confidential Data Remains at Risk

Data growth is a necessary outgrowth of a global information-based economy and as such, it is seen as an extremely valuable commodity. Unfortunately, the flip side of the increasing value of confidential data is additional risk. An accidental or malicious breach of regulated data can easily

Figure 1. Users Consider Most Data to be Confidential



cost millions of dollars while theft of Intellectual Property (IP) could quickly alter market shares, company capitalization, and long-term profitability.

With so much at stake, one would assume that large organizations monitor, manage, and protect their information assets with diligence and purpose. Unfortunately, this is not the case. For example, there have been over 300 publicly-disclosed data breaches in the United States since the February 2005 incident at ChoicePoint. These breaches resulted in the exposure of nearly 94 million American citizens' private data (source: Privacy Rights Clearinghouse, www.privacyrights.org). Why are things as bad as they are?

- **Confidential data is widely accessible.** At more than one-third of all large companies, at least 50% of employees have access to confidential data (see Figure 2a). This distributes the data around the enterprise and makes employees responsible for its protection. Little wonder why most security professionals believe that too many employees have confidential data access (see Figure 2b).

- **Mobility increases the risks.** Not only do employees access confidential data but they also store it on PCs, copy it to mobile devices, and carry it around on laptop computers. According to ESG Research there is a definite correlation between confidential data mobility and risk. When asked to identify where their organizations' confidential data was most vulnerable, security professionals pointed to laptops, desktop PCs, mobile devices, and portable media (see Figure 3).

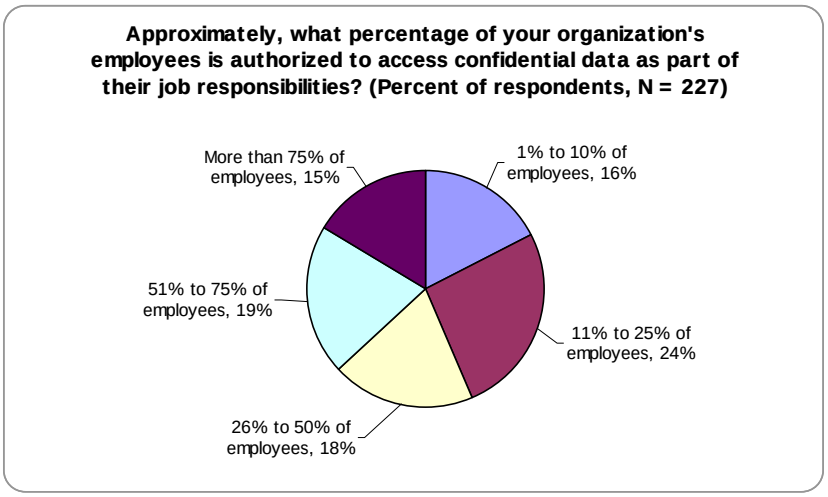
- **Large organizations do a poor job at monitoring and enforcing policies.** While most organizations have confidential data security policies in place, many lack the data and

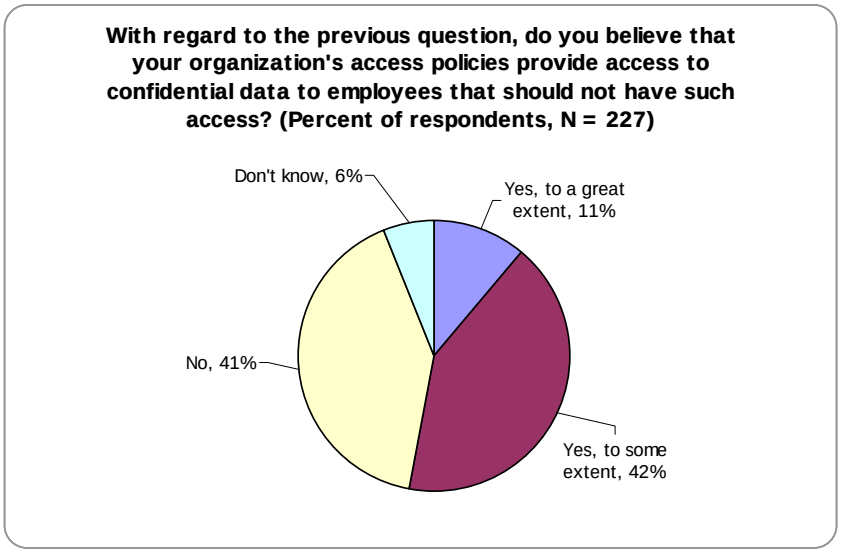
tools needed for policy monitoring and enforcement. This makes important policies little more than pieces of paper.

- **Storage security is rather new.** In the past, many enterprises applied security defenses to host computers and PCs but left the storage itself unprotected. Unfortunately, this led to damaging breaches related to lost or stolen laptops or inside jobs perpetrated by malicious storage administrators. Secure storage options are available today but this is a relatively recent phenomenon with limited implementation.

These shortcomings are not trivial. ESG estimates that the cost of a publicly-disclosed data breach ranges between $25 and $150 per compromised customer record. These costs include things like customer notification, postage, credit protection services, legal fees, and public relations. Total cost per compromised customer record ranges based upon the size and location

Figure 2a and 2b. Employees Access to Confidential Data



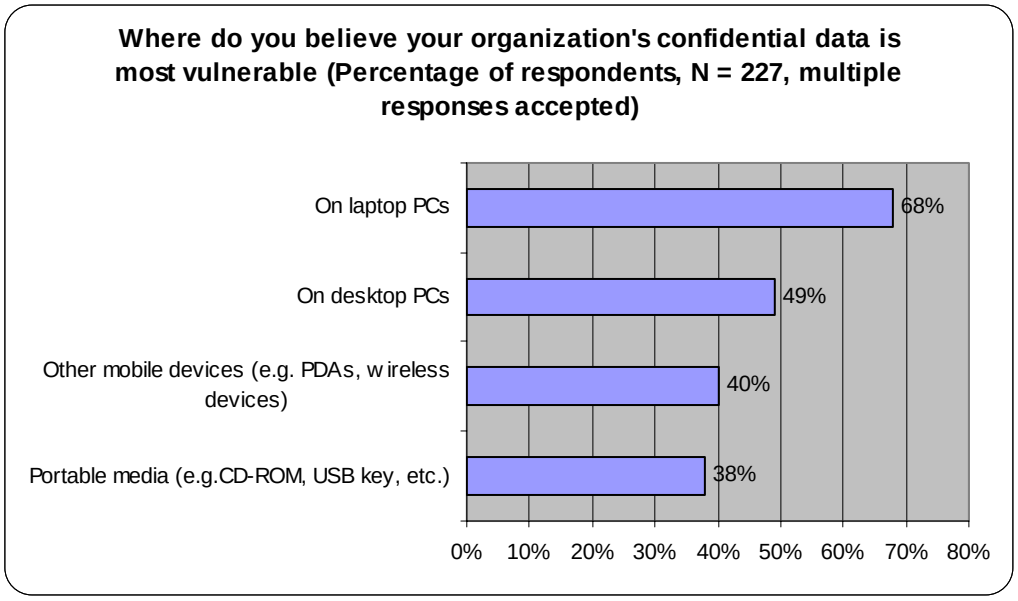


of the compromised organization, the number of regulations violated, pubic relations programs, etc. Based upon these estimates the total cost of exposing the private records of 94 million American citizens was between $2.4 and $14 billion.

What's Needed? A Trust-based IT Architecture

Protecting confidential data is a business-critical activity and should be a major pillar of any enterprise IT infrastructure. This has not been the case in the past where information security tools were often built on top of existing IT components on a tactical basis based upon the security

Figure 3. Mobility Increases Confidential Data Vulnerability



threat of the day. Layering on more and more security tools can quickly become too expensive and operationally challenging to be effective or feasible.

In order to address the growing risks to confidential data effectively, ESG believes that IT vendors and end-users must embrace a new model where security becomes an essential service built into the entire IT infrastructure. ESG calls this a trust-based architecture. In this instance, the word "trust" is defined as the access and permissions that one entity (i.e. application, system, or user) has with another.

Current IT technologies tend to disregard trust and minimize security. Even sophisticated IT architectures are based upon an ever-changing network where devices are implemented insecurely and configuration changes go undocumented. User provisioning tends to be a manual task involving multiple IT and business groups while authentication is still dominated by the insecure combination of user name and password. In order to provide some level of protection, security defenses are frequently layered on top of multiple functional technologies willy-nilly with no particular master plan.

As opposed to today's haphazard approach, a trust-based architecture:

- **Is based upon identity.** To understand communications and configurations, every user, device, and system peripheral is given a tamperproof identity that must be registered and approved before any access is provided. In this way, one identity can be given specific permissions to communicate with another within a formal and well documented structure – not a bunch of useless policies and best efforts.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

- **Manages relationships.** Once every user, device, and system peripheral has an identity, IT can set up trust relationships based upon business requirements. This means that a new trust relationship must be created when a new user is provisioned to a certain role or a disk drive is added to the storage system. This process can maintain security throughout IT by setting up a "chain of trust" (aka "transitive trust"). If network device A trusts server B which trusts disk drive C, then network device A also trusts disk drive C. Every relationship is authorized and documented from end-to-end. Alternatively, nothing happens without a trust relationship in place.

- **Provides on-going and accurate logging.** Since all identities and relationships are predetermined, logging activities should provide a detailed picture of behavior and activities. This creates a trust map for security management making security breaches more difficult while easing forensic investigations.

- **Guarantees data confidentiality and integrity.** Once a trust relationship between entities is established, all subsequent communication passed back and forth between trusted entities can be encrypted and integrity-checked in order to make it tamperproof and protect if from network sniffing or man-in-the-middle attacks. Only trusted end points have the ability to encrypt and decrypt point-to-point communications.

At the foundation of a trust-based architecture are technologies such as digital certificates, digital signatures, and PKI that can enable identity, encryption, data integrity, and non-repudiation functionality. Since these technologies are essentially "baked" into the IT infrastructure, they provide common and standard services for any system, business application, or management suite. This should normalize data across multiple systems while easing system integration burdens created by multiple proprietary technologies.

The Trusted Computing Group's Role (TCG)

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 requires IT to retrofit every user, device, system, and application for identity and trust.

ESG believes that the Trusted Computing Group (TCG), a technology industry non-profit organization formed to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies, has a potential solution to this technology conundrum. The TCG model is to instrument hardware and software with core security technologies that can generate and store keys securely for use in establishing identity and protecting data. These operations are accessed and controlled through standard software interfaces and readily available to security management, device management, or application software.

The most widely-deployed TCG standards to date are the PC-based Trusted Platform Module (TPM) and the Trusted Software Stack (TSS). TPM/TSS is instrumented into Integrated Circuits (ICs), systems, and applications and is readily already available today on new PCs and laptops as it is built into microprocessors from AMD and Intel and systems from leading companies like Acer, Dell, Fujitsu, Hewlett-Packard and IBM. As of the beginning of 2006, approximately 50 million TPM-based PCs are deployed worldwide and the resident TPM chips can be used for device authentication, rogue software detection, and secure credential storage.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

TCG Extends Its Model to Storage

A trust-based architecture depends upon a chain of trust where multiple systems, applications, and devices are bound by formal and tamperproof trust relationships. This is also the TCG vision. To that end, the TCG recently published its Storage Work Group, specifications which can be viewed as an extension of the existing TPM model. The Storage Work Group specifications provide 3 main security/operational benefits:

1. **Introduce the concept of trust relationships between storage devices and hosts.** Through mutual identity, authentication and trust of hosts and storage devices, the trust environment is extended beyond the TPM and into storage devices themselves. This limits who can read or write to a device.

2. **Enable secure control over storage device features.** TCG-enabled storage can place storage devices in a "trusted state", enabling specific configurations or security features. In this way, TCG-enabled storage provides protected storage for specific users, systems or applications and also allows exclusive control over data-at-rest encryption on storage devices.

3. **Create secure communications between storage devices and hosts.** Secure storage provides session-oriented security commands on top of general host to storage communications through security extensions of SCSI (ANSI/INCITS T10) and ATA (ANSI/INCITS T13).

In the TCG model, storage can become the actual "root of trust." In other words, storage devices (and sub-partitions of storage devices) can be configured to communicate with other trusted entities (applications, systems, users, etc.) and enforce security policies.

Like the PC implementation, TCG-enabled storage hard-code security functionality into device-resident security processors and firmware and thus cannot be moved or altered in any way. TCG-enabled storage devices contain cryptographic engines (i.e. for PKI and encryption) and enable different trust-based applications for protected storage. Security services are called through specific APIs, which isolates storage functions behind a "trust boundary." Only trusted entities with access and authorization to the API can see and use the TCG trusted storage functionality.

TCG-enabled Storage Can Help Improve Overall Storage Security

In the past, many storage vendors were slow to recognize growing security requirements but the industry has become far more proactive. Why? Regulatory compliance demands that storage systems support stronger authentication, access controls, while risk-averse business leaders are pushing security agendas to steer clear of embarrassing headlines. In response, storage vendors have been busy bolstering product defenses and acquiring security companies. In their quest to improve security, ESG believes that storage providers should actively embrace TCG-enabled storage as it can help them deliver (see Table 1):

- **Granular storage security configuration enforcement.** TCG-enabled storage provides a framework for granular role-based configuration management and change controls. For example, individual storage functionality 'containers' (called service providers or SPs by the TCG) on the storage device are "sand boxed" and exclusively controlled by a designated owner. This provides extremely tight control over storage assets and functionality where access control is based upon credentials. This would greatly improve storage security control and configuration management.

- **Improved storage access controls.** To protect storage from rogue applications and systems, storage administrators use a combination of zoning, LUN masking, and access

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com

control lists. TCG-enabled storage takes existing access control methods one step farther through the concepts of enrollment and connection. In simple terms this process can map specific hosts to specific storage devices and/or specific storage devices to specific hosts. The TCG-enabled storage provides more granular mapping as well where specific users, systems, or applications can be allocated a protected storage location.

- **Scalable device-level encryption.** Encryption is a major component of protecting confidential data. TCG-enabled storage provides an on-board encryption engine for high-speed encryption at the device level. This can help overcome the performance and scalability problems often associated with encryption. Cryptographic operations are handled by a dedicated processor in the drive itself, obviating the need for cryptographic software or appliances. What's more, since encryption is done on a drive-by-drive basis, encryption capacity scales with the addition of new drives. The TCG storage model complements encryption with read- and write-locking. Certain users or applications can access data on storage devices but cannot alter it in any way.

- **Automated backup.** TCG-enabled storage can enable backup from one secure "service provider" (i.e. storage sandbox) to another. In this scenario, the SP owner must have access to another SP with registry capabilities on another storage device. With this permission in place, TCG-enabled storage can mirror SPs on one or multiple other devices.

Table 1. TCG-enabled Storage Can Help Overall Storage Security

TCG-enabled storage function	What it does	How it enhances current storage security
Granular storage security configuration enforcement	Provides security service providers (SPs) based upon authentication and authorization	Enhances the security of storage system configurations and change controls
Improved storage access controls	Creates secure storage based upon trust relationships	Adds to existing access controls such as zoning, LUN masking and ACLs
Scalable device-level encryption	Instruments storage devices with on-board cryptographic processing	Provides a standard callable cryptographic service for management applications.
Automated backup	Creates a secure mirror image of an SP on multiple storage devices	Provides a standard callable mirroring service for data management applications

In total, TCG-enabled storage helps to lock down storage infrastructure and the data that resides on it. Access controls are based upon establishing trust relationships which are authenticated at run time with credential checks. These tight controls make the possibility of an accidental or intention breach of storage infrastructure or valuable data far more remote.

TCG-enabled Storage and Information Lifecycle Management (ILM)

In addition to offering basic storage hardware and software, storage industry leaders are developing new ILM products that automate the classification, movement, tracking, and storage of disparate data sets through various life cycle phases from creation to deletion. When this concept was initially proposed in 2003, the lack of security protection built into the model was striking. ESG quickly pointed out this security deficit and coined the infamous quote, "without security, ILM is DOA."

Three years later, ILM has been enhanced with security features but actual implementation remains an issue. TCG-enabled storage could help overcome these problems through its support of (see Table 2):

- **Distributed cryptographic and key management services.** ILM will demand that critical data is copied, verified, distributed, and encrypted. Managing multiple copies of documents and their associated encryption operations could mean managing multiple redundant encryption systems creating an operations nightmare. Additionally, if encryption keys are somehow lost, it could render critical data unrecoverable. TCG-enabled storage promises to ease the ILM key management burden by baking cryptographic services such as signing, hashing, verification, and encryption into the storage infrastructure. Smart ILM vendors can utilize the storage device's base level cryptographic services and focus on key and policy management rather than storage layer encryption services.

- **Pervasive logging.** Similar to cryptographic services, trusted storage will also support logging and clocking capabilities. With this infrastructure already in place, ILM vendors can focus on log aggregation and analysis rather than basic data collection.

Table 2. TCG-enabled Storage Can Help Enable ILM

TCG-enabled storage function	What it does	How it enhances ILM
Distributed cryptographic services	Provides cryptographic services for signatures, hashing, encryption, key management, etc.	Provides a standard callable cryptographic service for ILM policy and management applications.
Pervasive logging	Captures log data on a device-by-device basis	Provides a standard callable logging service for ILM reporting and auditing.
Operationally efficient data deletion	Deletes encryption keys associated with storage devices rendering data unrecoverable.	Offers a practical data deletion method for day-to-day operations

- **Operationally efficient data deletion.** When users want to retire or move storage devices they are faced with a multitude of choices for data deletion – from physical device destruction to full compliance with the Department of Defense DoD 5220-22.M process. These may not be the best choices for everyday moves, adds, and changes. Physical destruction means demolishing potentially useable assets while DoD 5220-22.M requires costly certification and validation. TCG-enabled storage provides a more pragmatic option, guaranteed destruction of encryption keys; a more practical and cost-effective way to deal with day-to-day enterprise needs.

Ultimately both ILM vendors and users will benefit from TCG-enabled storage devices. ILM vendors can accelerate security enhancements by building management functionality on top of the TCG API and utilizing the TCG security plumbing. For users, TCG-enabled storage should ease the inevitable interoperability problems posed by multiple ILM implementations since products will call the same APIs, use the same commands, and harvest the same device-resident data.

The Bottom Line

Business demands that drive data creation also make information a mission-critical asset. As such, company confidential and private data should be protected at all costs – sadly, this is not happening. Today's security methods are too tactical and costly to address the growing need for confidential data security.

Rather than continue to layer on additional security products, ESG believes that a trust-based security architecture is needed. This means instrumenting devices, systems, and applications with a foundation of trust technologies for identity, authentication, and data privacy. This would free users and vendors from developing "security plumbing" and instead focus on security policy monitoring, enforcement, and management.

The TCG shares a similar vision of a trust-based architecture. The standards group has already established itself with the ubiquity of the PC-based TPM chip. It is now extending its trust model to various types of storage devices. ESG sees this as a real step forward. TCG-enabled storage promises to enable a number of useful new security services for storage and ILM. As such, IT executives and technology vendors should be motivated to participate and support the TCG effort.

20 Asylum Street, Milford, MA 01757 ● 508-482-0188 ● www.enterprisestrategygroup.com ● info@enterprisestrategygroup.com