

WHITE PAPER

Infrastructure Integrity

Sponsored by: Tripwire

Charles J. Kolodgy

October 2004

INTRODUCTION

The strategic and tactical human capital required to administer, maintain, and protect enterprise computing systems in today's IT environments is consuming corporate resources at an ever increasing rate. Implementing an IT infrastructure that provides a high degree of availability, security, and regulatory compliance is a battle that corporate enterprises are fighting globally.

During each stage of progression in distributed computing, new dimensions in features, functionality, and capabilities have been introduced and made available to users. As a consequence, an entirely new set of risk factors has come into the already complex IT picture. IT organizations are dealing with a staggering number of issues, including:

- Industry standards and best practices along with evolving state, federal, and regulatory agency compliance requirements
- The rollout of new and enhanced systems and application software and the maintenance of legacy applications across an increased number of systems
- Viruses, trojans, hacking, and other malicious demons
- Staff training and turnover

Each of these critical areas is in a constant state of flux, with a constant barrage of new innovations and products. As the benefits of the progress afforded by the new IT infrastructures have been realized, so too have downside consequences emerged. To meet these issues head on, IT managers need to build a solid foundation upon which a coherent, secure, and functional network can be deployed, maintained, and updated. The keystone of that foundation is infrastructure integrity.

METHODOLOGY

IDC produced this document using a combination of ebusiness and security market forecasts, quantitative customer surveys, and direct primary research. To understand the most important issues challenging serious implementers of base footprint management policies, tools, and practices, we conducted in-depth, qualitative discussions with CTO/CIO-level experts, exploring the particular issues and challenges they found most pressing. In addition, designers and implementers of IT infrastructures shared perspectives on the practical issues involved in designing and maintaining the establishment and management of integrity within the IT infrastructure. This document reflects these research perspectives.

IN THIS WHITE PAPER

This paper outlines the nature of infrastructure integrity and change auditing solutions and describes how investment in change auditing technologies can stabilize IT operations, lowering the operational costs associated with IT infrastructure and providing a solid foundation that increases the effectiveness of investments in information security. A specific focus is directed toward describing the dynamics of infrastructure integrity and outlining the unique solutions provided by Tripwire.

PERSPECTIVES FROM THE "FRONT LINE"

Competitive business pressures, reduced time to market, regulatory compliance, and innovative methods of reaching customers, vendors, and partners all create constant IT change. This constant stimulus makes quality of life a challenge for IT managers.

The Innovators Dilemma

The IT infrastructure has grown to nearly overwhelming dimensions. As one veteran IT manager put it:

It used to be that you could ask me anything about my system — the IP address, what kind of software is installed, what patches are installed. I would know it from memory. You knew the edges of everything you had. Systems administrators aren't really like that today. There's a lot of complexity there that we are not in control of, and we are accountable for thousands and thousands of systems but do not have control of them.

A great deal of the complexity of networks has been driven by the need to "just get it done." This mindset has tolerated frequent circumvention of change control policies and best practices and created "kludges" to hardware and software designed to get to market quickly. Network vulnerability and instability has become much more prevalent as businesses have been seduced by a whirlwind of technology enhancements. Systems administrators, the front-line IT defenders, hold the final responsibility for implementation and ongoing management of this complexity.

For the IT manager and front-line IT defender, there is rarely time to document the "standard build" or conform to all change management policies. As a result, it is extremely difficult to determine what the desired state of the system is today or what it should be in the future. In addition, because of this lack of a common reference point, firefighting is the norm in IT. This does not allow IT to properly innovate and "raise the bar." When excessive firefighting exists, there develops a lack of confidence in the integrity of IT infrastructure and, by association, IT leadership. This is the crux of the innovator's dilemma.

Pillars of IT Initiatives

Business and environmental factors driving IT initiatives today can be categorized into three focus areas, or three pillars of IT: integrity, security, and compliance. These are fundamental IT areas of focus and discipline for enterprise IT management.

Pillar 1 – Integrity

Integrity issues arise out of the constant changes of software, firmware, and configurations occurring within an IT infrastructure. The integrity challenges for IT management and administrators are to account for and verify the validity of every change in these areas and to proactively deal with drifts away from desired states.

Pillar 2 – Security

Security issues arise out of the threat of malicious and nonmalicious attempts by intruders to penetrate external and internal perimeter defenses. Security challenges for IT management and administrators are to proactively thwart unauthorized intrusions and to quickly and effectively identify and react to any breaches.

Pillar 3 – Compliance

Recent and existing state, federal, and regulatory agency acts have made corporate executives responsible for the proper control and accuracy of protected information held and processed by the organization. The challenge for IT management is to ensure compliance through operational best practices and audits.

Integrity

What is overlooked in most cases is the integrity of the foundation upon which the critical IT infrastructure is built. Because of the complexities of IT software, it is becoming more difficult to know for sure what constitutes a "desired state" or baseline for server and network configurations, database management systems, and applications. An IT manager for a service provider stated that one vendor's Unix server software contained 30,000 files per install. Even after removing those that were not required for the specific task, there were still 16,000 files remaining.

To add to this complexity, commercial software itself is not always reliable. Operating systems and applications are complicated pieces of software that sometimes contain defects or bugs. System software is patched to correct problems. The patches themselves can sometimes cause problems with other software. Because of the inherent complexity of software, it is possible for it to be corrupted, lost, or deleted.

The difficulty in hiring and retaining IT staff is another integrity concern that is generally not addressed effectively. IT staff must be able to deal with the increased complexity of the systems. Yet, at the same time, they are required to protect corporate assets while opening corporate networks to customers, vendors, and partners. The scope is too large for the existing IT staff; therefore, process improvements and internal controls are required to make all the new business requirements possible while maintaining an acceptable level of integrity, security, and compliance.

Integrity Drift

"Integrity drift" refers to movement away from a specific desired state. The drift of IT assets comes about from both technical and procedural issues. One company's information security executive related that, when he came onboard, his organization had 200+ servers, each one configured differently than the rest. The varied machines also were not properly maintained. The company had a lot of operations staff focused on deployment, but there were no system administrator resources to maintain the machines. The CIO described the feeling of his lack of control of the assets by stating, "When I joined, it was clear that, well, the machines weren't really ours anymore."

From an operational controls perspective, drift can occur because roles and responsibilities for many routine functions are not established or enforced. At the company mentioned above, system engineers often built and deployed machines but did not maintain them. The operations staff wanted to take over certain systems in the field, but engineering wouldn't relinquish control. The problem with this is that both departments had access to the machines and were making changes without consulting each other. The result of this gap in communication is that control over the integrity of the system was completely lost.

How to Return to Integrity

How is integrity ensured? Through change auditing technology. "Elegant in its simplicity," this technology's function is to maintain infrastructure in a desired state. It works by, first, establishing the baseline of a desired state for any object (e.g., file system, system registry, and configuration file) or for any piece of infrastructure (e.g., server, workstation, database, router, and firewall).

After the desired state has been established, periodic comparisons can be made between the current state and the baseline state. Any deviations are flagged for an "integrity check," and alerts are sent to appropriate parties, so rapid correction and recovery can occur. Integrity drift can be identified quickly so as to expedite a return to the "desired state." IDC believes that the simplicity of this approach is powerful and, if implemented across all IT infrastructures, will protect security investment and increase confidence and trust in IT infrastructure.

Some specific business challenges solved by change auditing are:

- ☒ **Change controls.** It is no secret that software is ever changing. By anchoring software with technology (establishing a baseline of the intended, authorized state prior to putting infrastructure into production), it is possible to detect undesired changes that would normally be undetectable. Discovery and correction in a proactive manner will save time and money. This principle extended to operational activities (e.g., patch management and release management) gives IT operations a predictable, efficient way to ensure that they know the states of their key IT assets.

- ☒ **Operational controls.** It is possible to establish policies that can improve the efficiency of the IT staff and their processes. A large stock exchange that operates 24 hours a day runs three eight-hour shifts in its datacenter. Prior to "turning over the keys" to the next shift, the IT operations team runs a check to ensure that all server configurations are within expected parameters. When the check is completed, they know if anything changed on any of the servers outside of acceptable bounds. If anything is awry, the shift change does not occur. This ensures that the team responsible for the overall health of the infrastructure is not just accountable, but also empowered to maintain the integrity of its systems.

- ☒ **Asset management controls.** The first day on the job, a CFO navigates the landscape by inventorying assets, reconciling with the balance sheet and focusing on keeping surprises small. On the CIO's first day, he can count hardware, staff, and inventory software licenses, but he can usually identify very little else. CIO surprises tend to be large and difficult to reconcile. When one CIO came onboard, he knew how many servers the company physically had, but he didn't feel like he "owned" them until after establishing an integrity baseline. Through the establishment of a change auditing policy, information assets can be controlled and monitored in a fashion similar to managing a balance sheet and general ledger. In a public company, it is the fiduciary responsibility of a CFO to maintain financial integrity; it would follow that it is the fiduciary responsibility of a CIO to maintain infrastructure integrity.

Security

From the computer room to the boardroom, people are all too aware of active security threats such as viruses, worms, unauthorized intrusions, and denials of service. As companies become more reliant on the information contained within their IT systems, the damage that a threat can cause is considerable. To mitigate the risks, organizations apply significant resources on to security technologies and in the process develop a false sense of confidence that their IT infrastructures are becoming more secure.

Security, by definition, is reactive, periodic, and in place "in the event of." In addition, traditional perimeter defenses (e.g., firewalls, intrusion detection and prevention, virus scanning, and encryption) can mitigate only some of the risks of conducting business on the Internet.

This phenomenon has caused the growth of solutions that assure the integrity of systems on a continuous basis and focus on keeping the entire infrastructure in a "desired state." Assuring infrastructure integrity is salient to stakeholders like the CIO, especially because the degree of infrastructure integrity is directly correlated with the degree of confidence an enterprise has in the IT organization and, therefore, in the leadership of IT.

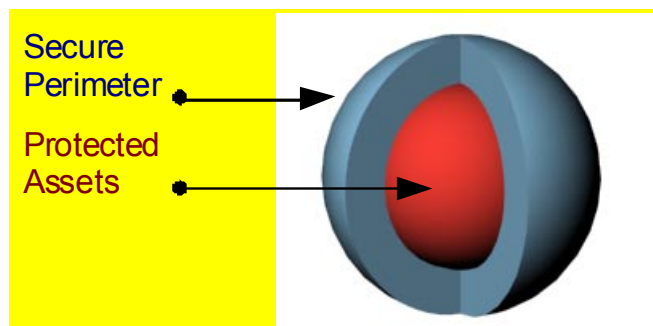
Why Is Perimeter Security Technology Not Enough?

The original network security architects were government agencies and defense contractors who were experts in handling confidential assets. Their training led them to create strong information security perimeter defenses. As long as the perimeter was secure, the assets being protected didn't need to be monitored or managed for integrity, because the command and control environment gave people assurance that core data was safe.

This is illustrated in Figure 1. The hard outer shell at the perimeter protected the soft, malleable data that needed to remain secure. Ironically, integrity — the protection of data and resources from unauthorized modification — has been one of the four pillars of conventional security. However, the approach had been to achieve integrity through tight restrictions of access, cryptography, and offline audits.

FIGURE 1

Early Perimeter Protection Model

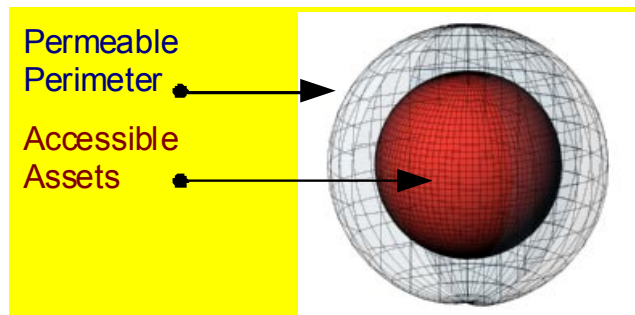


Source: IDC, 2004

In today's business climate, an enterprise must now grant (restricted) access to customers, vendors, and partners. There is no longer a hard, protective shell, but rather a porous membrane that grants access into different levels of the network (see Figure 2). One large financial institution articulated it this way: "Perimeter defense based on firewalls is still important, but more sophisticated security systems are needed, because we don't even know where the perimeter is anymore."

FIGURE 2

Today's Accessible Asset Integrity Model



Source: IDC, 2004

With the new emphasis on access through an ever-changing perimeter, the real security challenge becomes one of ensuring the integrity of core assets, not one of sealing off access to the environment. This requires changes in what is considered security. There must now be more emphasis on availability and continuous infrastructure integrity.

Executives are primarily concerned with growing their businesses. In order to reach that goal, IT security and infrastructures need to provide value by being business enablers. A high degree of confidence in the integrity of systems is paramount for business enablement. Today's customer-centric environment requires that change auditing solutions become statutory as part of robust information security strategies.

Compliance

Maintaining sound business practices and procedures has always been important for enterprises. However, a wave of industry and government mandates is making compliance a key issue for many organizations across all industries. Although most of the laws and regulations are not aimed at IT managers, IT does bear the weight of compliance, because it holds responsibility for information integrity and safeguarding information assets.

IT is a critical component of strategic compliance initiatives because it must sustain compliance-related process controls, mitigate risk, and manage ongoing costs. Compliance with new government regulations is forcing many organizations to reevaluate their overall business practices and the IT systems that support them.

Industry Process and Control Frameworks

For years, enterprises have worked to improve service availability, enhance security, and control rising IT operations costs by adopting and implementing industry best practices and standards. Now under the pressures of compliance requirements, these frameworks are the critical guides to IT operations and security professionals in meeting their compliance needs. The three key industry frameworks are:

- ☒ **IT Infrastructure Library (ITIL).** The ITIL is a best practice for IT service delivery and infrastructure management. By incorporating ITIL practices, organizations can identify procedural gaps and redundancies, reduce costs, and provide for maximum efficiency and control over the way changes are managed, software is released, and incidents and problems are handled.
- ☒ **Control Objectives for Information and Related Technology (CobiT).** The CobiT framework is an open standard for IT security and control practices that defines a methodology for controlling and assessing the effectiveness, efficiency, integrity, reliability, availability, compliance, and confidentiality of IS resources. It includes audit guides for more than 30 IT processes.
- ☒ **ISO 17799.** ISO 17799 is an international standard that defines best practices for information security. Some of its areas of control are security policy, asset control and classification, communications and operations management, and systems development and maintenance. By adhering to the standard, organizations can improve their overall security postures, enhance security planning and management, and experience more reliable security audits.

In addition to these recognized standards, a number of influential companies are requiring trading partners to document and audit security practices and internal process controls prior to allowing network connectivity. Companies such as Visa, MasterCard, and Wal-Mart have provided standards upon which other companies must comply to be given direct access to corporate IT resources. IDC would expect this trend to continue as data becomes more transient even among other companies.

Regulatory Compliance

Regulatory compliance can be defined as the management function that respects and abides by all applicable legislative regulations, focusing primarily on ensuring that all rules and regulations are followed. At its most basic, it is a mandate for a specific set of businesses to meet a specified set of objectives with the intent of protecting or enhancing the public good.

The interest in regulatory compliance is fueled by a recent expansion in what IDC calls "information-intensive legislation" (see Table 1). Information access and process integrity are increasingly becoming matters of public concern, not just a business interest, as all industries become more and more dependent on information to design products, track customers, and deliver services.

Organizations face the complex task of complying with various regulations and making sure that employees do not inadvertently, or deliberately, break the law. However, information integrity provides a bedrock for compliance auditing, especially when interpreting ambiguous and sometimes conflicting requirements from differing authorities.

The use of infrastructure integrity tools vastly improves the assurance level of internal policies and can measure the effectiveness of compliance processes. These same tools can provide a detective control that complements preventive controls (workflows and policies) and corrective controls (remediation procedures).

TABLE 1**Information Intensive Legislation**

	Intent
Sarbanes-Oxley Act of 2002	Affects financial reporting processes, with long-term effects on corporate governance and the regulation of auditors
Gramm-Leach Bliley Act	Addresses the public's increasing concern regarding the protection and use of private information and mandates that financial institutions take steps to ensure the security and confidentiality of their customers' personal information
Heath Insurance Portability and Accountability Act (HIPAA)	Relates to the privacy of patients' health information and is intended to protect medical records and other health information held or disclosed by health-related organizations
Federal Information Security Management Act (FISMA)	Provides a mandated security framework for federal government agencies and requires annual testing and evaluation of security controls and management accountability and agencies developing their own system configuration requirements and providing ongoing monitoring and maintenance
Basel II	A set of international risk-based capital guidelines due to take effect in 2006 created in response to recent growth in international financial markets and intended to encourage banks to manage their capital appropriately and to improve their risk-control processes
U.S. Food and Drug Administration 21 CFR Rule 11	Established the criteria under which electronic records and signatures will be considered equivalent to paper records and handwritten signatures in manufacturing processes regulated by the FDA
USA PATRIOT Act	Is among a number of antiterrorism and law enforcement activities and requires financial services and insurance companies to implement antiterrorism and anti-money-laundering regulations, including capabilities to identify customers and flag suspicious transactions
California SB 1386	Mandates public disclosure of computer-security breaches in which confidential information of any California resident (including Social Security numbers, California driver's license numbers, account numbers, and credit or debit card numbers) may have been compromised

Source: IDC, 2004

INFRASTRUCTURE INTEGRITY DEFINED

A new model of assurance has emerged as the foundation for an enterprise information integrity, security, and compliance strategy. This domain is infrastructure integrity enabled by change auditing. Change auditing solutions ensure the integrity of all infrastructures in a network — in essence ensuring that the infrastructure remains in a "desired state" throughout the implementation of the changes necessary to keep pace with the dynamic demands of the business.

Infrastructure integrity is the foundation or anchor upon which IT infrastructures should be built. When there is no infrastructure integrity, the internal process controls put in place to manage the infrastructure fail. Like a structure built upon sand, when

the ground underneath shifts, the building will crack. In essence, without infrastructure integrity, an enterprise's investment in operations management and information security technologies can become compromised at best and at worst wasted.

For an illustration of what it really means to have infrastructure integrity, see Table 2, which contrasts an environment with integrity with one that doesn't anchor its assets.

TABLE 2

Environments With and Without Infrastructure Integrity

Without	With
Extended problem diagnosis cycles	Rapid discovery of problem changes or compromise and exact location/nature of the incident
Undocumented changes to critical files and loss of repeatable builds	Lower total cost of ownership (TCO) due to consistency created through configuration control
Difficulty determining critical file modification following a compromise or a failed change	Quick damage assessment and remediation following an intrusion or undesired change
Inability to track critical metrics related to stability of infrastructure	Infrastructure stability through an ability to measure integrity
Delays in fielding new or replacement IT infrastructure components	Quicker deployments of IT infrastructure components
Loss of control over aspects of the IT infrastructure	Improved confidence in the IT infrastructure
Increased costs to maintain an acceptable risk level	Lower costs through proactive management of risk
Constant break/fix cycles and low IT staff productivity	Less firefighting and more business building activities
Unbounded loss scenario in the event of a failure/compromise	Lower outage costs due to ability to bound loss

Source: IDC, 2004

Infrastructure integrity is not something that is just of interest to the security professional, change manager, or system administrator who ultimately implements change auditing. It is of concern and interest to the whole company.

The CIO is ultimately responsible for the proper operation of the IT assets, maintaining infrastructure integrity and providing a compelling return on assets (ROA) and return on IT (ROIT). The CFO is concerned with risk management and audit compliance and needs to leverage infrastructure integrity to mitigate risk by reducing and bounding loss in the event of an unauthorized change or compromise and to minimize the effort and cost of producing audit reports. Business units need to count on uninterrupted business processes, maximum uptime and availability, and trusted

online systems. Ultimately, the CEO doesn't want to be surprised. To avoid surprises, IT infrastructure must remain in a "desired state," utilizing the following:

- ☒ **Change control.** Change auditing solutions demonstrate compliance to regulations by providing verifiable, documented evidence that the integrity of the infrastructure is intact by validating planned changes and exposing those that are unintended and unauthorized. Infrastructure integrity is also crucial in establishing better control of change by detecting circumvention of change control policies and providing the information needed to rectify the issue.
- ☒ **Intrusion detection.** Infrastructure integrity enables a deep level of intrusion detection. It is entirely possible for an attack to go undetected. Crafty intruders who understand how to scrub audit logs and disrupt automated tamper detection systems can be difficult to find. However, with a change auditing solution it is possible to uncover malicious activities because for a hack to work, the intruder must modify some critical files. Using change auditing technology, it is possible not just to determine the existence and extent of an intrusion, but also to quickly identify the exact location of the compromise so rapid recovery can occur.
- ☒ **Damage assessment and rapid recovery.** Costs associated with network downtime have risen exponentially. Having the ability to quickly recover from an outage, be it malicious or accidental, is of critical importance. After an unauthorized or unintended change has been detected, system administrators still face two difficult tasks: assessing the damage and restoring the system to a desired state. Infrastructure integrity optimizes the restoration process because one doesn't know the state the systems were in prior to the incident. In most cases, the organization won't need to rebuild the system from scratch, because it will be able to ascertain what had changed. This will save considerable time. The same scenario for recovery plays out when the system goes down because of an unintentional software corruption.
- ☒ **Forensics.** In the event of a compromise, because of the insatiable need for uptime and availability, rapid recovery becomes the top priority. In the process of recovery, the system administrator "steps all over the crime scene." Not only can the perpetrators not be prosecuted, but the opportunity for learning disappears, as well, because the compromise is not documented for future analysis. With change auditing, IT has the ability to quickly "snapshot" the compromised system and store it away in a secure place so that it can be used in court, or at the very least, to enhance organizational learning.

The bottom line of infrastructure integrity is that it offers a unique value proposition by creating a foundation upon which the infrastructure can be measured and by which deviations from a desired state can be detected. Infrastructure integrity provides investment protection by bounding the loss scenario in the event of an unauthorized change, lowers the total cost of ownership (TCO) of IT assets, maximizes uptime and availability, demonstrates compliance to an increasing number of regulations, and (most importantly) allows the scarce IT resource pool to focus on value-added activities rather than firefighting and crisis management.

In summary, all of the above — risks from hackers, network complexity, software errors, and inadequate IT staffing — are part of an intolerable problem that is frequently tolerated because of the business needs of rapid deployment and capacity expansion are paramount.

TRIPWIRE'S SOLUTION

We have explained the intolerable-but-tolerated problems associated with the IT infrastructure, the missing safety points, infrastructure integrity, and the business returns infrastructure integrity can provide. Now it is time to consider a change auditing technology solution that enables infrastructure integrity.

There are few companies that can claim infrastructure integrity as their domain, but one of the most complete is Tripwire. Tripwire was originally developed in 1992 by Gene Kim and Dr. Eugene Spafford at Purdue University. The commercial version of the software has been rebuilt from the ground up and has been dramatically enhanced to increase its functionality and usability for the enterprise. Tripwire currently has an installed base of over 4,000 customers.

A CTO for a major financial institution relayed how his institution had incorporated Tripwire as a fundamental part of its IT infrastructure management and security strategy. "A committee was created to establish consistent security procedures across the whole corporation. Part of the studies that were done was focused on looking at the technologies that need to be used as a bare minimum. Tripwire was on that list."

Tripwire is a change auditing solution that permits operations managers and security professionals to ensure the integrity of critical infrastructure items. The core application checks to see if what is being monitored has changed on servers and network devices and compares any detected changes to a desired state, which necessitates tight integration with change ticketing systems and other enterprise management tools.

Tripwire software creates a baseline of system files and configuration data for a desired state based on monitoring criteria. Subsequently, running the application detects changes and provides information on deviation that has occurred from the baseline. This is done by comparing the current state with the desired state. Any changes outside of specific boundaries are detected and reported. If the changes are valid, the administrator can accept them and update the baseline with the new information. If the change is not valid, remedial action can be taken, to return to the desired good state.

Tripwire as an Anchor

Tripwire will validate change control processes and keep integrity drift from compromising an extensive investment in the IT infrastructure. Using Tripwire as an anchor, it is possible for enterprises to establish "desired state" baselines for their infrastructures. The Tripwire baseline is used to detect any drift from the anchor point and to recover integrity when it is required. By recognizing the drift and addressing it

immediately, organizations can use limited resources in much more productive ways. Using Tripwire can reduce staff operational expenses that are part of the TCO formula but are often not fully considered with infrastructure operations costs.

CONCLUSION

When Tripwire software is used to anchor IT infrastructures, it provides a solid foundation upon which a coherent, secure, and functional network can be deployed, maintained, and updated. Managing change around the three pillars of IT has presented challenges for IT management and administrators in companies large and small. Hoping for success with a myopic strategy is an exercise in futility if grounded in an environment in which the core information assets and the infrastructure do not have integrity. Consequently, if the integrity of the core information assets, infrastructure, and procedures are in question, so too are the resulting corporate financials.

Tripwire addresses the three pillars of IT, providing confidence that the data contained within the IT infrastructure maintains its integrity, security, and compliance to meet operational and financial reporting requirements. With Tripwire as a solid foundation for addressing the three pillars, IT management and organizations can now concentrate on more productive business endeavors, instead of constantly putting out fires.

We expect change auditing standards to be developed and incorporated directly into best practice change/configuration management frameworks. Infrastructure integrity health checks will eventually be part of basic, statutory IT operations. A CTO for a large financial institution stated, "Most people will never be aware that over time some vendors will build it (integrity checking) into the system as part of basic operations. The features and functions that Tripwire currently provides absolutely should be in every vendor product as part of the base infrastructure."

Tripwire will continue to expand the scope of change auditing. However, until such time as infrastructure integrity standards become ubiquitous and incorporated into basic system components, IDC believes it is imperative that enterprises use off-the-shelf change auditing technology, such as Tripwire, to anchor their critical infrastructure components in a state of integrity. The integrity anchors ultimately protect the value of the total IT security investment, with additional ROI in accurate, timely, and readily available data for compliance reporting.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2004 IDC. Reproduction without written permission is completely forbidden.