



Advisory

How Much of Your Budget Are You *Wasting* on IT Security?

Introduction

CEOs: call in your CFO, your CIO, and your top information technology (IT) executives. Ask them this simple question: "how much are we spending on IT security?" Here's what you're going to find: they don't know!

Why don't they know? Because security is a pervasive cost. It's mixed in with your hubs/routers/switches; it is integrated into your database technology; it's in your operating system (allegedly); it's found on hardware (crypto); it's found in add-on security software (access protection, authorization services, identity management); and so on. Your security costs also include compensation for the people who manage and secure your environment – and compensation for those expensive consultants who perform your ongoing security audits. And don't forget to add-in the hundreds of thousands of dollars that you're likely spending on public security keys every year...

Depending on the size of your enterprise, you may be spending hundreds of thousands (if not millions) of dollars on IT security annually.

Now ask yourself two questions: 1) "am I getting maximum return-on-investment from my IT security spend?", and, 2) "are there ways to reduce my current expenditures?"

Chances are that if you're running a distributed computing environment with thousands of access points; a variety of disparate network, computing, and storage systems; and no centralized point of control, you are wasting a significant portion of your security budget on locking-down access points, on performing cross-system security integration; on security software site licenses to cover hundreds or thousands of distributed nodes; and on salaries and benefits for additional IT security personnel.

Are there ways to reduce your IT security expenditure? You bet! Do this:

Centralize your IT security under IBM mainframe (System z) control. Integrated mainframe security will significantly reduce your security software licensing and integration costs; greatly reduce your human resource-related security management costs; simplify your compliance testing; and eliminate your external public key costs. You can expect to save hundreds of thousands (if not millions) of dollars in hardware, software, testing and human resource-related costs by using IBM's mainframe security architecture.

In this *Advisory*, *Clabby Analytics* (that's me) explains why your organization might want to rethink its distributed IT security infrastructure design and move toward a more centralized, integrated IBM System z mainframe security design...

How Much of Your Budget Are You Wasting on IT Security?

What Your IT Security Organization Is Supposed to be Doing?

The overall goal in IT security is to protect data. More specifically, the goal of the IT security designer is to prevent unauthorized access to data on-the-fly (over the network) or data-at-rest (data located behind the firewall in enterprise databases).

IT security designers typically protect enterprise data by:

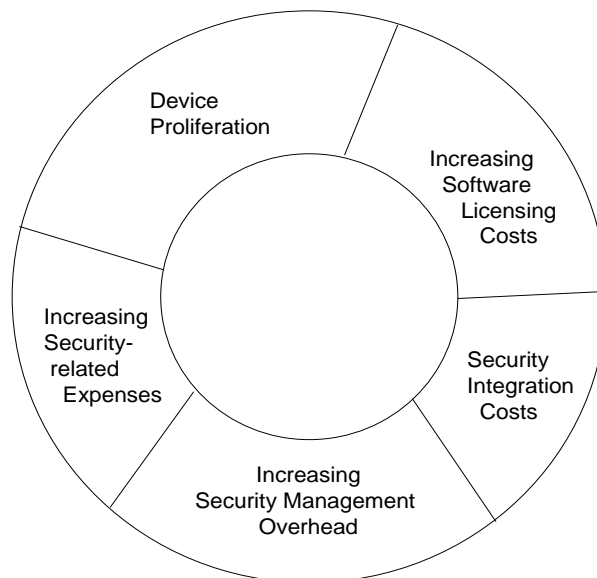
1. Building and maintaining a secure network;
2. Protecting data on-the-fly as well as data-at-rest by encrypting that data;
3. Implementing strong security control measures (access, authorization, ...);
4. Constantly monitoring and testing those measures;
5. Establishing a vulnerability management program; and,
6. Formulating and maintaining rigid information security policies.

What Your Security Organization Is Telling Me?

Every one of the mid-sized and large enterprise accounts that I have talked to over the past five years has followed the above recipe for building a secure computing environment. Enterprise IT executives have all built secure networks; put in place authorization/authentication/privacy schema (and sometimes complete identity management systems); and have established rigid policies and procedures to maintain data security.

Yet, even though they've followed the above recipe for success, security IT executives, managers, IT administrators, and systems/network designers are telling me that they are constantly encountering "trouble spots" when it comes to managing security across complex, distributed, three-tier-or-more architectures. These trouble spots fall into five general categories (see Figure 1).

Figure 1 – Trouble Spots When Managing Security Across Distributed Computing Environments



Source: Clabby Analytics, October, 2007

More specifically, these IT professionals are seeing:

- **Device proliferation** – distributed computing architecture inherently leads to a proliferation of server, storage, and network devices. Each-and-every one of

How Much of Your Budget Are You Wasting on IT Security?

these devices has a network touch point (or “access point”) that needs to be secured, monitored and tested on a regular basis to ensure that it has not been compromised.

- **Increased management data overhead** – As more devices are added, monitored and tested – the amount of security management data that is generated by each device increases. That data must then be forwarded, filtered and analyzed by security management systems and security personnel. (Note: dealing with all of this additional data often results in increased security management headcount as workloads increase).
- **Increasing software licensing costs** – most mid-sized and large enterprises buy security software on a “site license” basis, based-on the number of users or devices being secured. Site licenses are purchased for security and anti-virus products that run on network devices, systems/desktops/workstations/and mobile devices, on storage; and so on. The more devices that an enterprise has, the larger the site license cost...
- **Increasing integration costs** – As new security products and services are introduced into a given distributed computing environment, the integration of security software across disparate computing environments (for instance, across Linux, Unix, and Windows) is taking a bigger and bigger chunk out of the security operating budget.
- **Increasing security-related expenses** – the age of compliance reporting has brought with it a new requirement: that systems, storage, and networks be regularly tested to ensure that enterprise data is being kept secure. And compliance testing is far from free...

Further, IT managers tell me that they often have difficulty finding IT security expertise – forcing them to hire external consultants at inflated rates (burning even more of their limited IT budget).

Finally, every time an enterprise needs to acquire a public security key, a fee of around \$100,000 is paid to a 3rd party public encryption key provider. One way to eliminate this fee is to generate your own keys (as mainframe architecture combined with specialized cryptographic hardware can do).

Device proliferation, increases in management overhead, increased software license costs, escalating security personnel compensation, and increasing IT security expenses are characteristic woes of distributed network environments. In most cases, distributed computing architecture actually serves to exacerbate these problems. Mainframe security architecture can help mitigate these problems by centralizing security control, simplifying management, and decreasing software licensing costs.

How Do You Solve These Problems – And Save Money While Doing So?

Simply put:

1. Stop proliferating access points! Cut back on the purchase of new distributed systems and related network devices. Virtualize your servers under one common architecture – a centrally controlled and managed mainframe environment.
2. Blow away your software site licensing costs. Your anti-virus site license expenditure should be your first casualty (you don't need an antivirus site

How Much of Your Budget Are You Wasting on IT Security?

license on a mainframe). Intrusion detection and identity management licenses are also candidates for elimination (or significant scale-back).

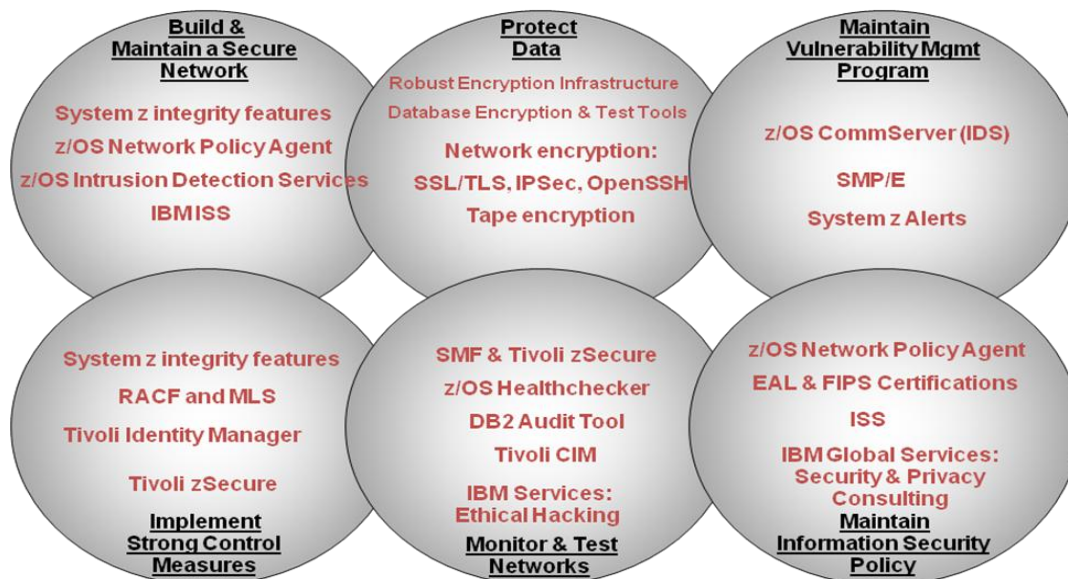
3. Buy an integrated security environment rather than putting together your own environment in piecemeal fashion. Leverage your vendor's integration efforts rather than your own.
4. Reduce requirements for additional IT security personnel by decreasing the number of devices that need to be managed, and by automating security policy and administrative tasks.
5. Generate your own public keys.

IBM's System z architecture can help you do all of these.

How Does IBM's System z Help Solve Distributed Computing Management Problems While Reducing Capital and Operational Costs?

From a security perspective, IBM's System z has been designed to act as a complete, end-to-end security hub. It is a security-rich, integrated system design that incorporates security features that offers direct protection from malware, viruses, and insider/outsider threats; monitor and control services; data protection services; vulnerability assessment services; as well as a blueprint for implementing and maintaining an enterprise-wide information security policy (see Figure 2).

Figure 2 – IBM's System z – A Holistic End-to-end Security Solution



Source: IBM Corporation, October, 2007

How System z Can Be Used to Help Build and Maintain a Secure Network Infrastructure

System z "integrity" features help protect data on the network as well as data behind the firewall at rest in the systems/storage environment. These features include

How Much of Your Budget Are You Wasting on IT Security?

workload isolation, access to executables only by authorized users, unique data keys for storage protection, security for virtualized environments – and more. Further, z/OS Network Policy Agent helps automate and enforce network policies across multiple instances of z/OS. And z/OS Intrusion Detection Services, and IBM's ISS (Internet Security Services) can also be used to help build and secure network infrastructure.

System z Integrity Features

To protect data, IBM's System z offers a variety of features that are integrated-into its z/OS operating environment, and a full complement of security protocols, encryption/-cryptographic services.

IBM's System z is an engineering marvel when it comes to protecting data-at-rest. System z architecture allows for:

- Workload isolation (each user is given a separate address space as well as supervisor state and system program protection);
- Access to executables only by authorized users (via z/OS's authorized program facility);
- Access to protected data only by using unique keys. Storage protection keys are used to control access to protected storage, and to provide cross memory services that prevent unauthorized data access.

Further, when it comes to securing virtualized server environments, z/OS isolates system images on LPARs (logical partitions) so data cannot leak between OS instances. This is important because in recent months other vendor's virtualization products have come under scrutiny for potential security holes. System z, on the other hand, has managed to achieve the highest certification ranking in the world for virtual machines– the Common Criteria EAL5 ranking.

In addition to providing highly secure virtual server environments, System z also provides secure virtual network access by allowing virtual servers to gain access to secure TCP/IP networks through system memory. This provides access to a highly secure internal networking environment – no external network is exposed.

These "integrity" features are a really big deal. Workload isolation protects information from leaking across hardware/virtual boundaries. Unique keys lock data from unauthorized access. And IBM has proven strength in virtualized server security – unlike some of the other virtualization software schemes on the market today.

System z Integrated Intrusion Prevention and Network Policy Agent

System z intrusion prevention services compliment network-based intrusion detection services (such as Netview's intrusion detection services) and enable automatic, real-time detection of attacks. Further, System z intrusion prevention services can respond instantaneously with defensive mechanisms.

To automate network security management, IBM's Network Policy Agent can establish and enforce network policies across multiple instances of z/OS – allowing data to be secured inside a single mainframe or across multiple mainframe environments.

How Much of Your Budget Are You Wasting on IT Security?

IBM Internet Security Services

To assist in network/system security design and deployment, IBM offers security design, deployment, and consulting services under its Internet Security Services (ISS) umbrella of services. IBM's ISS provides consulting security services; multi-layered desktop security solutions; e-mail protection services; emergency preventative incident response programs; intrusion response and detection solutions; managed security services; network anomaly detection, pre-emptive security, threat management, web content filtering, vulnerability management, and other data protection services.

With respect to security protocols, System z supports numerous security standard protocols such as IPSec, OpenSSH, and AT-TLS – as well as SNA session level encryption. Many applications included with IBM's Communications Server are enabled for TLS (Transport Layer Security) as well as Kerberos security. For an additional layer of network security, specialized System z crypto hardware supports cryptographic acceleration, and can take full advantage of the z/OS SAF digital certificate support (enabling streamlined digital certificate processing).

A Closer Look at System z Integrity Features

IBM's System z is extremely rich in security features. This is a partial list of some of IBM's security features, products and services:

- Data and application integrity features to confidently place mixed critical workloads on single System z system (Storage Protection Keys, Authorized Program Facility, System Access Facility, RACF);
- Centralized role-based access controls to resources access the System z enterprise (RACF);
- Virtualization technologies with strong integrity and security features (LPAR, HiperSockets, z/VM);
- Encryption solutions to help secure data from theft or compromise;
- Built on time-tested System z encryption infrastructure with System z availability, disaster recovery, and access controls (Encryption acceleration in every processor, Crypto Express2, ICSF, Trusted Key Entry);
- Tamper-resistant encryption module to protect encryption keys from detection with highest certification at FIPS 140-2 Level 4 (Crypto Express 2);
- Encryption options for protecting data over the internet using industry standards (IPsec with specialty engine support, SSL, TLS, OpenSSH, z/OS Intrusion Detection Services);
- Encryption options to help protect data at rest – on tape and in data bases (Encryption Facility for z/OS, IMS and DB2 Encryption Tool, TS1120 tape drives)
- Digital Certificate hosting solution built into z/OS to avoid costly third party charges (Public Key Services in z/OS);
- Allowing you to address compliance needs with more confidence
- Provides extensive audit information to enable regulatory compliance (SMF, RACF, z/OS Policy Agent);
- Extending the inherent compliance features of z/OS with tools for easier auditing and monitoring (Tivoli zSecure, Tivoli Compliance Insight Manager);
- WHO accessed WHAT data, WHEN and HOW?;
- Independent Common Criteria certifications attest that System z solutions have been methodically designed, tested, and reviewed for secure operations;
- System z is the only server with EAL 5 certification for logical partitioning;

How Much of Your Budget Are You Wasting on IT Security?

- Operating systems certifications include z/OS at EAL4+, Linux on z at EAL 4+ and z/VM in evaluation for EAL 4+;
- KEY MESSAGE - Mitigating the risk of security breaches and helping to protect your organization's brand image - and bottom line; and
- Vulnerability assessment and management service is performed within the z/OS operating environment using z/OS CommServer (IDS)...

Summary Observations

Every year, enterprises waste hundreds of millions of dollars on information technology security products and services. CEOs, CIOs, and IT executive management are overspending on security in five distinct areas:

- Security hardware (systems and Network) acquisition;
- Security software licensing;
- Security software integration;
- Labor-intensive security management; and
- Ongoing security compliance-related testing.

To correct this overspend, consider these points:

- First and foremost, IBM's System z is recognized as the computing industry's premier security environment as certified by the Federal Information Processing Standard (FIPS) and the Common Criteria organizations. IBM has obtained FIPS 4.5 and Common Criteria's Evaluation Assurance Level 5 (EAL 5) certifications – recognizing System z as the best commercial computing security environment in the world.
- Second, IBM's System z takes a holistic approach to security. Network security is tightly knit with systems/application/database security to create a complete end-to-end security environment. (Explained in greater depth in the following section).
- Third, the level of security integration on IBM's System z is extraordinary. Features such as workload isolation, access controls, and highly-resilient encryption key management are built into the operating system – protecting all users while ensuring that devices and programs clear-through centralized security controls. System and network intrusion detection also work hand-in-hand.
- Fourth, moving to a System z will help stem your device proliferation problem.
- Fifth, IBM's System z has outstanding vulnerability management, deep monitor and control capabilities, and an integrated security clearinghouse/policy creation/management environment (known as Remote Access Facility – RACF).
- Sixth, for enterprises that can benefit from the issuance of their own public keys, IBM's System z offers you the opportunity to save hundreds of thousands (if not millions) of dollars annually by so doing.
- Seven, IBM's System z can be used to reduce risks associated with data-on-the-fly by making use of its internal, high-speed switching.

How Much of Your Budget are You Wasting on IT Security?

By consolidating hundreds (or even thousands) of servers onto a System z, device proliferation (and the associated proliferation of access points) grinds to a halt. Reducing device proliferation reduces the number of devices that need to be individually managed – and thus reduces the mountain of management data that those devices produce. Further, by cutting back on the management of thousands of additional systems, network devices, and access points, fewer people are needed to perform security functions.

By pumping all security access through a centralized audit and control point (RACF), IT security managers know who is doing what (and when) with any applications and databases within their purview. System z's integrated security management products also reduce costs related to security system/program integration – and further reduce the number of people needed to secure systems and data. And System z can also issue its own public keys – potentially saving IT buyers hundreds of thousands of dollars per year in external costs.

Clabby Analytics
<http://www.clabbyanalytics.com>
Telephone: 001 (207) 846-0498

© 2007 Clabby Analytics
All rights reserved
October, 2007

Clabby Analytics is an independent technology research and analysis organization that specializes in information infrastructure and business process integration/management. Other research and analysis conducted by Clabby Analytics can be found at: www.valleyviewventures.com.