aimpublications LLC

www.aimpublications.com

synthesisseries white paper

1Q2002

Enterprise Security 2

Now it's about *survivability*

As an open, unbounded network, the Internet — where organizations and individuals alike must interact to do business, communicate with loved ones and educate and entertain themselves — is a wild, untamed frontier ...

On the Internet, there is no central authority or 'government.' No unified security policy can be enforced. Even the number and kinds of nodes connected cannot be completely known.

Thus, regardless of the best efforts to harden systems connected to the Internet, those systems remain vulnerable to attack and intrusion (as well as failures and accidents). Traditional security measures, which are founded on centralized control and administration, just don't work.

So what's the alternative? Security experts call it ***survivability***: ensuring that systems operating in unbounded networks are robust when under attack or subject to failures or accident, and can survive assaults that produce successful intrusions, so that the systems' missions can be carried out. The key is not the survival of a system but rather the survival of its ability to preserve mission-critical services.

Essential services in context

What constitutes a system's survivability success depends on the context. A company that suffered system losses in the September 11 attacks but preserved the integrity of all of its data and managed to get basic operations up and running in, say, a few days can conclude that its overall systems mission was fulfilled, although some systems were completely destroyed. After all, mission-critical services — preserving corporate data integrity — were maintained amidst great upheaval and devastation.

But if those same systems had crashed without warning a month earlier and remained out of service for several days under normal conditions — costing the company its ability to conduct business — then those systems would have failed in fulfilling their mission, since essential services would not have been preserved.

So what's really *essential*?

To achieve survivability, a system's essential services and the essential properties and assets that support them (*e.g.*, certain levels of performance, availability, integrity, confidentiality, etc.) need to be identified. This process can be started with a simple question: which services can be temporarily suspended without sacrificing what really matters?

Once these mission-critical services and properties are established, systems need to be designed to preserve them.

Survivable systems, then, must be able to

- ***Resist and withstand attacks.*** IT executives need to develop strategies for fending off attacks and intrusions. This means implementing various hardening techniques and technologies — including virtual private networks (VPNs), bastion hosts, firewalls and encryption — as well as maintaining strong configuration management, backing up data and key applications at secure offsite locations, diversifying systems, continually upgrading applications and systems for known vulnerabilities, and developing effective user/system authentication and access control.
- ***Perceive attacks and identify the damage caused.*** This involves not just detecting attacks and intrusions but also understanding the condition of the system itself and being able to evaluate damage. Techniques and tools to do this include auditing, internal integrity checking, system and network monitoring, recognizing intrusion usage patterns and virus scanning.
- ***Recover services after an attack.*** Efforts to maintain or restore mission-critical services, limit the damage and reestablish full services can be aided by ensuring an ability to function with reduced services or to a reduced user base, using alternative services like hotsites, exploiting system redundancies, isolating the damage, and implementing established operational procedures that restore data, programs and system configurations.

- ***Adapt to diminish the impact of future compromising events.*** Each attack, intrusion, failure or accident can teach us about what to differently — and better — next time. These insights as well as new patterns that can be recognized, new filtering mechanisms that can be employed, new data elements that can be logged and audited can improve response tomorrow.

Considerations for systems new and used

Although no system can be constructed (or refitted) to be invulnerable to attack, intrusion, failure or accident, the effort to create survivable systems has some implications for both new and existing systems.

Additional layers of boundary control like firewalls and bastion hosts, as well as redundancy in hardware and software, can boost the survivability of existing systems. It's also useful to develop and test administrative procedures addressing migration, back-up and restoration.

Survivability features, technologies and techniques should also be considered when new products and vendors are being selected. Mission-critical services and the assets that support them should be identified as part of the effort to develop system or software requirements and specifications, as should the ability to isolate, migrate, replicate and restore these services. The basics of survivability — resistance to, perception of, recovery from and adaptation to compromising events — need to be treated just like performance, availability, reliability and maintainability when it comes to system planning, design, testing, implementation and management.

Security policy

Many organizations have deployed networks and systems that are large, complex and include diverse hardware, software and formats; these networks also typically deal with large numbers of users and interactions. To protect critical resources and maintain mission-critical services, it's important that organizations develop and implement policies establishing how to handle compromising events like attacks or disasters as well as policies directing which users are allowed access to which information resources.

By setting up basic definitions, rules and guidelines, a formal IT security policy helps to prevent inconsistencies that can create risk and to establish a foundation for enforcement of more detailed procedures and processes.

Often two kinds of security policies are required:

- ***Program-level policies*** articulate goals and objectives, institute a security program, assign responsibilities and accountability, and devise enforcement fundamentals.
- ***Issue-specific policies*** identify and define areas of concern, articulating expectations about them, so that standard practices may be developed. Typical areas of concern to most organizations include risk management, contingency planning, administrative security, communications security, physical security and personnel security.

Once security policy is conceived, it has to be implemented and it has to be documented. Much of security policy implementation involves communicating its existence and particulars to all employees, since virtually all of them will be affected by it.

From the top

Clearly, making systems survivable requires an intimate knowledge not only of the systems involved but of the

missions they are intended to accomplish. Certainly, technical expertise is important, especially in creating and understanding the 'what-if' analyses that describe the rippling effects of various compromising scenarios.

But the business continuity planning necessary to maintain essential services in the face of attack, intrusion or disaster and then recover again requires the kinds of decisions about economic trade-off and risk-management that must be made by executive management. Survivability is only partly the responsibility of IT managers. The key decisions have to come from the top.

Approaching security comprehensively

Effective management of risk and maintenance of security for an organization can never be a haphazard effort. It must be approached comprehensively and it will include these fundamentals:

- ***Developing, testing and maintaining a security policy.*** This means benchmarking your organization's current state of security awareness as well as its technical security and its standard security procedures. Technical risks need to be identified, but this cannot be achieved without first identifying business risks — something which must involve the organization's executive leadership.
- ***Conducting an organization-wide vulnerability assessment.*** This will reveal the most obvious issues and problems — things like servers that are missing updates or patches, operating systems that haven't been hardened, ports and services that should not be open, bad passwords, unauthorized modems. Such vulnerabilities should be addressed and corrected as quickly as possible.
- ***Designing and then implementing an all-inclusive***

security architecture. The design needs to be based on your organization's security policy, which is in turn built on your organization's business risk assessment. This security architecture should incorporate authentication (who each user is), authorization (what each user is allowed to do), audit (what's happening) and administration (how users and resources are managed). And the architecture should be implemented with technologies, products and processes that enable administrators to enforce security policy.

- ***Undertaking a user security-awareness campaign.*** Your organization's security is only as strong as its weakest link — and chances are that will be a user who didn't understand or appreciate security procedures and the reasons for them.
- ***Ensuring that system and network security is regularly and consistently monitored.*** Ongoing monitoring of system and network activity should be accompanied by periodic analysis of events with an eye to trends.
- ***Creating an incident response capability.*** This means developing a set of incident response policies and the procedures and processes needed to carry them out — including training and assigning staffers.
- ***Building a security maintenance attitude.*** Regardless of how encompassing your security efforts may be, new vulnerabilities are always emerging. So it's important to do regular vulnerability assessments of specific networks and systems. As you discover or reassess vulnerabilities, review security policy and make adjustments.

Keeping your organization secure and able to survive failure, disaster or attack requires ongoing effort and constant vigilance. Demanding as that is, it sure beats the alternative.

aim*publications* synthesis series
white papers on **ENTERPRISE SECURITY**:

1 The porous new front line:
defending systems in
an unbounded network
(www.aimpublications.com/synth-esec1.pdf)

2 Now it's about *survivability*
(www.aimpublications.com/synth-esec2.pdf)

3 Corporate
countermeasures & security tools
(www.aimpublications.com/synth-esec3.pdf)

aim*publications* LLC analyzes and writes about how trends and developments in e-business and IT infrastructures — including security, integration, collaboration, database analytics and implementation of new technologies — affect business competitiveness.

As IT writers and marketing communications professionals, aim*publications'* principals also produce advertising supplement and editorial content for leading business and IT publishing companies — including CXO Media (publishers of *CIO* and *Darwin*), *Forbes*, *Fortune*, *Computerworld*, Ziff-Davis and others.

In addition, aim*publications* has created advertising, marketing and/or editorial content for many IT vendors — among them IBM, Microsoft, Sun Microsystems, Computer Associates, Oracle, NCR, Symantec, Hitachi, Quantum and many others.

For more information about aim*publications* LLC, please visit www.aimpublications.com.