Restoring Cyber Security

Bryan C. Crittenton
Vistronix Inc.

This article addresses the security management issues of millennium enterprise system environments. The intent is to define an approach that enhances cyber security and reduces negative system impacts through automated monitoring and management techniques. In addition, this article addresses the benefits of proactive security and systems management. This proactive approach details some of the automatic functional responses that can be initiated to alleviate a variety of security violations and systems malfunctions.

In the rush to provide Year 2000 (Y2K) compliance, many systems have not been adequately evaluated and validated from a security perspective. Most of the efforts have focused on date-oriented testing, with little concern for the post-Y2K security integrity of the system. Many of the patches and fixes developed have not been tested for potential security violations.

In the process of these developments, many security procedures have been bypassed to accommodate immediate access for online testing. Though some bypasses have been removed, many were left behind to allow for quick fixes. These backdoors may even be active in some commercial products. In short, the impact of the Y2K fixes may prove more devastating to the security of the operational systems than the Y2K bug itself.

The New Threat

Post-millennium systems and security administrators are facing several new complex problems. It is now obvious that Y2K impacts reach across the entire enterprise system to include security applications, security logs, security time stamps, and security access verification routines.

In addition to this wave of problems, several new security threats have appeared. New viruses are generated at an alarming rate, and some are designed to target the Y2K fixes. Some of the Y2K fixes have injected new bugs into operational systems and security management routines. In addition, several backdoors have been uncovered that are remnants of Y2K development efforts and test procedures.

Most fixes were never evaluated for security impacts or given sufficient operational time to ring-out all of the inherent problems. Many of the environment variables will not even be present for some time. This presents a staggering management challenge to all security and systems administrators.

Compromised Security

With the advent of these multiple challenges and simultaneous problems, current security practices will probably fail.

Security procedures that require manual intervention will be too slow to react before system damage occurs. Reactive systems and security management will not protect most enterprise systems in this new environment. Slow reactionary procedures may open the system to a high probability of swift and lethal damage. Over the next few months, all of the unknown variables will be brought into play. Most of the Y2K fixes have not been introduced to full battlefield conditions.

In addition, all the minor programming errors that have crept into these fixes can then become apparent. The full impact of various security violations, integration problems, interface disconnects, and programming errors will have to be dealt with in the near future. This collective impact is unpredictable. New and previously unknown bugs will appear, which will further challenge the security and integrity of our systems.

It must be recognized that many software developers have installed private access paths, or backdoors, in many of the online patches being implemented. Many Y2K development environments are such that none of the developers are certain as to how stable their patches or fixes are. Therefore, the implementation of backdoors has become a popular failsafe access for developers.

Unfortunately, the backdoors are insecure, and provide a vehicle for hackers to surf through the system. This new environment is a prime target for major security breaches.

System Monitoring and Management

The goal of Systems Monitoring and Management is to ensure that not only applications, but also all resources that support them, are online and performing optimally so user productivity and security remain high. Their availability, performance, and integrity are only as good as the system's weakest link.

Total systems management is best accomplished by taking a top-down data-centric rather than a bottom-up hardware-centric view. In the case of enterprise systems management, this means monitoring and managing the application, database, middleware, operating system, servers, network, and other related systems' hardware or software.

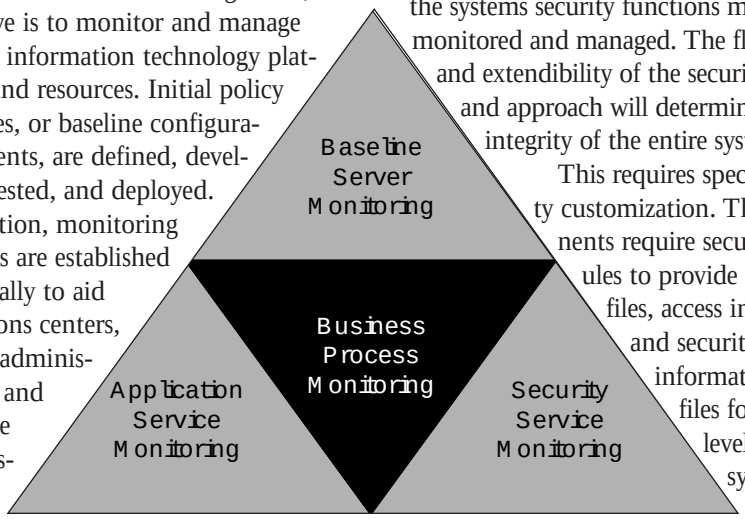
It is only when security and systems administrators view an entire environment, rather than a limited point-solution perspective, that they begin to support the overall objectives of true enterprise systems management: supporting end-user data access, security, and productivity.

Typically, multiple levels are involved in implementation of Enterprise Systems and Enterprise Security monitoring and management. Each successive level of implementation should add value to the previous level. In addition, security and systems administrators should assist in determining specific requirements for each level.

It is recommended that every system implementation include at least a baseline server monitoring function, an application service monitoring function, and a security service monitoring function. These areas of focus ensure that a significant level of operational protection is provided.

Capturing Enterprise System Data

One of the first levels of implementation is Baseline Server Monitoring. Here, the objective is to monitor and manage specific information technology platforms and resources. Initial policy baselines, or baseline configuration agents, are defined, developed, tested, and deployed. In addition, monitoring consoles are established specifically to aid operations centers, system administrators, and database administrators.



Necessary infrastructure and operations and administration support procedures also are established to support long-term stability. This level of implementation results in a fully operational, rapid deployment of baseline configured clients, agents, managers, and monitors. The baseline implementation establishes the foundation from which to implement the application service monitor or the security service monitor.

The next level of implementation is the application service monitor. Here, the management focus shifts from monitoring and managing individual systems to monitoring and managing the enterprise system. An internal service assurance manager and security service manager also should be implemented. At this level, flexibility and extendibility of approach and tools used are vital.

This phase generally requires specific customization to meet the unique systems or security requirements of the enterprise system topology. These components also wil require knowledge modules to provide product and platform information profiles on which tools can guide their management functions. When this level of implementation is reached, the approach must support the application service management, security management, and server monitoring and management.

The security level of implementation can be referred to as a security service monitor. Here, management focus shifts away from monitoring and managing application aspects of the enterprise systems to monitoring and managing the security of the enterprise system. At this level, all of the systems security functions must be monitored and managed. The flexibility and extendibility of the security levels and approach will determine the integrity of the entire system. This requires specific security customization. The components require security modules to provide user profiles, access information, and security level information profiles for multiple-level security systems.

Additionally, implementation should be oriented toward business process monitoring. This level of management service should be undertaken only after application service monitoring and security management are in place. At this level of implementation, the focus is to monitor and maintain critical day-to-day business processes. An example is monitoring the number of people using an application for license monitoring. When the number of users exceeds the license limit, the Business Process Monitor would generate an alert, and log out all inactive users.

This level of implementation adds business process monitoring to the functionality of the other previous levels.

Converting Data into Usable Information

By intelligently monitoring all of the necessary systems and security functional parameters, events, accesses, and processes, an effective management scenario can be implemented along with a proactive response agenda that will avoid major system malfunctions and security breaches.

The backbone of an automated management system is the data that is collected, and the response philosophy adopted.

Automatically monitoring all of the required functional parameters within the enterprise system allows the service monitors to build a baseline profile of the entire system. Once a baseline is established, trend information can be correlated.

With a trend database, a service monitor can identify out-of-tolerance conditions. In order to provide instantaneous responses, the service managers can automatically act upon these conditions, which can range from increasing security on endangered systems to putting failing devices offline, or calling the security administrator on a cellular phone to deliver a message about a breach condition.

Reactive vs. Proactive Management Environment

In a manually oriented management philosophy, viral attacks on the systems or security breaches could usually be dealt with in real-time increments. As systems have become more complex and communications more robust, reaction time has become more critical.

Management philosophies need to be reoriented to a more proactive posture. Problem responses now need to be handled on a nanosecond basis, which only a truly automated, proactive management approach can handle.

By implementing the new enterprise systems/security management approach, disaster can be avoided. For example, the automated trend analysis in the service monitor can indicate when a database caching size is incorrect. The service manager can then initiate a response function to increase or decrease cache size, eliminating a potential database failure.

A disk may be experiencing soft failures. The service monitor would detect this trend, and the service manager could soft-fail over to another disk drive or a backup copy of the data.

A security breach might be detected, and offending users piped to a dummy system while authorities are notified, all within nanoseconds.

Through the implementation of a security service monitor and a security service manager, all security functions can be dealt with at the computer's speed. Breaches can be contained, privacy can be maintained, new users initiated, inappropriate connections monitored or severed, virus handling automated, macros monitored, keywords tracked, and integrity verified. Security trend analysis information also could prove quite useful for future systems development.

Proactive Management Approach

A proactive management approach must be designed to manage exceptionally complex systems with high availability. Since most new applications demand global accessibility, constant availability is crucial.

Enterprise system applications may also be accessing and interacting with data in real time to support critical processes like tactical information processing. Availability requirements for these applications increase dramatically as users become more dependent on them.

The management approach must also be prepared for periodic and unscheduled disturbances, keeping the systems running regardless of a localized failure, or recover them quickly in spite of individual failures or breaches. For example, requests must not be lost if a processor or server goes down. This type of loss could result in lost information, increased operational cost, and lost confidence in the system.

Downtime for maintenance and unscheduled outages also can be planned and supported. Finally, the proactive management approach must be scalable to accommodate usual increases in load or multiple problems. As more applications come online, more concurrent usage can result in serious bottlenecks, loss of available services, lost incoming requests, and unacceptably slow response times. These are all taken into consideration in the proactive management system.

From a management standpoint, acceptable response times for applications must be no more than three seconds for typical actions, and no more than seven seconds for the longest operations. Failure to provide this rate of performance management can result in user dissatisfaction, and again, loss of system confidence.

For Internet applications, the performance management approach should expect larger-than-normal numbers of concurrent users. Managing Internet service demands that are above defined peak usage are not as predictable as similar demands placed on internal systems. As an example, a major news story could create an unexpected surge of hits to a site over a short time period. If any part of the enterprise system cannot handle the demand, cascade failures might occur, which may introduce security vulnerability.

Finally, the management approach must also manage all networked applications and the data they access. Both must remain secure to ensure absolute privacy and protection of sensitive information. Legal and financial exposures created by security breaches can be as high as tens of millions of dollars in damages per incident. With stakes this high, security concerns are critical.

Parameter Handling

The goal of enterprise management is to define the representation of management data, as well as the methods used to extract data or control managed objects.

The goal of security management is to define and enforce security policies, identify and channel the user community, and ensure that only authorized individuals access information. To meet diverse goals, parameter monitoring is designed to cover the entire technology stack from hardware drivers, to software applications, to network devices.

The data collected by parameter monitoring is translated into trend analysis databases and data models. New management technologies have been devised to support instrumentation of all systems and security applications and collections of parameter data required to quickly avert these systems problems.

To implement this technology, an enterprise systems management architecture was created. This architecture combines all the components to monitor, manage, and proactively recover from security breaches to systems malfunctions.

The enterprise systems management architecture has three basic components, as shown in the adjacent graphic.

This management architecture provides the definition of standard parameters, attributes, properties, and their association to the managed objects. The collection of the parameter data involves instrumentation of hardware, software, and access data, which is funneled to the service manager. This data can be used for advanced management, such as access and security correlation, security violation and problem diagnosis, or predictive availability modeling.

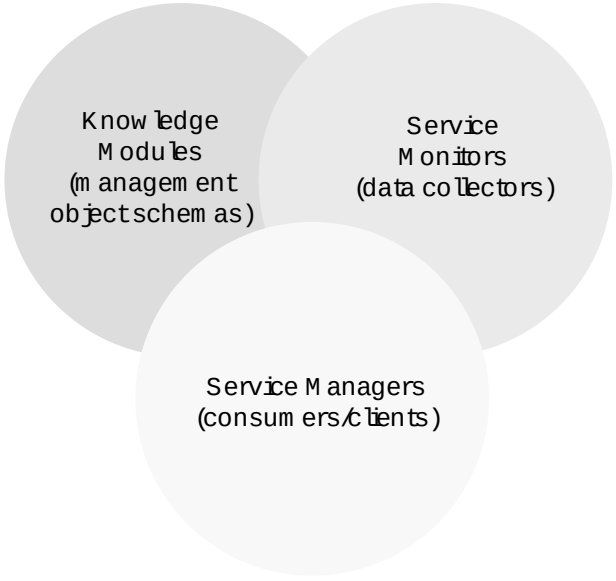
The resulting systems impact is increased security, availability, and reliability. Furthermore, this approach will reduce support personnel and systems downtime. The resulting operational cost reduction provides the driving force behind this new approach to enterprise systems and security management.

Conclusions

Systems and security administrators face multiple problems due to unknown and injected failures from Y2K solutions. These problems are multifaceted, parallel, designer bugs that could cause massive system failures and security breaches.

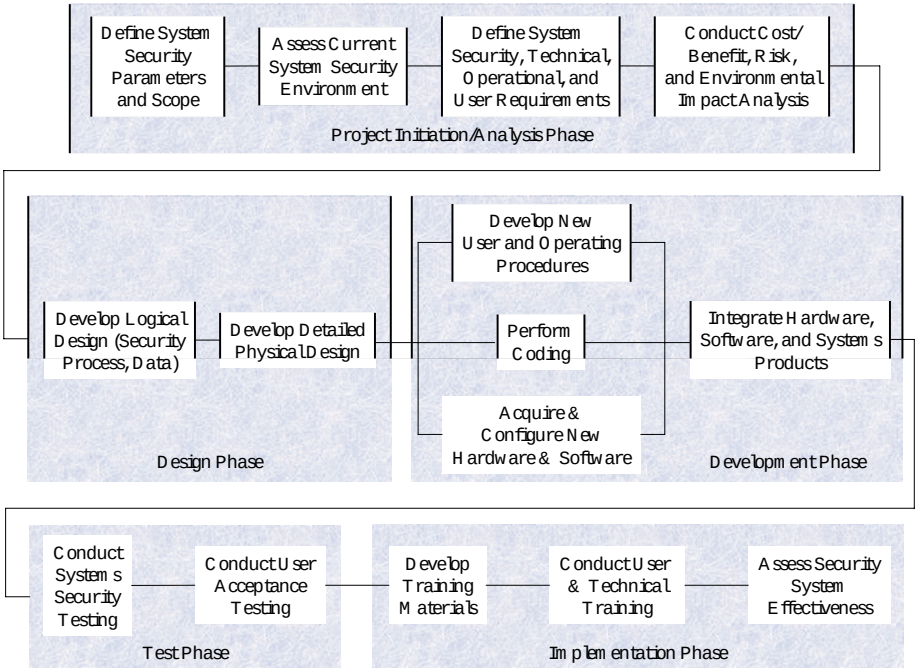
To counteract these looming failures, new automated management approaches must be implemented. These need to include well-thought-out automated systems responses that contain damage and protect system resources and users. Relying on existing manual procedures, or frameworks that do not provide a solid automated response to intrusions, viral attacks, or systems failures due to Y2K solutions will cripple most enterprise systems.

New enterprise management technology helps unify systems and security management. This approach to enterprise management provides a high degree of



conceptual breadth, and stands as an enabler for the next generation of systems and application management tools.◆

Our approach to enterprise systems and security management is depicted in the chart below:



About the Author

Bryan C. Crittenton is Director of Information Technology Programs for Vistronix Inc in Vienna, Va. He has more than 15 years experience supporting enterprise-wide management information systems in such areas as data, network, and Internet security and intrusion protection, network architecture analysis and design, department-wide financial and administrative systems design and development, and data warehousing and mining. Crittenton has numerous certifications in network design, software engineering, total quality management, and systems architecture and planning. He holds a master's degree in business administration from the Virginia Polytechnic Institute and State University and a bachelor's degree from the University of Virginia.

Vistronix Inc.
8391 Old Courthouse Road, Suite 205
Vienna, Va. 22182
Voice: 703-734-2270
Fax: 703-734-2271
E-mail: bcritten@vistronix.com

Web Addition

The following article can be found in its entirety on the Software Technology Support Center web site at http://www.stsc.hill. af.mil/CrossTalk/crostalk.html. Go to the web addition section of the table of contents.

Content Change Management: Problems for Web Systems

Susan Dart
Dart Technology Strategies

Behind the facade of a web site lies the task of managing its infrastructure and content. This is driving the Internet economy into a web crisis. The software community has experienced a similar crisis and knows that configuration management (CM) is a key player in resolving it. Nine challenges facing web systems are presented. As the entire world becomes connected to the World Wide Web, content problems will be magnified. While traditional software CM provides a static solution (such as via a centralized development methodology creating batched, planned releases), content CM will provide a dynamic solution (via distributed, real-time updates) in response to user traffic monitoring. It is imperative that the lessons learned from CM are applied to web tools. Otherwise, the Web community is doomed to experience all the delivery, quality and complexity problems that have plagued the software community.