



**A SHARED GLOBAL VULNERABILITY:
CYBERATTACKS ON BUSINESS OPERATIONS**

A WHITE PAPER

Forum Systems, Inc.

BOSTON, MA
95 Sawyer Road, suite 110
Waltham, MA 02453

SALT LAKE CITY, UT
45 West 10000 South, suite 415
Sandy, UT 84070

TOLL FREE
1-866-333-0210

WWW.FORUMSYSTEMS.COM



TABLE OF CONTENTS

THE NATURE OF THE THREAT HAS CHANGED.	3
<i>A shift in attack targets.</i>	4
<i>The risks of business automation</i>	5
<i>The risks of extensive networking</i>	6
STAYING AHEAD OF THE VULNERABILITY CURVE.	7
CONCLUSION	8

Author: Walid Negm
Vice President Product Marketing
Forum Systems Inc.

Release Date: 1/17/2005





THE NATURE OF THE THREAT HAS CHANGED

Despite heavy investment in security technologies such as firewalls and VPNs, enterprises now find themselves more vulnerable to attack than ever before. Malware intrusions, such as viruses and worms, continue to defeat network defenses and compromise mission-critical resources. According to a study by Computer Economics, the cost of worldwide losses from virus attacks is on the rise again, after dipping in 2001 and 2002. In 2004, the cost reached an all-time high of \$17.5 billion. The MyDoom virus alone cost businesses \$4.75 billion. (See chart.) Confirming the extent of this damage, the 2004 CSI/FBI survey reported that, although 99% of enterprises are now running AV software, 78% still detected virus attacks on their networks. Defenses such as AV software are proving essential but insufficient to combat the increasingly virulent and complex threat of malware.

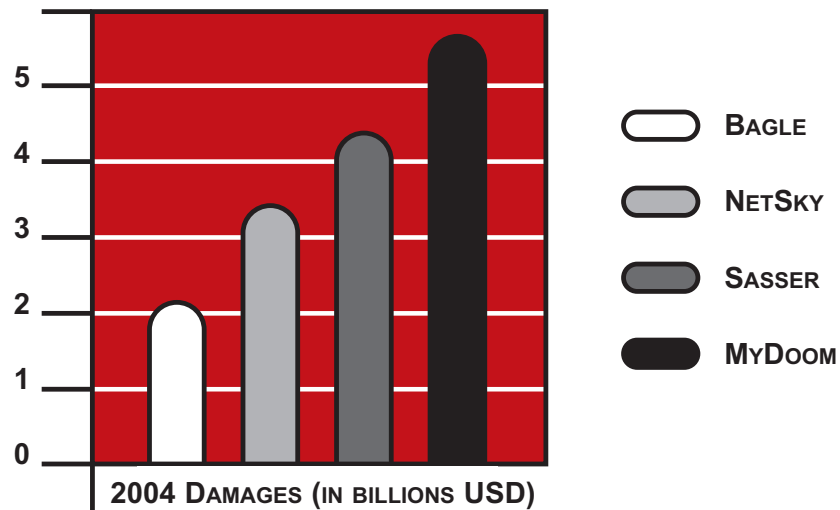


FIGURE 1: COSTS OF VIRUS ATTACKS IN 2004

Source; *Computer Economics Impact of Malicious Code Study of 100 IT and security executives*

Amplifying this danger, increased networking and automation—available in promising new technologies such as Web services—are creating new vulnerabilities by exposing previously sheltered, mission-critical business operations to attack. Recent failures of high-profile Web sites and business services (such as the failure of the Comair airline crew-scheduling software in December 2004) are reminders that any disruption to a company’s communications and connectivity directly impacts its profitability and in some cases its very survival. In the face of continued business automation and ever more extensive networking, information security must be more than a technical afterthought. Instead, information security must be recognized as critical to the mission of the enterprise.





A SHIFT IN ATTACK TARGETS

Until now, risk mitigation strategies have focused on guarding internal IT resources, such as Web servers, database servers, or PCs. But globalization, the extended enterprise, and service oriented architectures have changed the IT landscape. Web services and partner communications now tie businesses together in a complex, worldwide network. Everyday business transactions may involve network nodes around the world—including intermediaries that may have been selected automatically just seconds before they were used. In this lightning fast, hyperconnected world, any strategy that focuses on simply securing a limited pool of devices will prove dangerously myopic.

To protect business operations, enterprises must protect core functions running not only on their internal networks—but also on the public and private networks that their internal networks connect to. Today business functions run on local servers and desktop systems as well as on other systems far beyond the reach and scrutiny of the internal IT team. All these systems, local and remote, are broadly accessible, increasingly complex, and continuously prone to attack.

IT organizations and executive management teams alike must recognize the vulnerability of business functions that depend on networked services. This vulnerability comprises not just malware attacks, but also data interception, data corruption, and traffic misdirection. Management teams must work together to develop vulnerability assessment strategies and defenses for networked business functions. Failure to perform this planning can jeopardize the continued competitiveness of the enterprise.

To understand the scope of these new vulnerabilities, it's important to understand the cascading effects of attacks on networked business operations. The damage inflicted by a single cyberattack can snowball to bring down entire operations by disabling seemingly minor business functions. In the coming decades, we can expect attackers to shift their attention from targeting information resources to disrupting vital computerized business functions (Table 1). Information resources have been good pickings for hackers and malicious users who exploit vulnerabilities in databases, software applications, and servers. But how much more tempting will it be for these users if they can attack not simply servers, but essential operations, such as fund transfers, manufacturing schedules, and product deliveries.

Precautions that have helped guard internal resources will not necessarily protect networked operations. A company can mitigate the risks of a computer virus or a Denial of Service (DoS) attack by adding network bandwidth and redundant IT resources. Additional security controls such as cryptography and authentication can deter the unauthorized modification and outright theft of data. However, the interaction and interdependency of distributed and shared business functions make business processes sensitive to breakdown, even if most of the functions perform properly or make use of redundant configurations. A deliberate (or accidental) disruption in the way a company captures customer orders will not be alleviated by redundant databases. While an oil refinery will not skip a beat if its Web site is disabled, it may suffer devastating consequences if oil truck delivery schedules are altered.



INFORMATION RESOURCE ATTACKS (TARGETING WHAT IS NEEDED TO GET THINGS DONE)	BUSINESS FUNCTION ATTACK (TARGETING WHAT AND HOW THINGS ARE DONE)
INFORMATION, SERVERS, DATABASES ETC.	SALES, MARKETING, PURCHASING, CUSTOMER SERVICE ETC.
<ul style="list-style-type: none"> • Web site defacement • Financial data theft • Denial of service attack on Web server • Network performance degradation • Identity theft 	<ul style="list-style-type: none"> • Interference with on-line air travel bookings and hotel reservations • Interference with on-line banking and financial transactions • Interference with the provisioning of telecommunications services • Interference with demand-driven manufacturing and inventory management • Interference with automatically scheduled actions
<p>EXAMPLE:</p> <p>The Santy worm is an automated script “bot” that spreads by targeting web servers with vulnerable versions of the PHP Bulletin Board (phpBB) software. The worm constructs a web search query (e.g. using AOL or Google) to find web servers running phpBB. For each web server found, it installs a copy itself to the remote system.</p>	<p>EXAMPLE:</p> <p>Comair's computer system that manages flight crew assignments failed on Dec 24th 2004. Without that information the airline was forced to cancel all of its flights for the next day affecting 30,000 travelers in 118 cities.</p>

THE RISKS OF BUSINESS AUTOMATION

Ordering, fulfillment, manufacturing/assembly, payment, billing, sales, marketing and customer service are a few of the critical business processes that make up companies’ operations. The digitization of these business processes automates manual tasks and replaces them with streamlined and efficient computerized business functions. Companies of all sizes can realize these competitive benefits from automating business operations:

- Increased agility—the ability to act on timely and accurate business events
- Ability to rapidly deploy new transaction services such as on-line auctions and e-payments
- Straight-through-processing of transactions and removal of unnecessary intermediaries
- Convenience to the end-user through just-in-time product delivery and manufacturing





But with automation comes risk. Lacking live human management, automated services may be unable to achieve optimal results. For example, a highly trained hospital nurse is part of a chain of command that can mitigate any number of risks by making on the spot decisions that take into account years of experience and situational factors not accounted for in software decision trees. It is the quality of these real-time judgments that distinguishes human involvement in high risk situations from highly automated processes. Enterprises must recognize that they are making a real trade-off between rapid-fire automation and slower, but more comprehensive human oversight. Machines do not have the problem-solving capabilities that people do for responding to new types of threats or other irregularities.

VULNERABILITY EXPOSED: The risk of automation is that it will ignore telltale signs of attacks. Consider a purchase order that is processed electronically between a large supplier and a customer. While an incorrectly accepted \$10.00 purchase order may be inconsequential in the grand scheme of things, pennies that are systematically siphoned off would be a different matter all together. If the intricacies and interfaces described by an organization's web services are attacked, the consequences would be devastating to an enterprise and its entire trading network. To compensate for the lack of human oversight, web services require careful error-checking and boundary conditions to ensure that data tampering and transaction corruption do not occur.

THE RISKS OF EXTENSIVE NETWORKING

By definition, networks are about accessibility and have proven critical to organizational productivity and the ability to unlock isolated assets. Standalone business functions become part of larger systems as the "network becomes the computer." The competitive need to facilitate, rather than restrict, the movement and sharing of information has meant lowering the barriers to business. Resources that were secured by physical separation are now secured by logical separation. Today we are already seeing the growth of "on-demand" federated domains that blur the distinction between what is "inside" and "outside" an organization. The notion of a corporate perimeter has essentially been made defunct by virtual private networks, intranets, Wi-Fi, and messaging technologies.

Increasingly, corporate firewalls and security controls are being configured to facilitate the movement of data, support for mobile users, and remote transactions. But granting access to this legitimate traffic also allows smarter threats to propagate by means of:

1. Remote procedure calls
2. Wireless and mobile technologies
3. Instant Messaging
 1. Location based services and applications with presence
 2. Nomadic code: ActiveX controls, Java and JavaScript programs



A SecurityFocus report showed that of more than 10 million security incidents in the first week of February 2002, 64% targeted port 80, which supports the bulk of business functions. About 9% targeted port 139, used for Windows networking and file sharing, and 6% targeted FTP on port 21. A more recent Symantec security report shows economically motivated threats in the first part of 2004 to be on the rise. The report stresses that the proliferation of computerized business functions (web services, self-service applications) are overly exposing the enterprise.

VULNERABILITY EXPOSED: By using the network as a pathway to business functions, malicious users can access resources that would have been protected in physically isolated network architectures. As web services become more sophisticated and intertwined, they create an overlay “data-level” network that ties together multiple business functions. If one web service is brought down, its failure potentially creates a cascading effect, bringing down other web services downstream. Finally, by combining their own automation with extensive networking, automated attacks will become more adept at rapidly discovering vulnerabilities and exploiting them.

An attack against a single node supporting a purchase transaction in a supply chain could corrupt databases at several companies, interfere with logistics and third-party shipping organizations, and create errors in financial reports and inventory levels. The damage would not be localized to the node that was initially attacked; rather the damage would extend across the business network, spanning companies and perhaps even continents.

STAYING AHEAD OF THE VULNERABILITY CURVE

There are more than 50,000 developers signed up for the Amazon Web Services program. eBay’s business function API’s (Application Programming Interfaces) serve 1 billion XML (Web services) automated interactions every month and approximately 30 million web services transactions every day. The fact that 40% of the items listed for sale on eBay’s U.S. site come in through its API is a leading indicator of the new heights that automation and networking can attain. The transformation from a human-centric business to computerized web services is being adopted not only by the mega-portals but also Motorola, General Motors, and others.

Management needs to be aware of the following attack trends and understand their impact to business operations:

1. Automated intruder activity. Programs that automatically seek out vulnerabilities to exploit are more lethal than hackers working by hand. The threat of automated attacks is compounded by the way that new business process technologies expose their interfaces. Web services are essentially access handbooks for attackers because of their verbose descriptions of how specific services should be invoked. This exposure makes web services highly susceptible to compromise either accidentally or maliciously. Finding design or defense weaknesses simply becomes a matter of time. Malicious insiders can use their knowledge of networks, applications, and security controls to exploit weaknesses even faster than





outside hackers can. (In the 2004 CSI/FBI survey, 66% of respondents reported insider attacks on their networks.) To guard against internal and external automated threats, web services need to be protected at the data level, and security policies need to be enforced for insiders as well as outsiders.

2. Accidents, oversights, and failures. The degree of trust we place in IT automation should make enterprises more sensitive to break downs that are not necessarily due to malicious intent but simply due to the physical equivalent of a “mechanical failure”. Ideally, vulnerabilities that result from software designs flaws, programmer bugs or policy errors, and administration oversights should be discovered before applications are activated and these systems constantly monitored for abnormalities.
3. Emerging Technologies. Web services are the new front line in enterprise risk management. They represent business functions that will be targets for attacks. Supporting technologies such as grid computing, Radio Frequency Identification (RFID) should be assessed for potential vulnerabilities and the security adapted to meet new needs. Securing emerging technologies should not be an inhibitor to business.

CONCLUSION

Information security has traditionally been a reactionary process—the marshalling of technology in response to already exposed and exploited vulnerabilities. But when new threats appear that can deliver a fatal blow to essential business operations, taking a reactive approach to security is no longer a viable strategy. No organization can afford to wait for a disaster to hit and then go into a tailspin figuring out how to respond. Enterprises need to adopt a more proactive approach to security.

First, enterprises need to identify the business functions that need to be protected. Scenarios and situations that may be cause for concern need to be described and prioritized. This approach allows the articulation of a “process-centric” view of security one that is holistic and not simply based on the protection of discrete resources. Vulnerabilities should be determined through systematic discovery and attack simulation on critical processes. By documenting the severity of vulnerabilities and the consequences of the resulting damage, an organization can identify a baseline security policy and security controls. As the enterprise adopts emerging technologies, it will need to engage in a continuous process of vulnerability assessment and response.

Second, enterprise management teams need to put in place plans that can overcome the effects of attacks, accidents, oversights and failures that target business functions. An effective strategy for remediation will include continuous scanning for threats—not just in the form of virus signatures but also in the form of vulnerabilities that jeopardize high-priority processes. As security moves away from the technical realm of cryptography and network intrusion prevention towards business risk management and threat analysis, a company will be able to continue operations even in the face of attack or malfunction.



The ROI for this work promises to be highly rewarding. The Gartner Group predicts that “enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks than those that make an equal investment only in intrusion detection strategies.”

Awareness of attack trends, a continually refined assessment of the vulnerabilities of modern technologies, and proactive contingency planning should become strategic objectives for executive management.

