# Network Awareness:
## *Adopting a Modern Mindset*

## Presented by
## Black Hat Consulting, Inc.

Written By: Michael Bednarczyk, Claudia Giuli and Jason Bednarczyk

## Reality check – What's the current situation?

Information security needs no introduction. It is necessary in all areas of operations - a well-defined need that can be as vague or as specific as one's knowledgebase. As when moving to a new neighborhood, or purchasing a new automobile, one gathers all pieces of information available to help make the best decision that will bring the greatest amount of happiness in the long-term.

One of the greatest challenges that enterprises face, is not merely to generate income, but to ensure the protection of that income. Numerous resources are invested in equipment, tools and knowledgeable people in the name of increasing security.

In the daily operations of the typical organization it becomes imperative to protect the company's assets and moreover to act quickly and effectively against any threats that might impact business continuity. Network Awareness has been a neglected part of the equation.

### Unstoppable browsers and other challenges

The Internet is everywhere and has become a transparent component of our daily lives, and for a majority of the technically savvy, the primary form of communication. The World Wide Web and E-mail are the de facto services in use today. Web browsers have become the modern day newscaster; data packets have become the transport medium akin to pen and paper, traveling swiftly, the zeros and ones find their route to their destinations across the globe. The contemporary enterprise must provide these services to their employees, and as such, browsing, e-mailing and streaming media become seemingly unstoppable.

The Web browser is a complex animal. Although utilizing underlying protocols to accomplish its goals, it presents itself as an innocuous tool to the average end-user. Born from the need for more convenience, the browser integrates many commonly used tools in a simple interface. In some cases, the browser may be integrated into the operating system itself. It can execute whatever integrations, features, and add-ons available to it.

Peer-to-peer networks offer an exciting, yet frightening way to be compromised by downloading what may appear to be a movie, music file, document, or compressed file. However, the individual can never be quite sure what it is that they have allowed to be written to their hard drive while they are waiting for their download to complete. Still yet, the Trojan may be 'wrapped' around the download, allowing the payload to be delivered, as well as the intended application, picture, or song, etc. Statistically, in 2003, there was a 400% increase in the use of viral spread through IM and P2P clients. This trend is only increasing.

In these environments, a ripe breeding ground for potential threats is created. Can the Enterprise protect itself from these implied and explicit threats? Can the network administrator, hope to keep up?

**Common Network Components**

Naturally within the majority of networks in the world, some common infrastructure designs exist. Since components are chosen to perform a specific function within the system, often times they are not viewed as part of a complete ecosystem.

Along with the basic building blocks of the typical network environment, comprised of firewalls, routers, workstations, servers, remote access devices, and software, to name a few, the end-user is a constantly moving piece in the overall network management puzzle. Additionally, organizations may be running software, which they have developed and implemented, creating an additional layer of complexity.

Unpredictable, diverse, and dynamic the end-user needs the network to perform for them, and it is the network administrator's job to make sure that this happens. Diametrically opposed, the users and the administrators must work in unison to accomplish the goals of the organization.

## What is Network Awareness?

Network Awareness is a change in the mindset of the security professional. It lends itself well to any discipline that involves designing, building, managing, monitoring, diagnosing and maintaining a network. It is visualizing the living network from the proper perspective – realizing that each component of the network affects every other one: The people, packets, machines, subnets, sessions, transactions, traffic, and *any* movement on the network on all layers. Any change, action, or machination must be monitored, reported and integrated into the decision making process of the administrator, adopting this new mindset while utilizing the existing technology.

The key is information. By arming oneself with all available data, intelligent, well-formed decisions can be made. Make the wheel better, don't reinvent it. It is not the technology that will solve the problem; it is a shift in the overall approach to network management.

At the highest level, Network Awareness is becoming cognizant of all activity on your network!

*Administrators are aware of the following basic networking concepts, and should continually revisit them when maintaining the network fabric:*

**Accountability:**
The first step you need to take to secure your network is accountability: Can you track what people do? How do they access your services? What servers do they access? What versions of web browsers are they running? What types of traffic do the employees typically generate? The power to know what your employees do will make you not only able to track and act upon malicious traffic quickly and efficiently, but also will establish the groundwork to build an accurate security profile.

**Authorization and Accessibility:**
The second and third steps are relative to the first one and just as important when it comes to security: authentication and accessibility. Once you visualize each component of the network, you must then visualize how each component interacts with each other:

Who is accessing your information? How is it being tracked and stored? How easily can you access this information? Is it presented in a useful manner? What information is available to whom?

## What issues arise when you are not aware of your network?

In the early days of the Internet only a few people had the necessary knowledge and experience to orchestrate an attack, consequentially the number of sophisticated attacks were limited. However, the knowledge and skills have increased; virii and worms have become far more sophisticated, spreading faster and the time to respond has reduced to a matter of minutes.  The collateral damages that virii and worms leave behind jeopardize the Enterprise's profitability and performance. Beyond being a nuisance, the impacts are very real. Will administrators be able to act quickly enough, isolating the intruder and make informed decisions, if there isn't a clear and effective picture of your network topology and the activities that occur within?

Consider this: a malicious program may be infecting one or more hosts on a network, stealing sensitive data, remaining unnoticed, generating only small amounts of network traffic. With proper Network Awareness, this threat would be identified before causing more damage. Loss of information, particularly sensitive data, is unacceptable in the modern world. Proper traffic analysis empowers an organization to make educated decisions and act quickly if anything is compromised. Accountability is the critical factor in securing an environment where it may be nearly impossible to lock-down every network component. What cannot be secured must be monitored.

## What are the advantages of becoming network-aware?

Each organization will benefit from Network Awareness through improving efficiency in their IT department. With this newfound ability to focus their resources and eliminate undesirable traffic (such as malware, worms, peer-to-peer filesharing, instant-messaging, private email, etc), the entire organization gains the potential to become more productive.
In normal operations, the advantages are also apparent. Administrators are focused on keeping their organizations running smoothly, quietly and transparently to the users who depend on them. Even when incident-free, possessing Network Awareness makes it simple to prioritize and determine where the people responsible for maintaining, upgrading, and day-to-day care should spend their precious time. Enumerating machines, applications, services, and connectivity paths arms those individuals with critical decision making knowledge. How can you defend a fort without knowing the landscape that surrounds it?
Protecting against external and internal threats evolves from an abrupt reaction into a process that merely must be maintained through diligence due to being well prepared. Network operations in general benefit from possessing meaningful data that can be utilized in any decision that affects the business that it supports.

It is difficult to quantify the advantages to any specific organization due to the many variables involved in any particular situation, however it becomes obvious when presented as common points of reference that apply to all organizations:

♦ In most cases, time is money. Lost time is costly. When any part of an organization fails, the others that depend on it also feel the impact. In production environments, this can impact revenue significantly. In healthcare, it could mean life or death, quite literally. Consider financial organizations' *dependency* on timely information.

♦ It is not favorable to attempt to reconstruct or recover activity without adequate mechanisms in place. In the case of a critical incident, *accountability* becomes an important key.  Knowing the environment before the occurrence of an incident, such as the players on the battlefield, and the 'normal' movement of traffic, including operational data, transport mechanisms, infrastructural fabric (machine inventory and location) is vital.  Armed with this knowledge, it enables the administrator to devise a strategy to overcome any opponent while preserving the evidentiary chain of custody in the case of post-incident prosecution.  Locating and eliminating this activity becomes trivial with a properly implemented monitoring system. It simply becomes a non-threat.

♦  Another simple example is misuse of company resources. File sharing, Instant Messaging, Peer-to-Peer networking and the potential legal liabilities that they all introduce into organizations, introduce additional risk.

## Statistics – What do we know?

Virii and worms have become more sophisticated and spread much faster in the past few years. They travel worldwide in matter of minutes causing loss of productivity, loss of sales, and extra bandwidth costs among other damages.

According to the 2004 E-Crime watch survey, conducted among security and law enforcement executives by CSO magazine in cooperation with the United States Secret Service and the Carnegie Mellon University Software Engineering Institute's Cert Coordination Center, found that over half of respondents (56%) reported operational losses to be the number one type of losses their organizations experienced last year. Additionally, 25% were financial losses, and 12% declared other types of losses. The 2004 CSI/FBI Computer Crime and Security Survey list the virus as being the number one reason for economic losses among those surveyed (on page 11), amounting to $55,053,900. However, it is interesting to note the irony in the CSI/FBI survey, which placed anti-virus software as the number one used security technology (on page 12).

### The SQL Slammer worm (Sapphire)

The year 2003 reported events of seemingly endless worm out-break. The SQL Slammer was the first worm to take the front pages of newspapers in January and secured a spot in history for being the fastest spreading computer worm. According to the analysis from the Cooperative Association for Internet Data Analysis (CAIDA), Slammer doubled in size every 8.5 seconds during the first minute, reaching a full scanning rate of more than 55 million scans per second after just three minutes, continuing to infect more than 90% of vulnerable hosts within 10 minutes. The worm had congested most vulnerable networks significantly after three minutes, actually hindering its ability to

propagate. It is estimated that 250,000 computers had been infected between Saturday morning in Asia and Sunday worldwide.

**Blaster worm, also known as Welchia and Nachi**
  The Blaster worm screamed its presence to the entire world in August 2003, infecting 100,000 computers in the first three to five hours and 336,000 computers within 24 hours, exceeding the Code Red worm (2001) which had previously infected 265,000 computers within 24 hours and the SQL Slammer that was able to infect 55,000 computers within 24 hours (Rich Pethis, director of the CERT Coordination). On a single network, the Blaster worm had infected 1,000 hosts in August and 35,000 hosts in September (as reported by mycert.org).

**SoBig.F and MyDoom**
  The SoBig.F and MyDoom are both e-mail attachment worms. The SoBig.F was announced on August 2003 and MyDoom on January 2004. Both are attributed as being the worst email based worm infections in virus history to date. The cert@cert.org had accounted SoBig.F for 87% of all the email, receiving more than 10,000 infected messages a day, or one message every 8.6 seconds (Rich Pethis, director of the CERT Coordination). MessageLabs, which manages e-mail security services to businesses worldwide, claims to have stopped over 1.2 Million copies of MyDoom within the first 24 hours and reported a peak infection rate of one in every 12 e-mails. MessageLabs also reported stopping one Million copies of SoBig.F within the first 24 hours reaching a peak infection rate of one in every 17 e-mails.

**Damages**
  At the end of 2002, F-Secure Corporation reported that more than 80,000 known viral threats existed and hundreds more are discovered each month. And as it has been well demonstrated, it only takes a single one of them to cause great damage. External damages from a single worm can include the inability to interface with your clients, and meet the commitments of your company due to the inability to reach your web server, and additionally, the inability to exchange information with your partners due to the inability to reach the mail server.
  Internally, if an incident occurs, the loss will include time, resources and recovery. The losses from a single virus can drastically affect your predicted budget; a conservative yet realistic example follows:
  Company A has 2,000 employees and 100 ongoing projects that they are currently executing on.  Each project includes five people and their network is well configured and maintained. One of the 2,000 employees, named Chris is at home making coffee and getting ready to go to work. While waiting for the coffee to brew, Chris connects to the Internet and while browsing the morning news, decides to check corporate e-mail. Unaware of just being infected with the Xyzzy virus, Chris goes to work and turns the infected laptop on. In matter of seconds, IT starts receiving phones calls from numerous internal departments. Workstations are rebooting randomly, some will not even start back up. Clients begin to call as well, informing Company A that they are receiving numerous emails, and experiencing abnormal behavior on their network, as they realize that they too have become infected.

This fictional virus called Xyzzy has managed to enter the machine through malicious browser scripting code. The virus spreads through network connections that it spawns out, exploiting three vulnerabilities, two of which are known and the other one is not. It scans one million public addresses in only five minutes. It sends mass-e-mails through its own integrated mailserver.

When it becomes clear that Company A's intranet is under attack, the IT department starts to gather all available resources and knowledge available to them, and after a few hours announces their estimate that it will take at least three days to correct this problem. Meanwhile people cannot continue to work and production is halted until the machines are no longer infected.

Using conservative numbers, assessing the damages in this situation is not a difficult task. It becomes apparent that any mechanism that can mitigate this risk is most likely a good preventative investment. In the case of Company A, resources working on the projects are full time employees and make approximately $50 per hour. If it takes three days to clean the infected machines and two days to reassemble and catch up with the progress of the projects, the estimate below demonstrates how quickly the losses add up:

The loss in employee's time alone would amount to $10,000 per project:
8hrs/day at a rate of $50/hr = $400. Multiplied by five working it becomes $2000 per week. With five people on the project that brings the total to $10,000. Including all ongoing projects ($10,000 * 100 projects), it adds up to $1 million. This does not include the time of the IT department's response, costs for remediation, phone calls or hiring external help. It also does not include the loss or cost of any other employee's time, and important to note, the time needed to catch up with the aforementioned projects.

Consider for a moment that Company A may actually depend on web commerce to generate income. As the minutes tick by during the halt in productivity, Company A's Internet clients cannot purchase online. Or worse yet, the orders are coming in, however Company A cannot account or process those orders. It does not take much imagination to assess the magnitude of loss that would afflict this organization. This is not accounting for loss of reputation to their clients, or the affect this would have on Company A's brand.

## What is it that companies fail to realize?

### Chasing a ghost

One of the key elements to securing an environment is Network Awareness. Once again, having a clear picture of the network design empowers the administrators to make not only good decisions, but also to react quickly if the network falls under attack. By recognizing the threats, it enables organizations to isolate the problem, saving both time and money.

For example, imagine a virus as if it were a case of chicken pox: the symptoms are recognizable, and when it becomes apparent that a child is diagnosed with the infection, isolation from all the other children occurs to avoid any further spreading of the virus. However, like any virus, incubation times vary, and exposure to other children is unavoidable. By the time the child is isolated numerous other individuals have been infected. During this timeframe, it is imperative that accountability of the child's whereabouts and activities can be tracked to isolate the outbreak. Although all efforts have been made to prevent an outbreak, it is unfortunately unavoidable since the infection has already been spread.

What people fail to realize is that they are chasing a ghost: one's virus definitions can be up-to-date, server and host based firewalls can be properly configured, patches and software versions current, and yet still be vulnerable to unknown viral exposure; the antivirus is not a solution but a single preventive measure. Each time a newspaper reports a new virus it's reported as the worst outbreak ever. Over the years the virii have become quicker; from Code Red's 37 minutes spreading time to SQL Slammer's 8.6 seconds; smaller; NIMDA's 60,000 bytes to SQL Slammer's 367 bytes; and more sophisticated in deception; the I LOVE YOU's attachment to the Bagle.AQ pseudo-JPG (photograph).

### Protection vs. Monitoring

You cannot protect your environment from every single threat. The first step in defending against a threat is to recognize that the threat exists. In the mindset of the network-aware, you must realize that nothing can be perfectly protected. Once you acknowledge the threat to be defended against is always changing, and accept that in reality, an infallible defense mechanism does not exist, the only method for identifying and isolating the threat is to monitor activity and adjust ones threat model accordingly. *One must monitor that which cannot be thoroughly secured.*

## Common Network Management Problems

As in any common network environment, issues arise as the network and organizations are forced to grow. In many cases, the original network design has become a vestige, making room for current server migrations, partner integration, modern remote access technologies, and additional personnel and additional resources. Often the current network administrator is now responsible for maintaining, managing, and upgrading a network that he or she did not have a part in the original design. It is a very common scenario that a current network map does not exist. This presents many challenges for the average network administrator. It's commonly accepted as part of the job.

Managing an ever growing, always evolving network is similar to managing a growing city. As any system develops, the common needs are the same. The demand for more resources (people, hardware, software, and integration), new departments, infrastructure, and logging mechanisms to monitor and maintain the ever-growing organization can become overwhelming.

Network Awareness aids the administrator by providing a holistic perspective enabling them to visualize their progenitor's legacy.

## Solutions
*Remember that Network Awareness is visualizing the entire environment!*

Experienced intruders target and attack networks by mapping and understanding the environment. The adage 'know thine enemy' accurately describes the Network Awareness mindset. Do not assume that the intruder is playing the same game that his target is, or playing by any rules at all. Studying one's opponent to find their weaknesses depends on accurate information.

Attackers often know their target's environment better than the administrators responsible for maintaining and protecting it. They know the versions of software running, the OS platforms, the services on each host, and the typical traffic that traverses the network. They will also enumerate each machine at different times of the day to study the traffic flow, including when individuals are on their machines, running software, developing, sending instant messages and email, and so on. They will know their targets' weak spots and monitor them. An attacker, whose goal is gleaning information from their target, will take great care to not set off alarms or trigger popular IDS/IPS systems. The intruder will stay unnoticed as long as possible on their target's network.

Can any administrator hope to dedicate as much time as an attacker? Can any one organization know that much about defense and security? Can organizations hope to defend against all of these threats? It's unlikely that the individuals possess enough time, knowledge and resources to protect what is at risk in their current organization. Although not impossible, a proper mindset will ensure the best defense possible.

Presume that your organization can be compromised by threats. Assume the mindset of mapping, monitoring, understanding, and adapting to any threats by arming yourself with the same information that an attacker would gather.  Keep this information current, visualizing how it all fits together. Wash, rinse and repeat.

*Know the threats. Accept the risks. Understand the network as a whole:*

➤ Where is the network map? Does it reflect the current network structure?  If one doesn't exist, or is not up-to-date, CREATE it now! This is critical. Many, many organizations do not possess an operational map of their network to use as a starting point of reference. Without this, how can one expect to correct, or even understand any problems since this is the layer from which everything else emerges?

➤ What servers, hosts, network connectivity devices, printers, etc. are in use on the network? How can risk be accepted, mitigated, or transferred if it cannot be accurately assessed? Administrators MUST have an accurate tally of these items. This should be updated as often as possible as each component introduces risk into the organization.

➤ Are all of the devices in use patched to the current level of their OS? Are all devices using firmware up-to-date? Any server software should also be checked for updates and/or patches. Are any of these set to auto-patch? Is this process verified and documented? In an environment where many hosts are running unpatched services, applications or OS's, if a single vulnerability hits one machine, the entire network will be affected. This is another simple step to increasing the overall security profile.

➢ What kind of services are these devices 'offering'? Each service must be checked and verified. The administrator must be cognizant of any services being 'offered' on their network. Anything less will not suffice. A single low-hanging fruit is all that is needed for a complete compromise.

➢ Who is accessing the network and its resources? Are users on an access schedule? What is the process for users to gain access to corporate IT resources? Are VPN/remote users treated as local users and subject to the same stringent access controls? Are those users compliant with the security policy?

➢ Are these machines configured correctly? Misconfiguration is another common point of failure. A properly implemented security policy should detail out the base configurations for any device offering services on the network. Keeping a standardized, up-to-date configuration for commonly needed services can save time and resources.

➢ Logging is the tool that many organizations misunderstand and misuse. Logging is only as useful as the individuals reviewing them. If a tree falls in the forest, does anyone hear it? The impact of reviewing logs can be imperative. Consider this: single incidents noticed early on can prevent subsequent cascading failures. Logs aren't only for alarms; they are a critical component in visualizing activity as a whole.

➢ Near real-time or real-time network monitoring is an invaluable tool to any organization. Recognizing that every organization has its own limitations, there are a few optimal goals to this endeavor:

  o All typical traffic is monitored.
  o Logging and timely analysis is provided for an overview of operations; interactivity and typical network behavior patterns are identified.
  o Reconstruction, decoding and useful presentation and analysis of data is gathered for the purpose of identifying, isolating and mitigating any type of problem.

***As with any security process, there is a cycle of evaluation and change that is necessary to maintain.***

At the most basic level, utilize the ACI Network Awareness model to get started:

- ✓ ***Awareness***– become aware of the environment and the protagonists that inhabit it. By developing this baseline of knowledge, and extracting from it the current security profile, the organization can begin to understand what *corrections* are needed.
- ✓ ***Correct***-begin the process of correcting and adjusting accordingly. Examine the proposed corrections, and then design a plan to *Implement*.
- ✓ ***Implement***-Implement those corrections and begin the process again with *Awareness*.
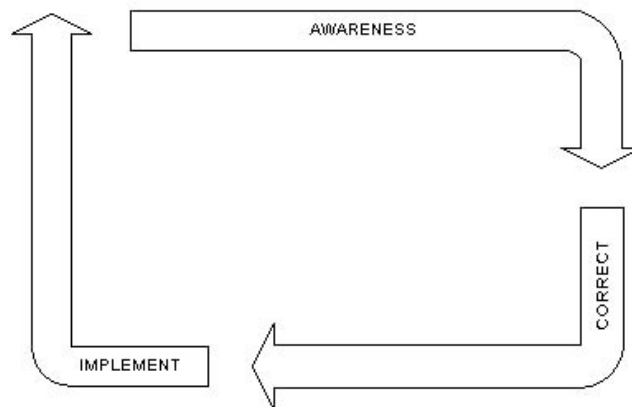


Although Network Awareness is a state-of-mind, accomplishing one's goals of gathering information, from which to begin building a security baseline to work with, likely will depend on the proper use of tools. There are a significant number of commercial and open source tools that exist to aid in this effort.

The choice of tools can be as important as the choice of employees in an organization. A significant level of trust must exist, due to the level of dependency that will arise. In a secure environment, this is of the utmost importance.

Useful aids to the Enterprise would include: tools to map, document, report, audit, monitor, maintain and manage your users, network, logs, communication, and the presentation of information. Perhaps one of the most critical tools necessary to complete the list is a mechanism that will automate and schedule these tasks, *repeating* them as often as necessary.

## Conclusion

 Network Awareness is a necessary mindset. The 'how does it affect me?' paradigm can no longer apply. Without a clear picture of what is happening, what has happened, and what may happen in any specific environment, organizations are at a severe disadvantage. The ability to analyze and tightly focus resources onto developing or current problems will yield significant returns on any investment, commercial or open-source. Armed with knowledge, awareness and capability, any organization can stave off the threats to their business continuity.

## References for further reading and statistical sources:

CSI/FBI Computer Crime and Security Survey
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

The 2004 E-Crime Watch Survey
http://www.csoonline.com/releases/ecrimewatch04.pdf

Rich Pethia, director of the CERT Coordination Center (CERT/CC).
http://www.cert.org/congressional_testimony/Pethia-Testimony-9-10-2003/

The Bagle.AQ virus
http://www.fortinet.com/VirusEncyclopedia/search/encyclopediaSearch.do?method=view
VirusDetailsInfoDirectly&fid=1313

SoBig.F and MyDoom
http://www.messagelabs.com/news/virusnews/detail/default.asp?contentItemId=734&reg
ion=

SQL Slammer
http://www.newscientist.com/news/news.jsp?id=ns99993309

SQL Slammer worm also known as Sapphire Worm
http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

W32.Blaster and W32.Nachi Worm on a single network
http://www.mycert.org.my/graphs/W32.Blaster_W32.Nachi/blaster_nachi.html

Number of Known Virii
http://www.f-secure.com/2002/

400% increase in peer-to-peer
http://news.com.com/2008-7355_3-5116826.html?part=rss&tag=feed&subj=news