Keeping the Chaos at Bay

BECOMING A REAL-TIME ENTERPRISE

PRE-EMPTIVE SECURITY

ALSO INSIDE:

9  • Continuity Plans Falling Short?

10  • The Drive for a Safer E-Government

11  • Planning for the Worst
From the Chairman

“More transparency” ... “greater security” ... “real-time access.” Each of these objectives is a critical challenge in its own right. But imagine trying to achieve these seemingly disparate goals at the same time, on a single system.

That’s the reality for today’s CIO. No longer exclusively focused on technology matters, the CIO is now likely to spend as much time with the general counsel and corporate finance department as with systems integration and database management. Facing hundreds of new cyber attacks this year alone, the modern CIO must work to stay several steps ahead of the latest virus, while simultaneously providing “real-time access” to dozens of new suppliers, contractors and customers. And just as he or she is fully caught up on convergence, there are critical compliance issues to manage.

There’s little doubt that today’s CIOs are facing challenges that never could have been predicted five years ago.

It’s against this backdrop that I’m proud to present Networking Views — a new magazine dedicated to issues, strategies and practical solutions in this often overwhelming new era of “open, secure, real-time” networking.

In this, our first edition, we focus on a range of relevant topics, from security and network safety to regulations and ROI. We bring you some of the best subject-matter experts — from the industry as well as from our own shop — to share their points of view and offer a few practical tips and, perhaps, a different perspective.

So that we can continue to bring you articles of interest, let us know what topics you would like featured in future issues by sending an email to networkingviews@att.com.

Chairman and
Chief Executive Officer
AT&T
As you read this, more than 10,000 viruses, worms and Trojan horses are trying to take down your operations. A habitual hacker may be trying to crack open your inventory records, erase the past year's transactions and dismantle the entire supply chain. Another sophisticated intruder using spyware may be peering into your customer database, stealing precious data and handing it over to your competitors. Any minute, the prized privacy of your customers could be compromised. And then there's the small but growing number of disgruntled employees who may be trying to snoop into payroll records or create an embarrassing breach in the flow of data.

The problems that keep security professionals awake at night are expanding every day. Thanks to the explosive growth of the Internet and the slew of IP-based automation it enables, the network now is intrinsically integrated into the central nervous system of the enterprise. Nearly all business functions, from R&D to distribution, are now integrated on the network, but the security solutions themselves tend to be relegated to the edge.

Additionally, government regulations mandate strict new rules for safeguarding information, and a growing number of companies must maintain auditable financial archives.

Add to that the growing public concern over privacy: As many executives can now attest, lax security measures of customer records can lead to legal violations and hefty fines. As if that weren't enough, nearly half of today's workforce is now able to log on remotely, leaving literally millions of access ports exposed like never before.

In short, the risks from security vulnerabilities are greater than ever. Should the industry start demanding more from the network itself?

> continued on page 12
After routinely cutting costs and consolidating, companies are collectively gearing up to capitalize on the next period of economic growth. At last, they'll be able to move beyond their short-term cost focus and suit up for more forward-looking initiatives that will sharpen their competitive edge like never before.

While many companies were in "competitive hibernation" the last few years, industry analysts were honing in on a new way of operating that could capitalize on the convergence of the latest communications technologies and the emergence of business integration on the network.

Companies today are turning into "real-time enterprises," with workers worldwide collaboratively making decisions based on up-to-the-second information. By operating with "real-time" data and analytics from every part of the company, every function — from advertising to supply chain management — can operate more efficiently, productively and competitively.

According to David Neil, vice president of Enterprise Networking Strategies at Gartner Inc., functioning "real time" is developing into a vital strategy for companies looking to capitalize on the next phase of growth. "Windows of opportunity," he says, are fast becoming mere "keyholes." The need to make decisions and act quickly upon them will be the major competitive advantage throughout this next phase of growth.

As Gartner defines it, the real-time enterprise is one that "competes by using up-to-date information to progressively remove delays in the management and execution of its critical business processes." Neil spoke recently to Networking Views about how today's companies can become real-time enterprises.

NETWORKING VIEWS: David, Gartner has been advocating the "real-time enterprise" strategy for some time now. But suddenly it seems that a lot more companies are paying attention. Why now?

NEIL: It's because there are several trends converging right now, leading many more companies to adapt the "real-time enterprise" strategy.

The first trend is a change in how we manage the supply chain. It used to be that a manufacturer would purchase raw products to build the intermediate component. But today, a manufacturer tends to purchase the intermediate product outright. By relying on a different kind of supplier, the manufacturer reduces the cost of manufacturing and increases the speed of the whole process. This is a new form of outsourcing — using an outside supplier to take over a critical link within a company's supply chain.

An example of this is the automobile industry. Historically, carmakers would purchase flat steel, chromed handles, window glass and paint from perhaps four different suppliers. Today, the same manufacturer would more likely purchase a door already assembled and ready to hang on the chassis.
NV: But haven’t supply chains become disruptive forces inside companies today?

NEIL: Yes, they have. And that’s partly why corporations are restructuring themselves.

This leads us to the second trend in the evolution toward the “real-time enterprise.” It’s the shift to a tightly focused organization, one that sticks to its core competencies. After years of vertically integrated structures, where companies tended to take care of every detail on the customer chain, today’s most successful companies tend to focus on what they do well and outsource what someone else can do better.

For instance, look at the Virgin Group, which includes Virgin Records, Virgin Air and Virgin Wireless. These lines of business have nothing to do with each other. Yet the Virgin Group is successful because it does what it does well: brand management. Virgin outsources its travel, music and communications, but it keeps in-house what it does best. Brand management gives Virgin its global mindshare. Out-sourcing gives it its growing market share.

NV: OK, but how do companies get there?

NEIL: First, of course, you’ve got to get buy-in from senior management. Not only do they need to embrace the changes required, but they have to drive the changes by their own example. They must decide to lead the organization toward more fluid, dynamic and flexible everyday operations.

Then, you’ve got to make sure that the company adapts to changes in new technologies and to ensure everyone uses them to build competitive advantage.

There was a time, not too long ago, when corporate IT resources were monolithic, residing in some remote data center, inaccessible to all but a few of the chief “tech” people. The process of getting to the data was slow, rigid and hierarchical.

Today’s model is a converged network in which voice, data and video are managed as standardized packets of data, all sharing the same switching, transmission and storage facilities. The optimal network today is resilient, redundant and reliable, capable of interconnecting multiple physical networks into a single, seamless structure.

So the third aspect of building toward the “real-time enterprise” is the evolved corporate network. This is a broadly distributed, fully interconnected computing infrastructure that is both adaptable and user-aware. Most important, it is a collection of universally accessible databases that store and organize information that can be retrieved quickly — any time, anywhere — by anyone authorized to access it.

In the end, the “real-time enterprise” delivers access to corporate data, on demand, to those who need it — and in the modern enterprise, data is the competitive advantage.

NV: These three aspects of the “real-time enterprise” evolution — in the supply chain, corporate structure and network — are complex and costly. But you’re saying they’re absolutely necessary for success in today’s world. How can corporations handle it all?

NEIL: That question really is about best practices and, fortunately, they exist. I say fortunately because many companies simply don’t have the expertise in-house to manage these changes in the strategic and holistic way required.

For instance, it’s certainly not necessary for companies to design and administer the network themselves. That critical job, increasingly, is getting outsourced to partners who have experience designing and providing IT resources for enterprise clients. Given the pace of technological changes and the danger of poorly maintained systems, outsourcing IT can be the preferred avenue for both the public and private sectors.

NV: Is this the time, then, for companies to do a bit of soul searching?

NEIL: Absolutely. We’re on the verge of what could be a major burst of growth, which makes this a great time for companies to reevaluate their operations, structure and IT.

Today’s real-time enterprise is challenged by a collection of competing forces — time-pressed customers, reduced decision intervals and strategies that need to change on a dime to accommodate the often chaotic nature of the enterprise customer. The firms that can manage these forces will enjoy a significant competitive advantage, but they need to be committed to reach that level of success.

If they begin to make some improvements now, they’ll be better able to take full advantage of the demands ahead and deliver the business intelligence that keeps them positioned in an ever-increasing competitive environment. The real-time enterprise really is all about being the right-time enterprise.
PRE-EMPTION Remains the Best Medicine

By Eric Shepcaro

Eric Shepcaro is AT&T's vice president, business strategy and development, and spent years with responsibility for AT&T's managed security and business continuity services. Formerly he was president of Netelligence Technologies and managed a variety of hosting and applications businesses. For 17 years prior, Shepcaro served in a variety of management roles at Sprint. He received his MBA from San Francisco State University.

On any given business day at the AT&T Global Network Operations Center (GNOC) in Bedminster, N.J., we monitor more than 3.6 petabytes of data traffic. This gives us a powerful perspective on a great part of the world's communications activity. Like air traffic controllers monitoring the world's plane travel in real time, our engineers keep tabs on trillions of bytes of data flying through the networks of AT&T and its customers, keeping the traffic on course, on schedule and undeterred by any threats it may encounter while en route.

But while scanning literally billions of packets for the normal, day-to-day delays and diversions, we sometimes see a burst of abnormal activity. Right out of the blue, there may be some cleverly concocted combination of code that has managed to penetrate the system. These objects are unpredictable, unavoidable, virtually impenetrable — and use every trick in the book to try to undermine our customers' networks as well as our own.

This year alone we've issued hundreds of alerts, each linked to a major worm or virus that was making its way across the Internet. The magnitude of the AT&T network allows us to spot them thousands of miles away, as they lurk mischievously inside crevices half the size of a pinhead. We can anticipate the trail of a worm and stop it dead in its tracks. We can size up the strength and mode of operation of a virus hours, even days, before it launches its attack. And based on its unique characteristics, we can create plans customized specifically to combat it.

A recent survey by the Computer Security Institute (CSI) and the FBI found that 92 percent of companies interviewed had detected a security breach on their network in 2003. In that year, the effects of cyber attacks cost American companies $13.2 billion, according to consultancy Computer Economics. Next year, network intruders are expected to generate even more challenges than they have this year, and the difficulty of defense is guaranteed to grow as well. In the banking industry alone, identity theft caused by cyber attacks in 2003 cost banks $1 billion, according to American Banker magazine; unfortunately, IDC and Gartner report that 80 percent of cyber crime incidents in the financial sector go unreported, so that number could be even higher. By contrast, ordinary bank robberies set banks back only $70 million, according to the FBI Uniform Crime Report.

As bad as outside intruders have been, the biggest concern this year for CIOs comes from inside the company itself. In the past five years, the
While an intelligent network can provide the best front-line defense, Eric Shepcaro believes that truly effective security comes only with a “dynamic, evolving and adaptable” company-wide security policy. Commitment from leadership, says Shepcaro, has become increasingly critical to the effort.

Eric Shepcaro

What used to be regarded as a relatively simple technical policy is now as much about operations, compliance, human resources, marketing, sales and revenue. Security issues, once the purview of the CIO and IT manager, are increasingly being dealt with by nearly every level of employee and just about every job function. Everyone with access to a computer today has a role in protecting the network.

That “security policies” are becoming so weighty with CIOs is not surprising. Until five years ago, the odds of getting hit were comparatively minuscule, and using budget against such a small possibility seemed almost frivolous.

Back then, the level of exposure was drastically lower than it is today. After all, it’s only been in the past few years that so many outside suppliers, working in a “real-time,” collaborative environment, have had so much access to the network.

The amount of sensitive “life and death” data now flowing online makes a security policy today as imperative as policies guiding employment, compliance, procurement and audits. That’s why a good security policy has become one of the major aspects of business continuity planning.

Security policies, of course, are never “one size fits all.” On the contrary, they are sized according to industry, the amount and type of IP traffic, e-commerce activity, security history and levels of accessibility. The trick is to develop a plan of attack that helps keep the network free of attack.

Today, corporate governance is playing an increasingly important role in the creation of a company-wide security policy. No longer is this just a matter of the network being “up or down”; today these matters are critical to the highest corporate officers. In fact, security now has such an important place at the leadership table that many companies have created new positions — chief security officers, or CSOs — to focus entirely on the issue. In addition, a growing number of leadership teams are regularly engaged in such matters as creating security standards and policies. An increasing number, as well, have gotten involved in creating and overseeing the implementation of new cyber-security measures throughout the enterprise.

Unfair as it may be, an attacker will always have better statistical odds at succeeding than the network will have in repelling an attack. The attacker only has to find a single vulnerability to slip into the

> continued on page 8

number of inside attacks has risen nearly 20 percent. In 1999, 37 percent of companies interviewed for a CSI/FBI survey on cyber security reported they had suffered between one and five attacks from the inside; that number has now risen to 45 percent. While fewer than five attacks does not sound chilling, it can be crippling to a company if just one of those attacks succeeds.

These attacks are potentially far more devastating than ones launched externally. Company insiders (or “former” insiders) have a much greater grasp of the inside workings of the company and its most vulnerable targets and most sensitive data, as well as the most convincing ways to sink into the system. Insiders, many with an ax to grind, may have far more patience than those without a personal interest in the company.

It’s no wonder, then, that cyber attacks have outpaced all other corporate crime in magnitude, cost and impact. Many types of attackers, before launching their destruction, first scan the networks’ likely vulnerabilities. This “trial and error” activity causes unique patterns in network traffic, setting off an alarm and enabling us to mobilize our defenses.

Thanks to AT&T Labs-designed artificial intelligence now embedded in our system, we can identify most intruders minutes before a human even becomes aware of them. With this “early warning system,” we can immediately shore up our defenses, deploy patches, close ports and recommend immediate actions to our customers — actions that are specific to fighting the foe at hand.

For companies whose networks “partner” with ours, the AT&T system functions as their front-line defense. If there are attacks to be launched, the AT&T network is there to run interference, so our customers don’t have to.

That’s one reason a growing number of CIOs are opting to have outside network experts maintain their network security. But there’s another reason CIOs are seeking outside help: guidance in developing company-wide security policies.

HOW AT&T INTERNET PROTECT HELPED PRE-EMPT SASSER

The first signs of an approaching intruder began to emerge on April 14, 2004. Subtle aberrations in traffic patterns made it clear that this was no routine virus, and AT&T immediately launched a series of notices to alert customers. As the days went by, AT&T issued a series of patches to customers in plenty of time to protect their systems. And when Sasser did finally strike on May 1, the patched systems emerged unscathed by the attack, unlike those of thousands and thousands of businesses caught by surprise.
system. On the other hand, the system has to be prepared at any one time for hundreds of individual attackers, each with a different mission, method and mode of operation. While the invader can fail hundreds and hundreds of times, the system needs to fail only once for the attacker to succeed.

So it's a critical exercise to size up potential attackers before they're able to size up your network. Attackers don't meander randomly; instead, they target only the hosts they want most. Like many companies today, attackers have

become so specialized that their skill sets now vary dramatically. Some are specialists in bank ID theft, while others only care about upsetting the supply chain or have their sights set on the payroll department.

So security policies should be designed to reflect the specific types of attacks and attackers most likely to affect the system. It's far more cost efficient to develop defenses specifically to protect against the most likely types of attackers. The challenge is in making sure the network is prepared not for all types of attacks, but for all types of attacks to which your network could be vulnerable. It's always wise to identify the most likely attackers for your type of business, based on industry, scope of operations, type of data and level of sensitivity.

As with any potential disaster, cyber attacks must be planned for with both facts and hypotheticals: What if this happened? How would we go on? What would be the impact on our customers? While the timing and nature of an attack will never be known, the plan to get back to business certainly should be.

And that's why a security policy — a dynamic, evolving, adaptable and driven-from-the-top security policy — is the best insurance against one of the world's biggest threats existing today. As integration and convergence continue to grow, so will the need for greater network security. The increasing reliance on wireless also brings with it a host of new concerns, many of which are first appearing on our radar at the GNOC. Clearly, the surest way for CIOs to keep their networks safe is to plan for the worst and take action to bring about the best.

Cyber-Security Action Plan

Any good cyber-security policy should cover the following areas: governance, assessment, protection, detection and response.

First, get the top leadership on board. A comprehensive security policy involves a total commitment — financial, managerial and emotional — from top officers. Everyone on the senior team should recognize the growing stakes involved and that "cyber security" is no longer just a technology matter; but a business priority. The senior team should be familiar with every aspect of the security policy.

Next, look critically at the most crucial business processes that need to be protected. What are the risks if they were attacked? How exposed are they? Is risk mitigated by handling it internally or outsourcing to a security consultancy?

Then create and implement solutions geared toward preventing the types of attacks most likely to hit your company. Once the measures are in place, conduct simulations to assure their effectiveness. The best measures are those that are proactive, flexible and based on real-time information.

Next, monitor the infrastructure, especially points of exposure, to detect for abnormal events or symptoms of an impending attack. Remember that attackers are continuously reconstituting themselves, camouflaged with new codes and new modes of operation.

Finally, once an attack is detected, launch your best defense. Unfortunately, even the best effort doesn't work all the time; an attacker can slip through and inflict damage. This is the time to put recovery efforts in place, engaging every level of employee, but driven from the top. Every second the network is not up to par costs the company — sometimes irreparably — in customer relationships, time to market, productivity, employee relations and, ultimately, the bottom line.
THRIVING IN ADVERSITY
The Benefits of Continuity Planning

Despite recent attention surrounding business continuity, nearly 25 percent of companies in the U.S. still have no plans to address the issue, according to a report released recently by the Partnership for Public Warning and AT&T entitled “Disaster Planning in the Private Sector: A Post-9/11 Look at the State of Business Continuity in the U.S.”

Ken Allen, executive director of PPW, explains why such planning is so critical now.

NETWORKING VIEWS: Why don’t more companies have business continuity plans, especially in the current environment?

ALLEN: In our survey, companies told us that while they may well be aware of the risks at hand, putting together a proper business continuity plan is just not a top priority. They believe that developing a proper plan would be too complicated and costly. But there actually are many things a company can do with minimal expense and effort that can make a major difference in how well a company weather a disaster. One example: creating a good customer communications plan, something most companies in our survey seem to have done already.

NV: What surprised you most about the survey results?

ALLEN: We learned that companies in New York and Washington, D.C., were some of the least prepared in the country. Given three years of terrorist warnings since September 11, 2001, this was quite alarming. On the other hand, South Florida companies were the most prepared, apparently because of their experiences with hurricanes. Nationally, it seems that having suffered a business disruption is a major factor in whether a company develops a plan or not. In the survey, 80 percent of companies that have suffered recent disruptions have developed a plan. Whether or not these plans are current and well tested is another story, however.

NV: What are the consequences of not having a plan?

ALLEN: In our survey, we found that of the companies that had suffered a disaster, half of them suffered financial loss. Some of them reported losing as much as $1 million a day. Companies need to develop plans that will minimize financial loss. The best way to do this is to keep the business up and running, as best as possible, during and right after a disaster.

NV: What are the most effective ways of doing this?

ALLEN: I think the most important part of the process is to establish back-up sites and redundant systems to protect applications and ensure no data is lost. Planning for alternative work sites will allow a company to maintain operations during a disaster and minimize any financial loss. The good news is that more than 60 percent of survey respondents said they already have taken these steps, and about 15 percent plan to do so in the near future. Wisely, these companies have taken the time to plan for the worst. Hopefully, they'll never have to put their plans into action.
Not surprisingly, cyber security has become a high-priority IT challenge for U.S. federal agencies. With the drive toward e-government, requiring agencies to share data and application services, and the post-9/11 emphasis on agency continuity of operations planning, most agencies have either significantly increased, or plan to increase, their IT and network security capabilities.

After all, in an increasingly vulnerable environment (1.4 million cyber attacks against agencies were reported in 2003), what's more important than protecting the integrity of a nation’s mission-critical information?

A U.S. federal mandate is helping to drive the process toward a safer e-government, with guidelines, metrics and specific recommendations for protecting the federal IT infrastructure. The Federal Information Security Management Act (FISMA), introduced in 2002 and managed by the Office of Management and Budget (OMB), has helped put cyber-security processes on the fast track at many agencies and has already spawned many tangible benefits.

According to Bob Collet, vice president of engineering at AT&T Government Solutions, FISMA has provided agencies the statutory and functional framework to secure their systems and data. Solid progress has been made toward implementing this mandate. In fact, while many agencies received poor security grades two years ago, a growing number have not just "passed" this year, but have been granted grades impressive by any standards. Agencies are striving to earn a "green" rating on the E-Gov Scorecard, which requires proving that their IT infrastructures are at least 90 percent secure.

"While only a few agencies have so far met this standard, other agencies are heading in the right direction," said Collet. "It hasn't been an easy road, but the journey itself has been more rewarding than anyone could have anticipated because it has advanced the goals of e-government."

FISMA provides uniform standards and mandatory measures that must be met by all agencies. But, in addition to doing just the required work, many agencies have also used FISMA compliance to advance their IT capabilities and to create more "security conscious" cultures.

According to Collet, FISMA has awakened agencies to the fact that cyber attacks are growing in sophistication and frequency. It has also prompted them to increase their security expenditures. In addition, thanks in part to FISMA, a growing number of agencies now have direct oversight of cyber-security activities by the agencies' top leadership.

"The most recent E-Gov Scorecards demonstrate that cyber security has become a real management priority at the agencies," said Collet. "More than ever, it appears that IT managers have the support they need from senior leadership."
Planning for the Worst

While cyber security continues to be a significant cause of business disruption, the biggest threats still come from physical forces: fires, floods, hurricanes and tornados among them. No matter how brief the downtime, the costs can be crippling; the impact on customers, competitive ability and credibility can last for years. And the damage on the business can be wide-ranging and deep. No part of the business goes unharmed when the operations come unhinged.

As important as business continuity planning is to a company’s very survival (the Disaster Recovery Institute found that 43 percent of companies suffering a disaster never recover sufficiently to resume business), nearly 25 percent of companies nationwide have not yet developed such plans, according to a recently released survey sponsored by AT&T and the Partnership for Public Warning. This survey also found that many CIOs have either never created a plan or are using a plan that has not been updated or tested in the last year. And even those CIOs who have suffered through a disaster, for the most part, have not created a plan to help them be ready for the next time.

Good business continuity planning spans the entire company, from server farms, call centers and warehouses to marketing, legal and human resources. While much of the focus rightly is on safeguarding data, it’s also critical to put into place contingency plans for manufacturing, customer service, employee relations and every other process, activity and function that keeps the operation going. A vital component often neglected in these plans is communications: keeping all key stakeholders inside and outside the business informed about the disaster and business recovery efforts.

Planning for the “what ifs” today shouldn’t raise the question, “What for?” Here are three best practices every CIO should think about:

1. Continuity Planning. Aim to keep operations up and running with a minimum of downtime. Arrange for back-up work sites and production facilities that can handle the typical daily workload. Are there alternative ways to manufacture products? How can client services continue to be performed?

2. Risk Management. Evaluate the probability and severity of different disasters, and analyze how each would impact the company’s operations — functionally and financially. Identify the company’s greatest vulnerabilities, and determine just how each type of threat could affect these weak spots. Qualify and quantify just how a business disruption would impact the business. How can you harden the most critical operations? How can you minimize the impact of any downtime?

3. Recovery Preparedness. Arrange for hardened back-up data storage sites whose functionalities mirror those at the home base. Make sure data and voice traffic can be diverted from the disaster site to the back-up center. What procedures should you put in place to ensure you can access your “mission-critical” applications? How well will your data be protected at the host site? How quickly can your business processes be restored?

Business continuity plans must be dynamic, flexible and realistic, preparing for the worst but aiming for the best and quickest recovery. They should be updated regularly, tested frequently and shared often with employees throughout the organization.
ever-mounting No consumed by experienced year resulted the growing volume larger-than-ever parts of the email "What was once primarily a technology job is today becoming one consumed by security," according to Matthew Kovar, analyst with the Yankee Group. "Just a few years ago, the CIO's biggest concerns were email access and keeping the network up. Today, CIOs are as consumed with legal and regulatory issues as they are with keeping the data flowing."

It stands to reason, then, that security management is consuming larger-than-ever parts of the day for CIO teams this year. And thanks to the growing volume and severity of cyber threats — the Computer Security Institute says that a third of all security-related incidents last year resulted from thefts of online data — the amount of time and money invested in defense tactics is expected to rise accordingly. A recent NPD Group study said August 2003 was the largest sales month ever for consumer security software, increasing threefold during the weeks following outbreaks of the SoBig and MSBlaster viruses. For virus detection, sales for August 2003 totaled nearly $27 million on 581,000 units, up from $13.7 million the year before. For security, sales for August 2003 were $19 million, up from $6 million the year before.

Ed Amoroso, AT&T Chief Information Security Officer, stands watch over one of the largest networks.

"Today, a company's ability to succeed depends on the CIO's ability to keep the network safe," he said. "And more and more CIOs are realizing that true safety starts from within the network, not with outside fixes."

With a networking system that spans millions of miles around the world, transmitting more than 3.6 petabytes of data each day, Amoroso works to ensure the integrity of AT&T's networks — both those that keep AT&T running and those for its business and government customers. His surveillance at the deepest levels of network operations has made the AT&T networks what many consider some of the safest in the world, and has given Amoroso the recognition as a "top cyber cop" year after year. And thanks to recent AT&T Labs innovations, Amoroso now has a Hubble-like view into cyberspace, allowing him to peer far past the orbit of existing firewalls.

"It's no longer about keeping a step ahead of the attackers," Amoroso said. "It's about keeping five, six, seven steps ahead, anticipating not what they may do next, but what they will do after that."

In fact, he added, once an attack has reached a company's firewall, it may be too late.

"You've got to get them where they live," he said. "You've got to take the fight to the enemy."

The Everyday Network

Despite attention paid to past security incidents and the need to protect against future ones, the biggest priority is still primarily on the business of today. And while security issues remain the fastest growing concern, ensuring smooth sailing for everyday operations remains top of mind for CIOs.

This is especially true now, as networks undergo their biggest transformation since the birth of broadband. Convergence of wireless, voice, data and video is coming full steam. Integration of automated business functions and real-time collaboration — while great for productivity — mean new challenges for everyday maintenance. This doesn't include, of course, the growing number of "outsiders" in the supply chain who need access to the network — and all the day-to-day details involved in clearance and validation.

Networks are fast becoming the corporate central nervous system, playing a role few analysts could have predicted a decade ago.

During these last few years of cost containment and rising economic challenges, the well-run network was able to quietly earn its stripes at corporations around the world. CIOs have used networked applications
Forestalling Sabotage, Corruption and Theft

Ed Amoroso, AT&T's Chief Information Security Officer, spends his days worrying about attackers so his customers don't have to. He and his team have helped literally hundreds of CIOs and IT managers avoid such threats as denial of service, reconnaissance attacks and sniffer programs. They have helped hundreds of companies successfully forestall sabotage, corruption and theft.

According to Amoroso, one of the most useful tools around is software that not only detects the launch of an attack, but just what type of attack it is. The software, acting pre-emptively, uses embedded artificial intelligence to help AT&T spot the danger before it even becomes known to an IT manager.

One type of attack is called the “sniffer.” It can literally eavesdrop on a company's operations and make copies of all the vital corporate data it wants. For this type of intruder, Amoroso says, encryption is the only effective defense. In fact, there are encryption tools that can be added to email and other applications.

“If I had my way,” said Amoroso, “there would be far more training and use of encryption techniques than there are today. Encryption surely is one of the most effective tools in the kit.”

One of the most loathsome attack strategies, he said, is called “address spoofing,” which conceals the true identity of the sender. More and more IT teams, however, have grown wise to this trickery and have installed software to authenticate a source by matching it with a list of approved senders.

Another frequently used strategy is network scanning, what Amoroso refers to as “door knob rattling.” At any one time, there may be thousands of intruders scanning the network for potential vulnerabilities. Once they find any “doors” inadvertently left open, they'll slip right in to wreak their havoc.

Yet another intrusion tool: social engineering. In this relatively low-tech scheme, attackers penetrate the deepest levels of corporate information architecture simply by tricking legitimate users into revealing login ID, passwords and access codes. While this can be one of the most devastating attack schemes, Amoroso said it's also the most preventable.

“Employee training and access control policies are key to preventing social engineering,” Amoroso said. “We'll never be able to eliminate the risk entirely, but training certainly can help.”

Despite all the best prevention, however, new challenges appear to emerge each day. Increased convergence of technologies, across the network and with IT applications, brings the potential for more threats and theft. And, of course, attackers will continue to grow in number and sophistication.

Thankfully, Amoroso and others are hunting down the attackers of today and tomorrow, uncovering ways to stop them in their tracks. Even if the attackers are more fierce and frightening than their predecessors, so, too, will be the network defenses that confront them.
patient information, from drug dosages to payment records, is a challenge for every nursing home, home health care provider and physician network. It's even more important for large medical institutions.

Financial institutions also are increasingly under government pressure to safeguard customer information. For example, in the U.S., the new Safeguards Rule of the Gramm-Leach-Bliley Act is creating growing challenges for IT managers as well as for their legal and compliance officers.

What this means for banks and brokerages is that every transaction must be accounted for in "who, what, where" kind of detail and analyzed at a moment's notice.

"Not only will you have to document who had access to what data and when, but who did what to it and why," Olsik said.

As more and more customers bank and invest online, the need for privacy protection will continue to increase, said Yankee Group's Matthew Kovar.

"It's been the chief obstacle to growing the online financial consumer market," said Kovar, "and if we can provide a greater sense of security for customers' privacy and the safety of their accounts, the consumer base should grow larger."

While privacy concerns will continue to be top issues for customers of financial institutions and government agencies, as well as many other types of businesses, a major hitch in compliance is that privacy regulations are not universal. Companies in Europe, for instance, are used to a much greater sense of privacy protection than companies in the United States.

For online businesses, where little distinction is made handling customers in one country or the next, the perils of privacy infringement can become a major issue in relationship management. And since privacy regulations in the European Union are far more stringent than in the United States, what might be deemed just a clever marketing ploy in New York may mean a major violation in Paris.

"In the United States, the onus is on the customer to 'opt out,'" said Kovar. "But in the EU, the onus is on the company. In the EU, the company must formally obtain consent from the customer to use personal data, and then show proof that the customer has consented."

Regulation, compliance and privacy issues will only mount in the years ahead, even as the technology side of security becomes increasingly complex.

"The biggest challenge a few years ago was just waiting to see what the next 'Sasser worm' virus was going to be or trying to track down the sources of inside fraud or training our remote workers how to protect their passwords and access codes," said Kovar.

But the role of the CIO today is far more extensive in its scope and implications. From an original focus on basic IT functionality to managing cost containment to the current growing pressure to deliver tangible business productivity and growth results, the choices CIOs make on a whole host of issues are more crucial today than they were even a few short years ago.
Detection and Prevention

By the time its presence is known, it’s already too late.

The worm bursts onto the scene out of nowhere — no warning, no clues. A spark, a flicker, the screen fades to black. The hard drive crackles breathlessly out of business. The database is suddenly damaged — its programs deranged, its contents destroyed.

A typical cyber attack circles far and wide, fierce and furious, forcing failure on everything in its wake. Much like a tornado, the whirlwind path of a worm is wildly unpredictable, its speed erratic, its damage incalculable until the damage has been done.

Until recently, worms could only be detected after they had been launched, usually well after their wreckage was waged.

But AT&T has discovered the method to their madness.

When the Sasser worm was launched earlier this year, AT&T’s Network Protection Services team was able to meet the challenge head on. By detecting minute, abnormal changes in network activity, the team was able to spot the worm’s developmental progress and observe it seeking out possible vulnerabilities in the network. Using the macro monitoring capabilities of AT&T Internet Protect Service, the team was able to accurately calculate Sasser’s path, speed and mode of assault. Thanks to this early detection system, AT&T was able to issue warnings to customers weeks in advance of the attack. AT&T created software patches, blocked ports and instructed customers on how to protect their valuable data and systems.

For thousands of companies, a potential fatal attack was thwarted, thanks to the work of the cyber detectives at AT&T.

According to Kovar, companies increasingly are looking to partner with specialist firms — for everything from database protection to compliance with federal regulations to networking security management — to help them keep their operations running and secure.

With the stakes so high and market demand surging, it’s no surprise that more than four million so-called “security vendors” emerge from a single Google search.

But Oltsik advises companies seeking outside support for their security management to do the highest level “security check” on their own. Potential partners should be checked not only for their technology expertise, but for their understanding of the unique compliance issues affecting every industry today.

“When CIOs can rely on an outside expert, a real partner they can trust to safeguard their network, not only does the CIO team benefit, but so does the company, its employees, suppliers and customers,” said Kovar.

Not surprisingly, both Kovar and Oltsik expect the rate of cyber attacks to only grow the rest of the decade, leading most CIOs to continue keeping security top of mind.

New government mandates will mean far more time dealing with compliance. New privacy concerns will mean more time creating policy. And new competitive pressures will mean great opportunities for CIOs to facilitate improved productivity, processes and performance.

But what may be most critical for the CIO today: an intelligent, flexible and responsive network that actively performs as the CIO’s partner in the quest for greater security.
TOTAL SECURITY. Can your network detect, isolate and eliminate virtually any security threat before it becomes a security breach? Whether intruders come from across the world or across the hall, AT&T’s proactive networking solutions can identify and neutralize threats long before they have a chance to damage your data, your systems or your business. **CAN YOUR NETWORK DO THIS?**

AT&T
The world’s networking company™

For a network that can, call 1-888-889-0234
att.com/networking