AUDITNEWS

Volume XXXIV **Spring 2003**

WELCOME TO OUR NEWEST STAFF MEMBER!

The Internal Audit Department welcomes Patricia O'Donnell (Tricia) as a new member of our department. Tricia comes to us from Deloitte & Touche, LLP where she worked for two years as an Enterprise Risk Services Consultant. Her duties at Deloitte & Touche consisted of providing control assurance services within financial, manufacturing and higher education industries and assisted management to identify and improve business processes. Within the University, she will be reviewing and evaluating the soundness, adequacy, effectiveness, and proper application of accounting, financial, and other operating controls for complex business operations. Additionally, she will determine the level of compliance with controls and other established policies, plans, and procedures, and determine the extent to which University assets are accounted for and safeguarded from losses.

INSIDE THIS ISSUE

ALERTNESS AND CURIOSITY IMPROVE SECURITY

"Eternal vigilance is the price of liberty" – attrib. to Thomas Jefferson

by: David Escalante, Information Technology

The Problem

Sometimes people expect their computers to provide complete "security" for them including protection from all sorts of potentially malicious problems, including viruses, hackers, network intrusions, and people sharing the same computer who may delete the wrong files by mistake. While a computer can be set up to do all this, a standard, out-of-the-box computer, even in a data center or computer room, is *not* set up to repel all attacks. In general, the nature of Boston College as an academic community performing research and learning leads to a computing environment that is more wide open and accessible than in businesses, or even in some peoples' homes.

Rather than spending large amounts of time making a computer completely secure, or "bulletproof," it frequently makes sense to simply monitor the computer's behavior and its records to ensure that it is not being misused. This monitoring, which serves to *catch* misuse of the computer rather than completely *block* misuse, closely models the way much of our society works. While there are many laws governing behavior, they are enforced when laws are breached. Fear of detection and punishment are most often why people obey the law, not limits on their ability to actually perform an illegal activity. Because people are not *prevented* from doing bad things, only *punished*, many truisms have arisen in day to day life having to do with observing the environment and ensuring that you are not placing yourself at risk (i.e., "Don't accept a ride from a stranger").

continued on page 6

THE RISK OF INTERNAL SECURITY VIOLATIONS

by: Tricia O'Donnell

It may go unspoken, but one of the greatest threats to our computer information systems is not necessarily external hackers but the faculty, staff, and students of the University. *Individuals with **authorized** access to the University's networks, systems, and proprietary information present a higher risk than outsiders who need a security hole to attack.*

In addition to the University, various corporations have been devoting efforts to increase defenses against external security violations. However, information systems are susceptible to internal attacks since restricting trusted users has been overlooked. Protecting systems from insiders requires a unique approach, and equal attention. The development and enforcement of security policies can be the initial step in preventing internal security breaches. But many companies have not created security policies due to the difficulty of designing, implementing and enforcing the policies. Or security policies are written or ignored until security violations occur.

While external attacks are serious, an internal violation is equally as destructive. A study was performed by Activis Security to research the origination of security breaches. The study included a survey of 146 companies which concluded that:

- 81% of security breaches originated internally;
- 13% originated from ex-employees; and
- 6% originated from external hackers.

Attacks may arise from a disgruntled employee who is motivated to bring down the network or manipulate data. It is these disgruntled employees, either current or former, who have the access to steal or corrupt information.

Without enforcement of formal security policies, employees are unaware of the consequences for their destructive actions. Security administrators are looking towards the implementation of tools to develop and enforce security policies. Systems have become so complex and vulnerabilities so numerous that it is impossible to manually enforce IT security policy today. Security administrators want security policies implemented within operational processes. For example, an alert would be automatically sent when a policy is violated during real time monitoring. Vendors are enhancing current products to automate the security process. Current security products available today are being modified in order to meet companies' growing needs. Versatile security tools need to provide processes to:

- Create and document security policies;
- Monitor system configurations and settings against policies to identify gaps and weaknesses;
- Enforce password parameters, such as minimum length, expiration;
- Monitor specific security applications such as firewalls;
- Enforce email, instant messaging, web surfing policies;
- Deploy and track security policies against best-practice templates.

Overall, security administrators want an easier way to investigate and fix security breaches. Security tools should be offered as a complete suite from policy creation to monitoring and enforcement.

If appropriate security tools are implemented, companies will expect to reduce the current high expenses that result from security breaches. Security tools are expensive, but the cost/benefit is favorable in the whole picture. Losses from security breaches average around $4 million per company, but security software costs between $10,000 and $50,000. Users are simply unaware that their actions can create expensive security risks such as turning off anti virus software or firewall software. Even reinstalling an old version of a web browser without updating patches creates a costly security risk.

The increasing number of wireless devices seeking to access company networks is also becoming a large concern. Organizations are put at risk when users set up a wireless access point in their home offices that is open enough for a determined hacker to gain unauthorized access to the system. Desktops, notebooks, and handheld devices are also subject to a

more secure network. The unprotected notebook of a trusted employee or consultant is a large threat to an organization. Settings and enforcing security policies is a big step toward protecting enterprises from the inside threat. Vendors are in competition to develop the easiest process for providing real-time protection to desktops, notebooks, and mobile devices and automatically enforce security policies.

Sources:
Hulme, Geroge V. (2003, April). The Threat From Inside. *Informationweek.com.*

Robb, Drew (2002, July) *Internal Security Breaches More Damaging.* Retrieved from http://www.itmanagement.earthweb.com/secu/article.php/1405031

DOING BUSINESS ETHICS JUST RIGHT

by: John Soto

"The issues that provoked the present crisis were not overly subtle. You don't need a weatherman to know which way the wind blows, and CEOs do not need a business ethicist to tell them right from wrong."
Gordon Marino, Professor of Philosophy at Olaf College in Northfield, Minn.

During the past year, business ethic scandals have been headline news. We are reading more and more about what happens when business ethics go wrong. Wouldn't it be wonderful to read some stories about what happens when business ethics go right? There's the paradox. When we get business ethics just right nothing much happens, since we don't need to engage in damage control, firefighting, and expensive legal defense. That's what we want.

So, what can an organization do ensure that its employees get business ethics just right? Organizations, both for-profit and non-profit, should adopt ethics programs that contain the following seven factors:

- Establish compliance standards and procedures that are reasonably capable of reducing the prospect of criminal conduct.
- Identify high-level personnel within the organization, and assign overall responsibility to oversee compliance with standards and procedures.
- Use due care not to delegate discretionary authority to individuals whom the organization knew or should have known had a propensity to engage in illegal behavior.
- Effectively communicate the organization's standards and procedures to employees.
- Take reasonable steps to achieve compliance with standards by utilizing auditing and monitoring systems; put into place and publicize a reporting system whereby employees can report criminal conduct without fear of retribution.
- Consistently enforce compliance standards through uniform disciplinary action, thereby establishing common expectations about business conduct in all business units.
- Take reasonable steps, if an offense is detected, to prevent further similar offenses, including any necessary modification to the program to prevent and detect violations of the law.

Many Organizations that have implemented ethics programs are less likely to be involved in criminal misconduct, to be targets of criminal investigations, or to be prosecuted, and, if found guilty, may receive less onerous penalties and fines.

Once ethics programs are established, organizations must consider whether they are working and affecting employee behavior in a positive fashion. If the goal is to create an environment for ethical action, employees must feel that they can come forward with questions and concerns and be treated in a civil, respectful, and confidential manner. Hence, one must examine employee perceptions and attitudes when measuring program effectiveness. Employee perception drives behavior. For instance if employees trust that calls to the organization's ethics "hotline" are held in confidence, they will act accordingly and continue to call the office with questions and concerns. If, however, employees perceive that the program does not safeguard their anonymity or confidential information, they will stop calling. When every employee has the courage and ability to talk about ethical dilemmas, we are doing business ethics just right.

Sources: "Business Ethics: A Set of Practical Tools," by Joan E. Dubinsky, *Internal Auditing*, July/August 2002, pp.39-45.
The Wall Street Journal, 7-3-02, page A14.

TOP SECURITY RISKS IN THE FUTURE

by: Pamela Jerskey

Gartner Research has recently released a report that outlines future security risks and recommendations that every business should be aware of.

Web Services

Web services are growing fast and make it easier for enterprises to integrate existing legacy applications. Enterprise web services are usually protected behind firewalls and are used to exchange data inside and outside the organization. Applications that manage this data can reside on different software platforms. Therefore Web services are extremely valuable when enterprises shift the primary focus of application development from enterprise application integration (EAI) to secure extranet access management (EAM). Organizations are reluctant to expose valuable data and computing resources over open networks in the absence of adequate security mechanisms. For this reason, Web services require closer attention to security than do other applications. A trusted Web service incorporates mechanisms for confidentiality, data integrity, non-repudiation, authentication, and authorization.

Wireless LAN

Wireless networks pose a major threat of information theft because security for wireless systems is not ideal. Wireless security will evolve to fit with the needs of advancing technology. The following principles apply to all systems, including wireless: (1) authentication, (2) access control and authorization, (3) non-repudiation, (4) privacy and confidentiality, (5) integrity, and (6) auditing. Authentication is the process of identifying who is asking to get into your system. Access control and authorization is the process of controlling entry to specific resources. Non-repudiation is the principle that a user or process be identifiable and accountable for its actions. Privacy and confidentiality is the principal that a user has a right to protect his/her information from unauthorized disclosure. Integrity is the principle that a user has the capability to verify the accuracy of information. Auditing is the principle that activities are reviewed to ensure appropriateness for a given entity.

Identity Theft

Most identity theft is accomplished by ordinary means such as "dumpster diving." Someone can steal your identify by co-opting your name, Social Security number, credit card number, or some other piece of your personal information for their own use. Identity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft. Organizations should have identity management and provisioning plans in place to educate workers on dangers and prevent workplace identity theft.

Role of Security Platforms and Intrusion-detection Systems

Security systems are developing from detection into programs of prevention of intrusions before they occur. Many intrusion detection systems base their operations on analysis of OS audit trails. This data forms a footprint of system usage over time. It is a convenient source of data and is readily available on most systems. From these observations, the IDS will compute metrics about the system's overall state, and decide whether an intrusion is currently occurring.

Correlation of Events for Reporting, Monitoring, and Managing Consoles

Organizations will become more efficient by implementing console software to compare data across all parts of the network to determine if an attack against one part of the infrastructure is related to a problem on another part of the network.

The Next Code Red/Nimda

Code Red and Nimda cost organizations $3 billion in lost data and time. Businesses will need to minimize vulnerabilies, including putting patch-management policies in place to prevent future attacks. Keeping an operating system and applications up-to-date is a fundamental security practice. Weaknesses pose threats. The volume of weaknesses and the number of patches required to address those weaknesses can be a threat if not managed carefully. Without patch-management tools, many network administrators track patch status in their heads and fix holes on the fly. The complexities of networks and number of patches have rendered this approach ineffective.

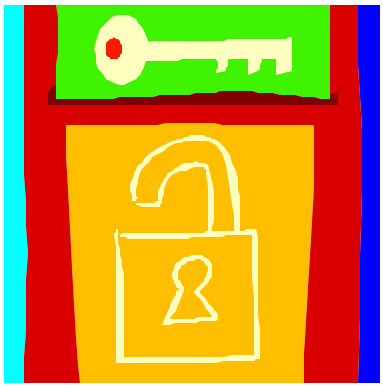
Instant Messaging

Instant messaging and other peer-to-peer programs create holes in a network's defense. Without IM policies, users can publicly expose sensitive company data and information. Unlike e-mail, IM leaves no record of communications. In addition, IM file transfers aren't subject to server-level virus scans, so users face a real threat of virus infection. Since deployment isn't controlled, an organization can't control how systems are used. Given IM's pervasiveness, businesses need to think about IM security as a part of a company's security structure.

Homeland Security

The Department of Homeland Security is still getting underway and needs to incorporate various risks and recommendations by industry and government agencies. The document, "The National Strategy for Homeland Security, was developed to (1) provide direction to federal government departments and agencies that have a role in homeland security, and (2) suggest steps that state and local governments, private companies, organizations, and individual Americans can take to improve security.

To read about these issues and others, go to http://www3.gartner.com/1_researchanalysis/research_overview.html



(continued from page 1)

This statement has to do with being aware of your environment and alert to unusual changes or activities because someone *could* break the law and physically assault you. In the same way that a person will be safer by not placing himself or herself at risk, a computer whose user is alert for and monitors unusual activity is much safer than a computer where unusual activity is ignored.

What to Do

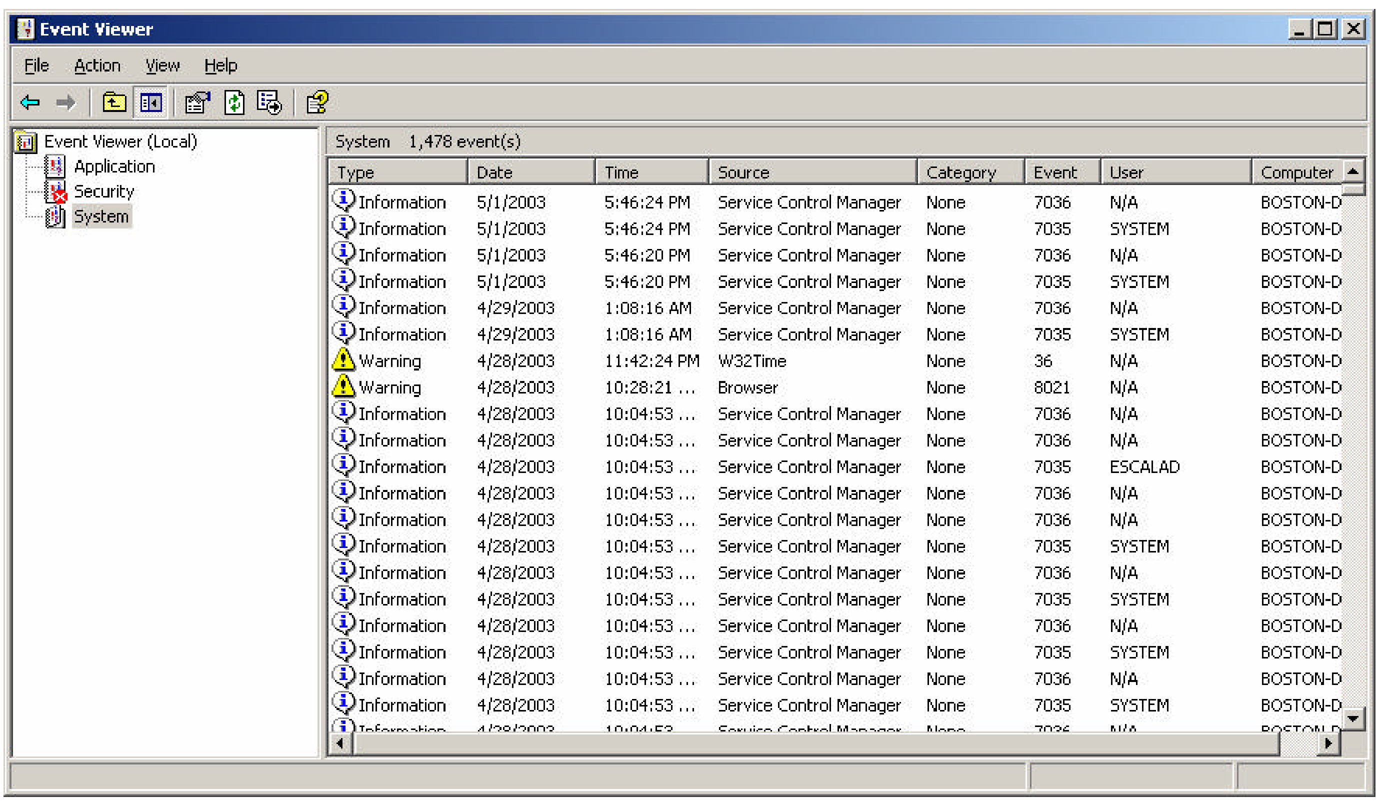
As the quote that opens this article implies, **be vigilant**. In an open academic environment, you must assume that there are people conducting experiments on their computers that may not be helpful to the health of your computer. Therefore, be alert to the way your computer usually looks and behaves and, if you notice significant changes that you don't understand, seek an explanation. Especially important are new error messages such as a log being full, or something being detected. I once encountered a user who infected a whole department with a virus because when an unusual message appeared on the computer screen that said, "Your computer is infected, click 'fix' or 'continue'", the user always chose to 'continue' over a period of weeks until the virus had spread. At Boston College, you can report puzzling changes to your Technology Consultant. They in turn may call on various resources in Information Technology and Services to determine if there is a problem.

Examples

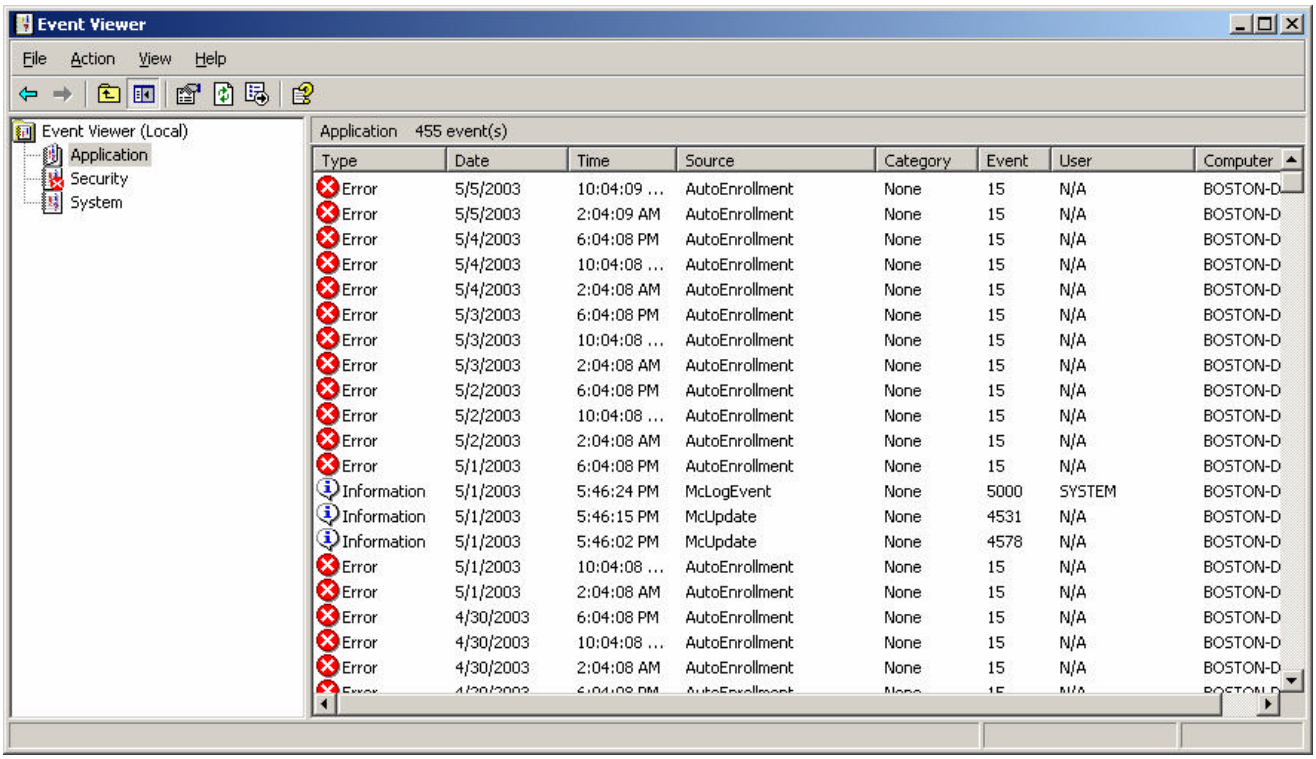
It's easy to say "be vigilant" and "watch for unusual behavior", but what does that mean in practice? Let's take a look at a Windows XP system and see a few places you can look for unusual behavior.

Event Viewer

The "Event Viewer" program on your computer displays both usual and unusual activities in three areas: Application (programs), Security (accesses to computer), and System (the computer itself). It can be accessed from the "Start" menu under "Administrative Tools." Each event will have one of 3 icons – an "I" for informational, an "!" for a warning, and an "X" for an error. Below is a normal-looking set of events.



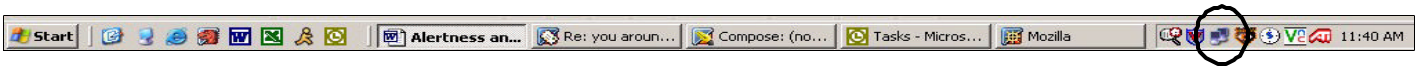
Now, for contrast, let's look at the same computer's Event Viewer for applications:



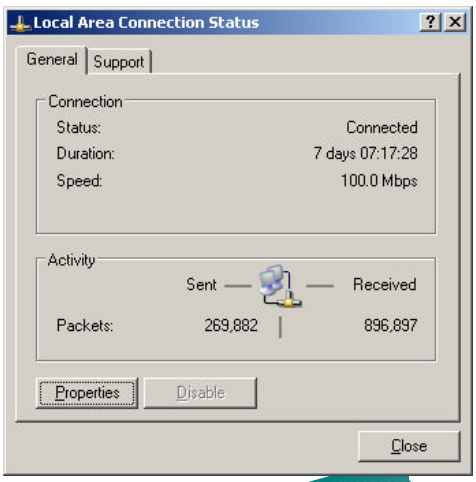
Note the large number of errors by something called "Auto Enrollment." If you double-click on one of these errors and can't understand it, and there are large numbers of errors, it is wise to seek advice from a more knowledgeable source. (N.B. The "Auto Enrollment" error is actually O.K. to have.)

Network traffic

If your computer has been "hacked," how can you tell? One way is to see if a lot of information is going in or out of the computer when you're just talking on the phone, or typing into a word processor or spreadsheet. That would be suspicious if it were a *lot*, versus an e-mail program doing a quick background check for new messages. In Windows XP, it is possible to put an icon on your Taskbar that shows a graphic of network traffic as circled below:



The icon looks like a pair of small computers, and the screens of these computers blink unobtrusively when information is going to or from your computer over the network. If you double-click on the icon, you can get more information, as shown to the right.

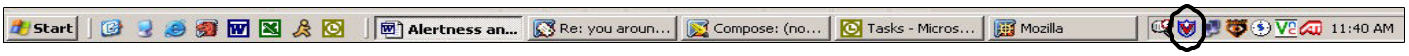


If your computer is sending a large number of packets, that is unusual because in general, people receive more from the web and e-mail than they send out, unless there was a large attachment sent recently or something similar. To place this icon on your taskbar, the steps are:

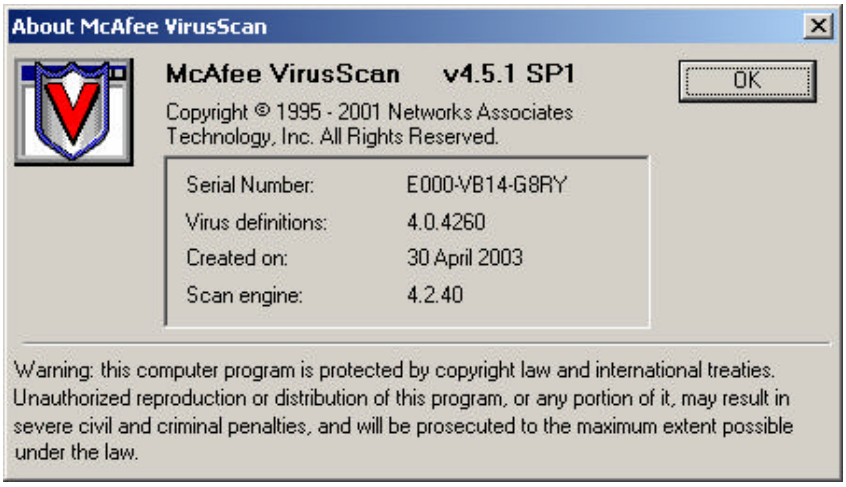
- Choose "Start", then "Settings", then "Network Connections", then "Local Area Connection".
- Double-click the "Local Area Connection" to get to the Status screen shown above, and then click on "Properties".
- Under Properties, click the checkbox on that says, "Show icon in notification area when connected."

Virus check

Your computer should be running an anti-virus program such as McAfee. You can check for this by looking at the taskbar and seeing an icon like this for McAfee:



If you right-click the icon and choose "About", a message is displayed which shows the latest virus definitions you are running. The one below, for example, shows April 30, 2003 definitions. Your definitions should never be more than a few weeks old.



If you right-click and choose "Status", you can see various information about what parts of the computer are being scanned for viruses and when.

Examples Summary

The examples above – events, network activity, and virus updates – are three easy things anyone can do to monitor a Windows 2000 or XP computer for unusual activity. Remember, vigilance to change and unusual events is a key factor in improving the data security of both the computer on your desk and the campus as a whole.