LockDownIT
Securing Your IT Equipment

1434 Roxbury, Ann Arbor, MI 48104
www.LockDownIT.com

(877) LockIT0   [877-562-5480]
info@LockDownIT.com

A White Paper Provided by LockDownIT LLC:

Complete IT Security

A systems level overview of IT security issues

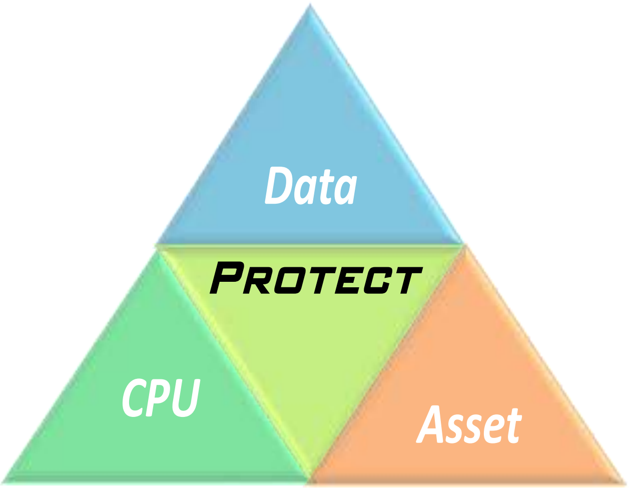
IT Security Overview

IT installations in general encompass many types of equipment: servers, workstations, handhelds, laptops, mobile phones, PDAs, Network Attached Storage, printers, and network devices such as routers, switches, firewalls, etc. Some of these components may be located in internal, locked and secured areas while others may be in public or quasi-public spaces. The comments and discussions in this white paper are addressed to all of these different pieces of equipment.

There are three central components to securing IT installations:

- Protecting the Data
- Protecting the CPU
- Protecting the Asset

The 3 Components of IT Security



1. Protecting the Data

Data are vulnerable in many:

- **What is data?** Not such a silly question. Obviously data about customers requires protection. So does company information like financials, accounts etc. Less obvious but also critical are data and files about processes; for example an image file used to certify documents is a valuable piece of data [think passports, drivers licenses, etc.]
- **Where in the World is the Data?** Data no longer sit in guarded vaults in corporate headquarters but can be found on laptops and palmtop computers, on data CD and DVD, diskettes, thumb-drives, SD cards, various forms of data chips and cards found on cell phones, mp3 players, cameras, etc.
- **Loss of Data.** Organizations can be damaged if their data is damaged due to fire, hurricanes, tornados, earthquakes, vandalism, etc. The point is data doesn't have to be stolen to damage an organization.

What can get stolen? What's the value for the thief?

- **Identification Theft.** We've all seen and heard the stories of laptops going missing with customer information on them, credit card numbers being compromised, servers being hacked and sensitive, personal information being stolen.
- **Data Theft.** Confidential company information such as financial information, product information, and customer information all have the potential to seriously damage an organization if they are stolen. There have been stories of CIA and pentagon laptops going missing / being stolen with the loss of classified information.
- **Data Insertion.** What if instead of stealing information, a criminal succeeded in inserting erroneous data into an organization's data base? Admittedly a more difficult task but at the same time having the capacity for much greater rewards for the criminal: they could give their credit card unlimited credit, they could manipulate financial data in order to profit on the stock market or they could manipulate experimental data from, for example, drug testing to profit from the lucrative drug market.

Clearly there is no argument that data need to be protected. What then are the effective means of protecting data?

When it comes to protecting data, there is no single solution or single element that provides complete coverage. Rather there are layers of strategies and tactics that give rise to system data protection. Not every organization will implement every solution from the list below but they will choose those components suitable for their organization.

Solutions to data protection include [in no particular order]

- **Encryption**.
  - Encryption of individual files can be used and/or encryption of entire [disk] drives. Suppose for example that a laptop is stolen or that thieves vandalize the office and steal the hard drive.
  - With encryption the data are fairly safe; encryption can be defeated with enough time and a powerful enough computer driving it but for all practical purposes encrypting the data will protect the data if the physical storage device is lost or stolen.
  - How does one go about encrypting the data?
    - There are software solutions available that do an excellent job of protecting the data.
    - Microsoft has built data encryption as a capability in Vista.
    - Many hard drive manufacturers are building hardware implementations of encryption onto their drives so the penalty in slower throughput or longer computation cycles is minimized if not eliminated.
    - PDAs and mobile phones should also have encryption capability.

  - Choosing to implement encryption is a no-brainer – every file today should be encrypted.
  - Even in the context of a corporate or office-wide storage server, encryption can protect data files against hackers should they gain access to the network.
  - Encryption of files should be enforced especially for mobile data: Optical media like CD or DVD, Thumbwheels, SD cards, chips, etc.

- **Backup**. Is there any reason to explain data backup or argue for its implementation? There are many products and many published backup policies to help an organization implement effective backup. Everyone needs to implement data backup. The one important piece of advice to impart is that the backup data needs to be tested on a regular basis to insure that in the event it is actually needed that the data can be successfully recovered.
- **Control where the data goes.**
  - Data should not be kept or stored on computers which sit in public or quasi-public areas and are thus susceptible to being stolen or vandalized. [A few years ago an office of the Pennsylvania state Department of Motor Vehicles was broken into and computers that sit in the public areas were stolen; the computers contained data about how to print valid drivers' licenses.
  - Companies and organizations should store all their data files on servers that are physically located in secured areas. Large corporations may have security personnel to prevent unauthorized access to the physical devices. Small and medium sized business should also keep their data files on equipment that is locked in a room or even a closet but they should understand that such installations are still vulnerable to break-ins especially after hours and thus they should take the additional precautions of encrypting these devices and files.
  - In any event, individual data records and fields will find its way over the network to workstations, laptops, PDAs, mobile phones, etc. in response to application requests. Applications should be written in such a way that caches and temporary files are purged periodically or when a record is no longer needed by the application; laptop and desktop computers should have scripts and procedures invoked at power-off, stand-by or hibernation to positively erase all traces of the data [positive erasure is a method whereby the physical sectors of a disk are overwritten to destroy any trace of the previous data stored there].
  - Data should be kept in a way that when data is checked back in from an application that its integrity and credentials can be checked to verify that the returning data is trustworthy and not a 'poison pill' from a hacker.

2. Protecting the Processor

The second component of a total IT security policy is to protect the CPU – central processing unit – on each of the computers [servers, workstations, laptops, palmtops, PDAs, mobile phones, etc.]. This means insuring that only certified, trusted programs and applications that get executed – as opposed to allowing, say, viruses, worms, renegade scripts, malware, etc. to seize the CPU and run their destructive codes.

This aspect of security has received the most publicity, headlines and attention since the advent of the personal computers in the mid-1980s. Initially there were viruses that would be hidden on floppy disks and diskettes and which would install themselves on the PC. The advent of networking and internet connectivity and emails with attachments increased the number of ways and the ease with which such malware could be sent around and inserted into unsuspecting users' computers. One of the myths about malware is that only Windows devices are at risk; this is untrue as Apple computers and Unix and Linux computers are all at risk as objects of a malware attack. One of the dynamics at play here is that a majority of the hackers have been motivated by an intense dislike of Microsoft and Bill Gates and on the other hand have a high degree of regard and respect for Apple and Unix-like systems and so Microsoft has been targeted much more heavily [in some circles attacking an Apple is considered poor sportsmanship].

There are a large number of anti-virus and anti-malware programs available – from companies such as Symantec, MacAfee, TrendMicro – and many magazines and websites that test and review all these offerings on a timely basis and provide recommendations. Almost all of the anti-virus products work on a reactive basis – attacks are spotted because they fit a profile or signature for a specific known virus; stopping an attack of a new virus is very difficult which is why a good IT Security policy includes bans on emails with attachments or users bringing in outside software and installing it themselves on their machines. The point we would make here is that it is critical that every device be protected by and anti-virus/anti-malware program and there should also be IT policies in place to restrict or eliminate a user's ability allow uncertified code onto a device to insure that only trusted code gets to run on a device.

A second part of protecting the processor lies in network devices like firewalls which can protect computers from having unrequested files inserted onto their storage drives. That is, a firewall is a device which typically only lets into a [private] network messages [data packets] sent by a trusted source in response to a message that a member of the network has sent out in the first place. There are cases, though, where hackers gain control of a computer within a network by managing to deliver messages [containing code in the form of scripts or viruses] through the firewall to a trusted computer by exploiting a hole in the firewall, typically an open firewall port. This is one of the issues in setting up a network and in establishing an IT security policy – some applications insist on opening obscure ports in the firewall and hackers are adept at seeking out open, insecure ports in a firewall.

Protecting the CPU involves anti-virus and anti-malware software packages, knowledgable users who don't allow untrusted messages and files onto their devices and a firewall and IT security policy to enforce rigorous standards of operation.

3. Protecting the Asset

The third component of a total IT security is to protect the assets themselves. In Protecting the Data we discussed how theft of a computer or its disk drives was one way that data can be stolen. Beyond that, though, preventing the theft of the computers themselves is an important part of IT security because of the cost to the organization. Also, more than just computers, IT is susceptible to loss of expensive equipment like laser printers, high quality scanners, projectors, large screen monitors and TVs all of which have high street value for criminals.

Many organizations are susceptible to theft and vandalism – especially educational institutions, health care organizations and small and medium sized businesses. In addition, many of these educational and health care institutions self-insure – which means that in the event of a theft there is no insurance company sending them a fat check to cover [part of] their loss. For these organizations, theft results in a total loss.

Let's examine the total cost of the theft of a computer:

- Cost of replacing the computer
    - If the equipment was insured then this is perhaps only the cost of the deductable.
    - If the organization self-insures then the full price of a new unit:
        - Typically cost $500-$1000 for a workstation
        - Typical cost $700-$3000 for a laptop
        - Typically cost $1000-$8000 for a server.
- Cost of missed productivity until a replacement unit is obtained.
- Cost of staff time spent ordering or purchasing the replacement.
- Cost of staff time spent configuring, integrating and commissioning the replacement
- Lost budget opportunity.
    - Computers and other electronic equipment are typically bought with capital expediture budgets. Institutions [like schools, colleges, libraries] that obtain their funding from governmental units and/or philanthropic organizations may not have an opportunity to return and request budget for the same item. We know of a school in a local district that spent several years wooing a foundation to fund a computer laboratory that ultimately opened with 25 new workstations; when the entire laboratory contents were stolen within months of the opening the opportunity for a computer laboratory disappeared – the school could not go back to the foundation or any other foundation for that matter and request the money a second time. For self-insurers, theft makes them two-time losers – they lose both the asset and the budget opportunity that was used to purchase that asset.

How, then, does an organization protect its IT assets? Again, the answer is with a layered approach where different items get secured in different ways.

In large organizations security is insured by means of restricted access enforced by security guards and individual ID cards with embedded electronic controls. Larger organizations will centralize their servers and network devices into data centers which again can be protected by means of security guards, locked doors, etc.

So the first layer, where possible and feasible, is to place the equipment behind locked doors and control and monitor access with security guards and/or electronic mechanisms.

Small organizations, public organizations such as schools, colleges and libraries, and quasi-public organizations such as health care facilities are less able to restrict access and employ security guards. Indeed, for schools, colleges and libraries, part of their charter is to provide computational facilities for their public to use. Small businesses especially office-oriented ones like accountants, lawyers, real estate, etc. are susceptible to small-time thievery; there was a case on the TV news a few months ago showing film from a security camera of a gentleman dressed like maintenance worker who quietly dropped printers and computers into his oversized Rubbermaid trash can at 3:00 in the afternoon!

Thus, for many organizations protecting their IT assets devolves into a requirement to secure each piece separately. LockDownIT LLC provides Lockdown Security Plates specifically to enable organizations to secure their individual pieces of IT equipment and to do so in a cost-effective manner without compromising the effectiveness of their ability to deter theft.

The efficacy of Lockdown plates in preventing theft is evident: In over 18 years of business, there has not been a single report of a theft where the thief was able to break the Lockdown plate in order to extract the protected equipment.

Each Lockdown plate is compromised of two, interlocking, pieces. In use a Lockdown plate is used to attach the protected IT equipment to a massive item or building structure. That is, the base portion of the Lockdown plate is attached to a desk, table, bookcase, floor, windowsill, wall, etc. and then the equipment is attached to the top piece of the Lockdown unit and the two pieces of the Lockdown then slide top into bottom and is secured with a lock. Lockdown plates allow equipment to be removed for servicing. Moreover, LockDownIT LLC plates feature 'NoMar' technology – the plates attach to furniture or structures with high-strength tape that provides upwards of 9 tons of holding power and without the need to drill holes or otherwise deface them; the glue used also allows for the Lockdown plate to be removed without leaving any residue or trace – truly no marring of the surfaces. And because Lockdown plates are removable, they are reusable and provide excellent value to the customers.

The Lockdown plates are available in a variety of sizes so that they can be readily matched to the size of the equipment being secured. Below are several examples of items secured with Lockdown Security Plates and also the Lockdown Security Cage which is bolted to the underside of a desk or table.

Lockdown security plates are a cost-effective means of securing high-value IT equipment. There are additional pieces of equipment such as inkjet printers and monitors whose cost does not justify a dedicated security plate. In these cases, LockDownIT provides a kit to be used in conjunction with the security plate; the kit is comprised of a cable and several 2" metal brackets; in use the brackets are glued to each of the smaller equipment and then the cable is passed through the equipment, attached to the Lockdown security plate and secured with a lock.

There still remains to be addressed the question of securing mobile computing equipment and especially laptop computers. According to FBI statistics, over one million laptops are stolen annually in the US alone. Laptops are readily stolen at airports, hotels, convention centers, restaurants and cars – places where users may momentarily forget them or be distracted from monitoring them every instant. However, many laptops are stolen from offices too. There is no good, single solution to preventing theft of a laptop computer. Some security solutions reduce the mobility of the laptop by adding on plates or other components. Many cable kits for securing laptops are sold. Security experts agree that cables can foil the opportunistic thief but that cables are easily defeated by a determined thief who comes armed with cutters. Typically the attachment point of a cable onto the laptop is the weak link in the security system – the attachment of the security cable to the laptop itself may be just on the plastic case or through a thin piece of aluminum. The 'butterfly' brackets that are sold to connect the laptop's security port to the cable can on many model be easily prized off. Finally, there is the need to consider how the opposite end of the cable is secured – is it looped through a table leg or other element that can be readily picked up to free the cable? Cables are not a great solution for securing laptop computers.

Another trend in securing assets is the recovery of stolen computers by means of special signals sent by the systems when they are attached to the internet. We believe that this approach has several significant problems:

- The asset is stolen; so this doesn't work to foil thieves and doesn't prevent the stealing of the computer. Also, it only works for network aware devices such as computers.
- The service provided is merely a notification to the owner that the device has been spotted on the Internet and an IP address provided; it is not always the case that the stolen devices would be connected to the internet without modification.
- It assumes that the IP address can be traced to a specific ISP and a node within the ISP; it may or may not provide a specific real world address and it will work only if the new operators of the computer don't spoof the IP address.
- Finally, the computer's owners will have to somehow get the computer back – either by getting police to track it down or by hiring their own private repossession guys. Again, there is either a cost for the repo guys or a problem getting the police to respond to recover thee computer.
- ***If the computer is recovered it should not be placed back in service***. It should be assumed that the thieves have inserted malware onto the operating system or even modified the BIOS to report back, for example, keystrokes, which would allow them to remotely enter the system and provide a 'Trojan horse' for attacking the organization. Any recovered computer should have its BIOS replaced and the hard drive totally cleaned or replaced and the Operating System completely rebuilt. This is an extra expense in using the recovered asset that should be recognized in the ROI.

A variant of this is the use of permanent asset tags whereby the owners information is affixed or etched onto the computer. Again, there are significant problems with tracking down the equipment, recovering and then the expense of re-commissioning the equipment.

Yet other trends in securing mobile equipment uses alarm devices on the equipment which emit loud sirens if the equipment is moved. Again, this seems on the surface to be a worthwhile solution but in practice they are not useful. They tend to create many false alarms, which, like the boy cried wolf, render them ineffective because people tend not to react to the alarms. It also assumes that good Samaritans upon hearing the alarm will intervene to stop the theft whereas in practice most people will be reluctant to become involved, especially if they think it's a false alarm. In addition, such devices rely on battery power which implies that the user monitors the battery levels to insure that the battery is functional at all times.

For all these problems, we believe that tracking and recovery is not a viable anti-theft strategy and that external alarms are not a useful anti-theft strategy. There is no guarantee that the equipment can be found, can be recovered and will be useful once it is recovered. We recommend instead that hard theft prevention devices be employed.

4. Where Do You Go From Here?

Total IT security requires protecting the data, protecting the processor and protecting the asset itself. Care must be taken with the data to insure that is not compromised as it is used around the organization and especially when it is used in mobile devices which are susceptible to theft because they cannot be physically secured. Protecting the processor requires anti-malware software packages coupled with strong, effective IT policies and procedures. IT assets are at risk for theft because of their high street value and opportunities for being stolen; protecting IT assets is best accomplished with individual, dedicated, strong security plates.

Each organization needs to construct their own total IT security system based on their systems and processes:

A. Protect the Processor
   1) Analyze the explicit and implicit trust relationships throughout the organization. The key question is: if somehow a piece of malware became introduced in this computer, would it spread to others? Which ones? Are we certain that no malware could become introduced to this unit?
   2) Analyze the topology of the organization's network. Which servers, desktops, laptops and other mobile devices are inside the organizational firewall and which ones are outside?
   3) Which ones need individual firewall, anti-virus and anti-malware protection and which ones can rely on organization-wide protection?
   4) Procure and install as required by your analysis:
      a. Firewall hardware and software
      b. Anti-virus
      c. Other malware sniffers like adware, scripts, cookies etc.
   5) Keep software and firmware up to date

B. Protect the Data
   a. Map the flow of data through the organization's processes and systems.
   b. Compare the data flow to the map of processor exposure developed in the previous analysis. When is the data protected behind the firewalls etc. and when is it exposed to the outside world?
   c. Institute encryption to protect the data on every hard drive in the organization.
   d. Institute backup policies to capture each piece of data as it is modified during a daily 24 hour cycle. Constantly test the backup data to maintain assurance of its integrity and the organization's ability to survive loss of data.
   e. Institute processes and procedures to remove/erase data from at-risk workstations, laptops and mobile devices the instant the data is no longer required.

C. Protect the Asset
   a. Identify which of the computers and other equipment can be safeguarded behind effectively locked doors [hollow core doors, flimsy doorjambs and bargain locksets don't qualify as safeguarded entries]. Insure that the doors, doorjambs and locksets are of sufficient quality to keep intruders out and insure that the doors are always locked.
   b. Identify which of the computers and other equipment may be at risk because they are placed in public areas, in quasi-public areas [like health care waiting rooms, public offices, etc.]. Also indentify which computers and equipment may be at risk because they are in offices that could be easily entered at night or on weekends; or may be stolen by maintenance workers or by thieves posing as maintenance workers.
   c. For those workstations and other valuable equipment which are at risk, purchase security plates, security cages or other high-quality security device. Beware of relying on cables; cables may be sufficient to deter the 'opportunistic' thief but they are easily compromised by a determined thief.

d. For laptops and other mobile computers, arrange for security plates within offices and other structures under your control. Since something is better than nothing, provide these devices with a locking cable security device for use outside of the office or home office and insure that the users of these devices have a proper regard for the risk of loss and consistently lock the units when they are outside of the office.

In summary, it is most important that every organization from the smallest [professional offices, retails stores] to largest [universities, health care, manufacturing, financial institutions, etc.] need to have policies, processes and systems in place to protect their IT infrastructure in a system-wide manner that protects the processors themselves, their data and their assets.