Given the realities of an increasingly mobile workforce and the growing regulatory obligations of organizations, IT security professionals need to craft, communicate, and enforce more specific laptop security policies to prevent company and customer data from being compromised. Laptop policies either don’t exist, and if they do, they’re not enforced. The lines of responsibility are often blurred between IT and Facilities/Security departments and conflict with effectively implementing existing policies. The weak link in the security chain, the end user, is left ill-trained to protect the vulnerable mobile computer. End users need more specific rules and training, IT staff should implement automated and non-automated enforcement practices, and management should lead by example, provide clear direction and highlight good behavior. Laptop security policy and regulatory compliance requirements need to be balanced with knowledge worker productivity targets in order to help the organization achieve both its security and bottom line goals.

THIS PAPER ADDRESSES THE FOLLOWING AREAS:

I. WHY A SEPARATE LAPTOP POLICY?
II. REGULATORY ENVIRONMENT
III. LAPTOP SECURITY POLICY OVERVIEW
IV. BALANCING PRODUCTIVITY AND SECURITY
V. LAPTOP SECURITY: WHO IS RESPONSIBLE?
VI. TRAINING
VII. MANAGEMENT ROLE
VIII. POLICY CONSIDERATIONS
IX. LAPTOP SECURITY POLICY CHECKLIST
X. REFERENCES AND LINKS
I. WHY HAVE A SEPARATE LAPTOP SECURITY POLICY?

Since the ChoicePoint case of 2005, the watershed data breach event where ID thieves compromised 163,000 accounts, hundreds more data breach cases have been reported resulting in over 150 million consumer records being compromised. Many of these were a direct result of lost or stolen computers and computer components. The trend continues in 2007 with over one third of the 119 reported data breaches in the first three months of the year a result of lost or stolen computers.¹ In such cases, organizations are left vulnerable to fines, customer loss from reputation damage, and costly remedies like consumer notification and credit report monitoring. ChoicePoint ended up paying ten million in civil penalties and five million in consumer redress. A study by the Ponemon Institute last year concluded that twenty percent of data breach victims cut ties with organizations that compromised their privacy. Much of the blame for computer theft can be attributed to the end user

It’s time for those responsible for IT physical security to reevaluate their policies in order to improve the way end users guard their mobile windows into the corporation’s data vaults.

II. INDUSTRY REGULATION TOUCHES NEARLY EVERY ORGANIZATION

The stakes have risen over the past decade and gone are the days when only a handful of industries operated under serious security regulation. Recent corporate governance scandals (Enron, Worldcom) have increased the spotlight on corporate ethical behavior and the handling of data. Governments and individuals are insisting on accountability from public and private corporations to control their data. With information access now ubiquitous, sensitive corporate and personal information needs to be protected more than ever. To prevent repeated scandals, protect the integrity of enterprise owned information, and ensure customer privacy, dozens of privacy laws pertinent to all types of companies have emerged and more are on the way. Some of today’s most prominent security mandates include:²

**Sarbanes Oxley** – the Sarbanes Oxley Act of 2002 requires strict internal controls and independent auditing of financial information as a proactive defense against fraud—with potentially serious civil and criminal penalties for non-compliance.

**HIPAA** – The Health Information Portability and Accountability Act of 1996 requires tight controls over handling of and access to medical information to protect patient privacy.

**GLB** – The Gramm-Leach Bliley Act of 1999 requires financial institutions to create, document, and continuously audit security procedures to protect the nonpublic personal information of their clients including precautions to prevent unauthorized electronic access.

**FISMA** – The federal information security management act requires federal agencies to develop, document and implement agency-
wide programs to secure data and information systems supporting agency operations and assets, including those managed by other agencies or contractors.

**PCI** – Although not a law, the PCI Data Security Standard was established by credit card companies to ensure the proper handling and protection of cardholder account and transaction information.

**California SB 1386** – Known as the Security Breach Information Act, this state law governs organizations that serve customers residing in California and store confidential data about those customers on computers, or transmit such data over networks. The law requires proactive protection of private data for Californians, and provides a model for electronic privacy legislation that has been enacted in 33 other states.

**IT Frameworks Provide Detailed Direction**

Corporations faced with multiple compliance requirements are addressing this enormously complex challenge by utilizing industry and government sanctioned standard practices. They have invested millions to adopt IT governance frameworks that cover a large percentage of regulatory mandates. Three of the most widely employed frameworks include:

**COBIT 4.0** – Published by the IT Governance Institute (ITGI), COBIT® 4.0 emphasizes regulatory compliance. It helps organizations to increase the value attained from IT and enables alignment with business goals and objectives. COBIT offers the advantage of being very detailed, which makes it readily adoptable across all levels of the organization.

**ISO 17799.2005 (ISO 27001)** – This is an international standard for the management of IT security that organizes controls into ten major sections, each covering a different topic. These are: business continuity planning, system development and maintenance, physical and environmental security, compliance, personal security, security organization, computer operations and management, asset control, and security policy.

**NIST 800-53** – This publication from the National Institute of Standards and Technology is a collection of “Recommended Security Controls for Federal Information Systems.” It describes security controls for use by organizations to protect their information systems, and recommends that they be employed with and as part of a well defined information security program.

**A Tree within the Forest**

Given all the heavy lifting being done at the macro level to help companies comply with regulations and standards, it’s not a stretch to see how a specific laptop security policy might get buried within a larger IS policy document. After a security score of “F” due in part to inadequate policies, one U.S. federal agency created 1,700 pages of policy documents.

**III. WHAT SHOULD A LAPTOP SECURITY POLICY ACCOMPLISH?**

Security policies are a means of standardizing security practices by having them codified (in writing) and agreed to by employees who read them and sign off on them.

When security practices are unwritten or informal, they may not be generally understood and practiced by all employees in the organization. Until all employees have read and signed off on the security policy, compliance of the policy cannot be enforced.
“What I see are policies that exist that no one ever pays attention to” said Mike Cantrell, an expert in computer forensics and data security at Secure Source, a risk consulting firm. “We’ll go into client’s offices and say ‘What are your policies? Do you even have a policy?’ Those that do may not review them often enough with employees...” he said.

“More companies are requiring employees to sign computer usage agreements that spell out how workers will use their laptop and the information on it” said Ms. Berman of CBIZ, a national business services and consulting company. “The usage agreement should cover everything from hardware to the software. It should include use of Internet technology to anything that could otherwise compromise the computer itself like viruses and physical security”. “Employers should also reinforce that employees are to “guard that laptop like it’s your own wallet. It shouldn’t be any less than that” Ms Berman said.

Mike Mullins, security author for TechTarget, says “Many companies make the mistake of looking at the multitude of regulations and trying to decide: Are we compliant? But that’s not the right question. What companies should be asking is: Are our policies compliant, and do we follow our policies?” Mullins argues that technology changes too fast to base policies on specific solutions. “For example, don’t say “We must secure files containing customer information using file security and encryption. Instead, create a policy that states: “We must secure customer information so that only authorized individuals can view or modify it.” How you carry out the umbrella policy statement is then defined according to the standards and practices that work for your organization. The key for end user compliance is to put policy and practices into language they will understand, and enact programs that make adhering to these practices second nature.

This may sound rudimentary, but imagine driving your car and not knowing the rules of the road. Disaster will surely ensue. The same applies to a laptop policy. Your organization might have one, but if it isn’t presented as a serious set of rules to be observed, with consequences if ignored, how seriously will it be taken? Will the company have to incur a security incident for the policy to get teeth? The policy itself should also be under scrutiny by IT staff to ensure it stays a relevant, living document that accurately reflects how the organization protects IT assets.

IV. STRIKING A BALANCE BETWEEN WORKER PRODUCTIVITY AND SECURITY

Some IT managers suggest limiting sensitive data to only desktop computers, and not letting such data off the premises. Others suggest issuing laptops to just those employees who absolutely need one because they work remotely, travel, or work in teams in company conference rooms. Welcome to the 21st century folks. Most workers want the flexibility of a laptop to enable them to, among other things:

- Work offsite when there’s a work crunch demanding night and weekend hours
- Share information with distant business partners
- Keep up to date with business transactions

What employer wants to stand in the way of more productivity? Besides, who wants company data residing on home computers that are even more out of the IT departments control and susceptible to viruses and theft? There are plenty of ways to protect company equipment and data that won’t limit worker productivity.
V. LAPTOP SECURITY: WHO IS RESPONSIBLE?

When a security breach such as a computer theft occurs, whether in the office or in the field, someone needs to be accountable so the process can be managed and the risk of a repeat event mitigated. Certainly the end user has primary responsibility once the machine leaves the premises. What about in the office? “It’s always somebody else’s fault when there’s a break-in in the building,” says Steve Stasiukonis, VP and founder of Secure Network Technologies. IT security blames facilities security and vice versa. In many organizations, physical security is often focused more on protecting copiers, printers, and fax machines from theft—not servers or computer equipment” Stasiukonis says.7

A laptop policy should incorporate the respective roles that facility/security managers, IT managers, supervisors, and employees play in protecting mobile computers.

For example, who enforces the use of a cable lock in the office? Who checks to see if users log off their computer when not at their desk? Who trains users on how to develop complex passwords? Answer: It doesn’t matter as long as someone is assigned the responsibility.

Out of the office, the end user is responsible for the physical security of the laptop. Together with whatever security software is installed on the computer, the safe return of the machine with its vital customer and company data is now at the mercy of the end users common sense, street savvy, and training. Since the company can only impact one of these three, the role of training to protect computers becomes critical.

VI. THE ROLE OF TRAINING

Regular security awareness training is especially critical for the mobile laptop users. Hosted security tools and the physical security of the workplace can no longer be relied upon. Some of the worst security problems originate from the things end users do, from the seemingly obvious no-no of opening attachments from strangers, to connecting to the closest WiFi connection while on the road. Pretend your employees don’t know anything about securing the company’s information and train them to meet security policy standards.6 The key to a good training program is identifying your audience and the level of training they need to do their jobs. End users and technical staff each require different types of training goals, so be sure to fashion it properly for each group. According to Brian Joyce, IT director at CPA firm Joseph Decosimo and Co. “We are increasingly finding that, regardless of the amount of money we spend on security technology, an educated end user community is a first and critical line of defense.”8 A common, and often mandated security training regimen for industries like healthcare, includes reviewing policies at new employee orientation, and regular awareness training every 6 to 12 months. Todd Fitzgerald, systems security officer for United Government Services suggests other tactics. “Security awareness training needs to be more in your face and real, with things like posters, computer based training, compliance tracking, and face-to-face interactive training.”

“The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won’t suffice. Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully.”

Kevin Mitnick, Founder Mitnick Security Consulting, LLC Convicted Computer Hacker
VII. MANAGEMENT’S ROLE IN LAPTOP POLICY

Just like parents, manager’s make more of a statement by what they do then by what they say. The policy will have the best chance of being observed if everyone from the CEO on down is held to the same standards. Indeed, CEO’s often pose a greater security risk than most employees due to the sensitivity of the data they carry and the level of permissions they own. For example, Irwin Jacobs, CEO of Qualcomm had his laptop stolen from his podium during a speech while standing 30 feet away. Since the boss will be held accountable to the board in the event of a data breach, all the more reason to get him/her involved in formulating, approving, and communicating the policy. By adopting a multi layered approach to policy, you can add layers of security to where they are most needed. One approach is to identify security levels and add security tool features as the sensitivity of the computer’s data increases. See figure 1.

VIII. LAPTOP SECURITY POLICY CONSIDERATIONS

‘One size fits all’ policies aren’t adequate. Each organization needs to take into account their unique operating environment to arrive at a useful and effective policy. Considerations include: legal/regulatory, contractual, third party, company philosophy, and industry accepted best practices. Other considerations include the work environment: mobility of the workforce, flexible workplace (home/office), rental cars, hotels, airports, conferences, tradeshows, inter-company office travel, and if personal machines are employed for company business. These elements will dictate the level of detail in the policies you create. The following best practices are derived from over 20 published policies from a variety of organizations: Fortune 500 businesses, universities, military, healthcare, and IT and security professionals from various articles and email user groups. Common elements of these sources were gathered and are presented below.

MULTI-TIERED LAPTOP SECURITY MODEL

<table>
<thead>
<tr>
<th>LEVEL 1</th>
<th>LEVEL 2</th>
<th>LEVEL 3</th>
<th>HIGH / CRITICAL</th>
<th>RESTRICTED INFORMATION</th>
<th>MODERATE /HIGH</th>
<th>CONFIDENTIAL DATA</th>
<th>INTERNAL INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASIC SECURITY</td>
<td>MEDIUM SECURITY</td>
<td>HIGH SECURITY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cable Lock</td>
<td>Full Disk Encryption</td>
<td>Tracking Software</td>
<td>Strategic plans</td>
<td>Employee Handbook</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disabled Admin log on</td>
<td>Offline Storage Options</td>
<td>Disk Swipe Software</td>
<td>Online Access Codes</td>
<td>Telephone Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong Passwords</td>
<td>Insurance</td>
<td>Biometrics</td>
<td>Encryption Keys</td>
<td>Org Charts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset tags</td>
<td>Disable unnecessary ports</td>
<td></td>
<td>Credit Card Listings</td>
<td>Policies and Standards</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

LOW SENSITIVITY

HIGH SENSITIVITY

fig. 1
IX. LAPTOP SECURITY
POLICY BEST PRACTICES
CHECKLIST

1. Basic Physical Security
   ▶ Have users read and sign an acceptable use policy describing precisely what is and isn’t acceptable on the company machine
   ▶ Lock down laptops with a cable lock wherever you are: office, home, airport, tradeshows, or hotel rooms. If an immovable anchor isn’t available, loop the security cable around a chair, or other hard to move object. Keep a spare key apart from the one on your keychain. If a resettable combination lock is used, change the combination whenever you suspect someone has observed you opening it. Register the key or combination on the lock manufacturer’s website in case you lose it. If you’re responsible for computers in a facility, use a master key or master coded combo system to manage lost key/combo issues.
   ▶ Lock away PCMCIA/NIC cards if computer is left unattended on the desktop
   ▶ Register computer serial #/model # with manufacturer, and store information separately. This will help recovery if the computer is turned in for service
   ▶ If leaving a machine unattended, log out or turn machine off
   ▶ Apply a tamper resistant Asset tag or engrave the machine to aid authorities in recovery. These could also prevent the resale of the machine.
   ▶ Use of a non-descript carry case. Place the laptop in a padded sleeve inside a backpack for example.
   ▶ While traveling, never leave a laptop unattended in a public place
   ▶ When leaving a laptop in the car, lock the computer in the trunk using a cable lock to secure it to a permanent vehicle mount.
   ▶ Consider Biometrics as an alternative to passwords. Fingerprint, retina, and face scan technology can speed up access to the computer.
   ▶ Consider Recovery software that allows computer to “phone home” in case of loss or theft
   ▶ If a laptop is lost or stolen, report it immediately. Time is of the essence to keep thieves from intruding on the company network.

2. Operating System Security
   ▶ Use the latest operating system affordable as new security measures are being added all the time. Enable auto updates from the company network and the Internet when not at the office.
   ▶ Lock or disable all unnecessary ports to limit access. USB ports are especially vulnerable to data leakage and unauthorized data transfer.
   ▶ Enable BIOS passwords for added password protection. Determine if the BIOS (Basic Input/Output System) password locks the hard drive so it can’t be installed and accessed in a similar machine.
   ▶ Disable boot-up capabilities of other drives. Disabling the secondary boot drive sequence hinders the ability to access the system from a secondary drive.
   ▶ Rename the Administrator Account. Attempting to hack local accounts is a common method. When renaming, don’t use the word “Admin” in its name.
   ▶ Prevent the last user name from displaying in the login dialog box
   ▶ Disable the Infrared port on the machine. Hackers can read the contents of your machine from across the room without you knowing it!
   ▶ Ensure only one active connected interface is enabled at a time. For example, if WiFi is enabled, then other access methods are disabled. This ensures that devices cannot be accidentally or intentionally used as bridging or routing devices between two or more networks.
   ▶ Do not let users download third party software and applications or enable unauthorized protocols or services (much as they will want to).

3. Network Security
   ▶ Install and regularly update an Antivirus product. Enable real time protection by default.
   ▶ Install host-based Adware and Spyware utilities
   ▶ Install a host-based firewall to deter intruders and malicious logic from entering the system.
Enable all auditing available on the computer necessary to support the network environment.

Install VPN technologies to access to the organization LAN. The VPN should protect and encrypt at Layer 2, data-link layer.

Use client Patching management software to receive the latest fixes to OS and software.

Enable encrypted protections on connections from untrusted to trusted network connections.

4. Secure Connectivity

Ensure that Antivirus and Firewall software is installed, enabled, and receives regular updates.

For VPN connectivity, disable split tunneling for all internet access. Not doing so renders the VPN vulnerable to attack.

5. Protecting the Data

Have in place a password policy that requires users to create complex passwords between 8-14 characters. Passwords should use at least 3 of the 4 complexity requirements: uppercase letters, lowercase letters, numbers, and non alphanumeric characters. Don’t write passwords down, and don’t share them with others. See this article for how to create and remember complex passwords: http://articles.techrepublic.com.com/5102-1009-6028857.html

Back up and synchronize your files on a regular basis

Consider using offline storage products when traveling. USB drives, RW CD’s, or external hard drives provide a good back up should your laptop be unavailable.

Use privacy screens when using your laptop in public places such as airports or hotel lobby’s.

Use system encryption tools such as EFS (Encrypting File System) on Windows XP for encrypting individual files and folders. MAC OS X users can use FileVault

For the most complete protection of data on the computer, install whole disk encryption.

For machines with sensitive data, consider installing Disk Wipe technology that wipes the hard drive clean in the event of loss or theft.

6. Security Awareness Training

Raise security awareness-put up posters, put policies on the company Intranet. Establish regular communications in company newsletters and emails about the latest threats and incidents that could affect your end user community.

Review your policies at new employee orientation, and with regular awareness training every 6 to 12 months

Conduct security training classes between 45 to 60 minutes in length and cover topics such as email, web surfing, physical security, and procedures to follow while traveling.

Keep employees alert by doing occasional compliance spot checks and pop quizzes at staff meetings. Don’t rely solely on your automated systems.

Give travelers a pre-trip checklist on key security procedures to follow to reinforce training.
CONCLUSION

If you have a laptop policy, make sure your workforce reads and signs off on it. If you don’t have one, write one. Anything is better than nothing. Links to a few examples are included at the end of this paper. Don’t wait until you have a breach to put policies to work. Raise security awareness in your organization. Schedule yourself in the new employee orientation trainings and conduct periodic refresher courses. Ensure IT and Facilities/Security is on the same page when it comes to training and compliance. If you think you have everything covered and you have the budget, check your vulnerability by hiring a third party to conduct a security audit or do intrusion testing.

A final thought from Eric Maiwald, senior analyst at Midvale, Utah-based Burton Group. He said “the only way to completely eliminate the risk of data being stolen from a laptop is to lock that data down and forbid it from ever leaving the company. However, for business to occur, data must be accessible. Probably the most important step is to have authentication and encryption technology on mobile computers. In reality”, he continued, “encryption will only slow the sophisticated thief from accessing data on a stolen laptop.

It may seem obvious, but the best way to protect the data on a laptop is to prevent it from being stolen in the first place.

Plus, companies must have good policies about protecting data and using laptops. More importantly, they must enforce that policy.”11

Laptop Security:
As Strong as the Weakest Link

LAPTOP LOCK
BEWARE OF WIFI
DONT’ LEAVE LAPTOP UNATTENDED

COMPLEX PASSWORDS
LOCAL FIREWALL

AUTHENTICATION
ENCRYPTION
INCIDENT RESPONSE
SECURITY AWARENESS TRAINING

ANTIVIRUS SOFTWARE
OS UPDATES

PREVENT UNAUTHORIZED SOFTWARE DOWNLOADS
ORGANIZATION SPECIFIC CONSIDERATIONS
REFERENCES
2 Operationalizing Security & Policy compliance. A unified approach for IT, Audit, and operation teams, Qualys
4 Conducting a Security Audit: An Introductory Overview, Bill Hayes May 2003
5 “Firms ready to put leash on laptops” Dallas Morning News, July 2006
6 Take technology out of your security policies to maintain compliance, Mike Mullins, TechRepublic, April 2007
7 Dark Reading, The 10 most overlooked aspects of security, Nov. 29, 2006
8 By addressing data privacy, companies avoid public scrutiny, SearchSecurity.com, Craig Norris and Tom Cadle, March 28, 2007
10 SecurityFocus.com, Laptop Security Part one, preventing laptop theft, Josh Ryder, July 2001
11 SearchCIO.com, Fidelity laptop snafu spotlights need for security policies, Shamus McGillicuddy, March 28, 2006

EXAMPLES OF LAPTOP POLICY DOCUMENTS / ARTICLES
- http://labmice.techtarget.com/articles/laptopsecurity.htm
- http://security.berkeley.edu/MinStmts/Physical.html
- http://www3.georgetown.edu/security/10574.html
- http://www.asu.edu/it/security/s101/

IT SECURITY POSTER LINKS
- http://www.us-cert.gov/reading_room/distributable.html
- http://security.arizona.edu/index.php?id=780

ABOUT THE AUTHOR
Jason Roberts is the marketing manager for PC Guardian, a manufacturer of computer and data security systems. In his 19 years in management, Roberts has held director positions in field marketing, training, and operations. He holds a BS in Business Administration from Fresno State University.

ABOUT PC GUARDIAN
PC Guardian is a leading designer and manufacturer of computer security solutions for corporations, educational institutions, and government agencies. Protecting computer assets with patented, award winning products since 1984, PC Guardian successfully serves organizations, including many Fortune 1000 companies, by solving their security needs and ensuring compliance through innovative products, quality, integrity and commitment to exceptional service and results. For more information, product availability and distribution, please visit us at www.pcguardian.com.