ASIS FOUNDATION

ASIS FOUNDATION™

CRISP REPORT

Connecting Research in Security to Practice

Lost Laptops = Lost Data

Measuring Costs, Managing Threats

by Glen Kitteringham, CPP

ABOUT THE CRISP SERIES OF REPORTS

Connecting Research in Security to Practice (CRISP) reports provide insights into how different types of security issues can be tackled effectively. Drawing on research and evidence from around the world, each report summarizes the prevailing knowledge about a specific aspect of security, and then recommends proven approaches to counter the threat. Connecting scientific research with existing security actions helps form good practices.

This series invites experts in specialist aspects of security to present their views on how to understand and tackle a security problem, using the best research evidence available.

Reports are written to appeal to security practitioners in different types of organizations and at different levels. Readers will inevitably adapt what is presented to meet their own requirements. They will also consider how they can integrate the recommended actions with existing or planned programs in their organizations.

In this CRISP report, Glen Kitteringham, CPP, analyzes strategies to protect laptops—and data—at the office, on the road, or at home. Practical checklists and classification schemes help the reader determine adequate levels of data protection. Replacing stolen units is just the start: lost productivity, damaged credibility, frayed customer relations, and heavy legal consequences can cripple both public and private sector organizations.

CRISP reports are based on the Problem Oriented Policing (POP) Guides produced by the Office of Community Oriented Policing Services (COPS) of the U.S. Department of Justice, which can be accessed at www.cops.usdoj.gov. While that series summarizes knowledge about how police can reduce the harm caused by specific crime and disorder problems, the CRISP series focuses on specific problems facing security professionals.

Martin Gill
Chair, Research Council
ASIS International Foundation

ISBN-13: 978-1-887056-85-4

CRISP REPORT

Connecting Research in Security to Practice

An ASIS International Foundation Research Council CRISP Report

Lost Laptops = Lost Data

Measuring Costs, Managing Threats

Glen Kitteringham, CPP

ASIS International Foundation, Inc. : Alexandria, VA

Contents

Executive Summary

Laptop computers are essential for organizations to make sure their employees have access to information they need wherever they are working…at home, in a meeting, or on the road.

A lost laptop creates a two-dimensional problem. First, the laptop itself must be recovered or replaced. Second, and even more unsettling, is the prospect that critical information on the company, its plans, and its customers could have been lost as well.

This report looks at both types of losses, from a statistical and cost point of view. It also examines the internal and external factors that contribute to laptop theft. Who steals laptops? What motivates their actions? Why are companies targeted repeatedly?

Based on an extensive review of published research, the report explores the scope of the problem. A range of detailed solutions is offered. In a sample of worldwide jurisdictions, current legislative efforts impose new sanctions. Several product innovations may help to prevent thefts. Disrupting the ways thieves can unload their bounty is another deterrent. The appendices include exhaustive lists of physical, electronic, and procedural security enhancement, so organizations have specific ways to discourage or prevent thefts.

The report encourages companies to set goals to counter laptop theft and then implement those goals through situational prevention techniques and the seven steps of loss prevention.

Additional research could aid in preventing the theft of laptops and the data that resides on them. The report concludes with suggestions for further exploration by academic and corporate investigators.

Lost Laptops = Lost Data

Laptop computers are essential tools in today's global economy. Employees at all levels, in all business sectors, must be mobile. They must have access to information whether they are at home, on a sales call, or in a hotel.

Because laptops are portable, they are highly susceptible to theft. The theft of business laptops and the loss of the confidential and propriety information residing on them can occur when the user is in the office or on the road. Researchers at Credant Technologies have determined that 25% of laptops are stolen from the office or the owner's car. Another 14% are lost in airports or on airplanes.

Laptop theft is a two-dimensional problem. On the surface, companies must devise ways to secure the actual devices from crafty thieves with easy access to pawnshops and fences. Even more sinister, the data on a stolen laptop has enormous value among the illicit networks that prey on unsuspecting consumers, or reap rewards from insider information.

In their attempts to stay competitive in the world marketplace, companies cannot afford to overlook the seemingly insignificant loss of a laptop. Details on the scope of the problem, the high price of ignorance, and the determined thieves looking for loopholes will convince even the most ardent skeptic to take the actions recommended in this report.

Researchers at Credant Technologies have determined that 25% of laptops are stolen from the office or the owner's car. Another 14% are lost in airports or on airplanes.

Statistics on Stolen Laptops and Lost Data

Since the mid 1990s, private sector and government researchers as well as the media have tracked not only the growth of the laptop market but also frequent losses. At the same time, law enforcement and security professionals quickly realized that laptop theft was a swift portal to even more valuable confidential information. Researchers began to amass alarming statistics on the scope of both problems.

Stolen laptops

The chance that a laptop will be stolen or lost during any twelve months is one in ten, according to a 2002 Gartner Group study. Estimates among industry analysts confirm the frequency with which laptops disappear. A 2004 *InfoWorld* article, for example, estimated that the annual number of stolen laptops ranges from 700,000 to 1 million. That same year, an *Entrepreneur* Magazine article used an FBI estimate to report that 1.5 million laptops had been stolen in 2004, a 50% increase from the year before.

Both public and private sector organizations are at risk worldwide. In a 2006 report, the Committee on Government Reform noted that in the previous five years 1,137 U.S. Department of Commerce laptops had been lost, stolen, or reported missing. A 2006 Australian Computer Emergency Response Team survey of 17 industries found that 58% of the 389 respondents detected laptop thefts during the year of the survey.

Between 2005 and 2007, 4,700 laptops were stolen from offices in Calgary, Canada, according to a 2007 survey by the Calgary Public Safety Committee of the Building Owners and Managers Association (BOMA). Medical, financial, oil and gas, legal, engineering, transportation, personnel, and property management industries were included in the study. Appendix A is a checklist that can be used to track a company's laptop inventory and monitor how the laptops are being used.

In a sobering note, Credant Technologies found that 82% of stolen or lost laptops are never recovered. Other estimates are even more pessimistic. According to the FBI, for example, 97% of stolen laptops are never recovered.

Stolen confidential information

Statistics that measure the loss of business and personal information residing on laptops are even more alarming. A 2006 Ponemon Institute survey found that 81% of the U.S. companies studied reported the loss of one or more laptops containing sensitive information in a twelve-month period. The computer security Web site, www.attrition.org, includes an extensive list of laptop and data thefts. In early 2008, the site reported more than 900 data breaches yielding 310 million records.

As stated by Credant Technologies researchers, "most users are in denial about the severity of the information stored on their laptops" and are unaware of the real risk involved in losing a laptop, which is "exposed corporate information and customer data."

Authors of the Ponemon Institute's 2006 U.S. Survey on Confidential Data at Risk concluded "both business and government organizations are not taking appropriate steps to safeguard sensitive or confidential information such as intellectual property, business confidential documents, customer data, and employee records."

The Committee on Government Reform reviewed data breaches among 19 U.S. government agencies and observed "data loss is a government-wide occurrence." The committee concluded that the agencies do not always know what has been lost and that physical security of data is essential.

As a first step, then, companies must be aware of the important information that is available through laptops. Not all information needs the same level of security. Appendix B shows a classification scheme for company information that executives can use to determine adequate levels of data protection. Similar approaches can be found by searching the Internet under "classification of data." Once managers have classified the types of data they control, they can then determine what should or should not reside on a laptop—knowing that putting data on a laptop increases the likelihood that it could be lost.

Appendix C shows a threat and risk matrix model that can help organizations determine the types of information that hold value to the company and the likelihood that it could be lost. By working through the model, management can rate the high, medium, or low probability and criticality of an event. Answers can then be charted on the matrix.

For example, assume that a company's management determines that its classified secret formula gives it a competitive advantage. Losing it would cause the company to lose market share, incur significant financial losses, and suffer a stock price reduction. So the company rates its secret formula as highly critical. Management also decides, based on available data, that it is highly likely the company will lose the data if it's on a laptop.

Armed with that information, management must determine whether the information either does or should reside on a laptop. If the data is available on a laptop, management must allocate the appropriate levels of security to that unit.

Measuring the Cost

For years, many international groups have studied the costs associated with laptop theft and data loss. In 2004, for example, Safeware Insurance found that all laptop thefts in that year caused an estimated $720 million in hardware losses, but $5.4 billion in the loss of proprietary information.

Many studies focused on just one aspect of the monetary loss to businesses. Consider the following statistics that deal specifically with the cost of laptop thefts:

1. Authors Whitehead and Grey calculated that the cost of laptop theft between 1996 and 1997 was £2,616 ($5,021) per incident.

2. In 2000, researchers in the United Kingdom found the cost per laptop theft exceeded £60,000 ($115,158).

3. New Zealand researchers reported in 2005 that the average laptop loss cost $14,000.

4. A 2007 annual survey conducted jointly by the Computer Security Institute and the FBI found laptop losses averaged $345,000 per incident.

5. According to a 2008 article in *Infoworld*, the cost of stolen laptops to businesses ranges from $700,000 to $1 million annually.

The following studies report the costs of data losses only:

1. According to the 2003 Brigadoon Software (BSI) Computer Theft Survey, proprietary data losses averaged $690,760 per incident. The survey involved 676 participants from around the world.

2. In 2006, the Ponemon Institute estimated data breach losses at $4.8 million per incident. In 35% of those incidents, a "lost laptop or other device" was listed as the breach source.

Calculating the costs associated with laptop and data losses includes many factors. A major issue is lost productivity, since the affected employees can be prevented from performing their normal duties for weeks. Other factors include replacing or repairing damaged property, purchasing new hardware, and recreating data.

Lost productivity

Productivity is the first victim of a stolen laptop. Should an employee lose his or her laptop, that employee's ability to work is compromised, often for days. At one company, for example, eight laptops used by key employees were stolen, including those in the firm's finance and engineering departments. It took three days for replacement units and back-up data discs to be found before the business could resume operations.

Credent Technologies found that, in 50% of the organizations participating in a 2005 survey, employees who had lost laptops were unproductive for two weeks before they were able to resume regular activities.

Productivity can also be compromised if employees feel insecure in the workplace. After laptops were stolen in one large organization, employees altered their work patterns for several weeks, fearing that they might encounter another theft in progress. To alleviate employees' concerns, additional security personnel were hired. Even more unbudgeted costs were added to the recovery effort.

Damaged property

In their attempts to gain access to laptops, thieves may kick in walls, destroy doors, peel door frames, attack locking hardware, snap astragals and latch guards, remove ceiling tiles, and smash windows. Repairing or replacing these items costs money and time.

Replacing laptops

According to the BOMA study, of the roughly 4,700 laptops stolen from downtown Calgary, Canada, from 2005 through 2007, fewer than 20 were actually recovered.

In most cases, stolen laptops must be replaced. The complexity and unique qualities of the machine, as well as specialized software for unique applications, must be considered when searching for replacements. These factors further delay the return to normalcy and add to costs.

Recreating data

Depending on a company's data back-up practices and its use of a central server for data storage, data may be replaced in a few minutes—or be lost forever. In developing adequate data replacement and recreation strategies, company executives must resolve many questions, such as what procedures must be developed to ensure that important data is secured, as well as how quickly it can be replaced or retrieved, and at what cost.

Added Costs of a Data Breach

Should a company lose data that includes personal information on customers, the cost of that breach escalates. Additional costs may include notifying customers, monitoring credit, paying fines and penalties, and accumulating legal and investigative fees.

Two other important factors are the potential loss of customer loyalty and the prospect of a dip in the value of the company's stock.

Customer notifications

Laws in many jurisdictions mandate that companies notify customers when personal data is compromised. Companies, therefore, immediately incur the cost of preparing and disseminating letters and e-mails, adding notifications to web sites and media campaigns, and monitoring call center inquiries. Costs escalate quickly when thousands and even millions of customers are affected.

Credit monitoring

After a laptop from the U. S. Department of Veterans Affairs (VA) was found to be missing, potentially affecting 26.5 million constituents, the department pledged to monitor the credit rating of victims for one year. The VA estimated the cost of the monitoring could exceed $160 million.

After the laptop was recovered and investigators determined that it was highly unlikely that the data had been accessed illegally, the department rescinded its offer. But the potential for incurring a similar cost is a scenario every company must consider.

Liability

Should investigators, legislators, or lawyers determine that a laptop theft and resulting data loss is a result of an organization's insufficient security practices, that organization may find itself liable for fines and penalties levied by government agencies or the courts. In the VA case, at least three class action lawsuits were launched in 2006.

In addition to the potential for huge payments to victims, the company incurs the cost of launching a defense. Investigating the extent of lost data may include examining forensics, interviewing and interrogating potential perpetrators, and preparing briefs for law enforcement. Employees from the specific business unit that incurred the data loss will certainly invest time, taking them away from their regular duties. But a variety of departments may become involved as well, including legal, public relations, IT, and security, which will affect overall business operations.

The potential for employees to be injured during the commission of a laptop theft cannot be ignored. In an interview with a known laptop thief in Calgary, the thief revealed that employees had unknowingly confronted him during the actual crime in numerous cases. Since laptop thieves often carry tools to assist them in gaining entry to a premises or vehicle, employees who encounter a thief can quickly become victims. The legal consequences of such actions can be severe if the injured worker levies charges of "inadequate workplace security".

Lost business

When customers learn of a data breach, their faith in the company incurring the loss can be shaken. They may shift their business to competitors. According to the 2007 Ponemon survey, data breaches exposing customer data can cost a company $128 in lost business, per victim. In a similar Ponemon study conducted in 2005, researchers found data breaches seriously affected corporate reputation, corporate brand, and customer retention. When notified of a breach, almost 20% of customers terminated their relationship with the company. Another 40% considered termination.

Competitors can easily use any lost data incident to their advantage. Just underscoring the lack of security that lead to the breach may be enough to drive customers to their doors. If competitors are the recipients of the purloined information, they can adjust their own timelines and marketing strategies to gain an unfair advantage in the marketplace.

Shareholder value

If the theft and subsequent data breach is significant, an organization may suffer a reduction in shareholder value. Recouping lost market share or stock value can take years, and can permanently damage a company's relationship with creditors, suppliers, unions, and partners.

Internal Factors Contributing to Stolen Laptops and Lost Data

Why are laptops easy targets for gaining access to data? The answer involves a combination of misperceptions on the part of the company and the users of the laptops. Some companies simply fail to maintain an adequate inventory of their laptops, while others completely refuse to invest in appropriate security policies and procedures.

Users often fail to understand the value—not only of the units themselves—but also of the information they contain. Consequently, they can resist applying appropriate security policies and procedures when they are enacted.

Accountability

A 2004 survey by Ernst & Young found that few organizations and individuals feel they should be held accountable for failing to protect laptops and data. In many organizations, when a laptop is stolen, the affected employee simply acquires another from inventory. Even some security practitioners hesitate to emphasize laptop theft. One corporate security professional admitted that he had more global issues to confront than the theft of a laptop.

Current privacy and data breach laws promote enforced accountability. Organizations now must take more responsibility to protect laptops and data, or face legal consequences. Simply put, many organizations are implementing protective measures for laptops because they have been forced to do so by law.

Inadequate security

When finally caught, one Calgary laptop thief responsible for hundreds of thefts over several years admitted to the arresting officers, "companies made it too easy for these types of crimes to be committed, because of the lack of appropriate security measures." Even when adequate security measures are in place, they are often ignored for two reasons: the security staff is not available, not credible, or unable to sell the value of protective strategies; or employees are uninterested or have been poorly trained.

Perception

The relatively low price of laptops can suggest that they do not merit protection. Even though many organizations spend thousands of dollars on individual laptops, they are often viewed as a minor part of a departmental or organizational budget. Organizations that embrace this thinking fail to understand the true cost of a laptop, or the value of the data residing on it. Even privacy legislation assigns a value to data by assessing fines for losing it.

External Factors Contributing to Stolen Laptops and Lost Data

Even a well-designed security program must be tweaked constantly to keep ahead of external factors that are determined to uncover its weaknesses. The market for a company's proprietary information and personal data on customers and clients is lucrative. Determined thieves are more than willing to take the risks to reap the rewards.

Once thieves have been successful at one property, research shows that they are likely to return.

Determined thieves

According to the 2003 BSI Computer Theft Survey, 99% of survey respondents who experienced computer theft reported that the thief was never caught. Some thieves are simply opportunistic and take advantage of situations to steal laptops. In interviews conducted for the 2007 BOMA survey, one thief admitted that he made between $500 and $600 per unit, and had stolen as many as fifteen laptops at a time. At the other end of the spectrum, thieves admitted they sold laptops for as little as $40 of crack cocaine.

Thieves intent on stealing laptops will put tremendous effort into overcoming significant security measures. They will conduct security assessments to look for weak entry points. They will bring props, such as maintenance, janitorial, or security uniforms, so they appear to fit in. They will make phony identification badges, develop cover stories, and communicate with partners using cell phones and radios. One offender indicated that he would conduct research on the latest equipment and develop "want lists" before orchestrating a hit.

Organizations are vulnerable to laptop thefts from both outsiders and employees. Research is contradictory about which poses a greater threat. But there is no doubt that those inside organizations are also stealing laptops. Authors Clarke and Eck posit that laptops are "CRAVED" by thieves. The acronym explains why.

- **Concealable:** Because they are small, laptops are easy to hide beneath a jacket, layer between other items, place in a backpack, or put in a gym bag.
- **Removable:** The portability of the device is partially what makes the laptop desirable to both companies and individuals.
- **Available:** Many individuals and companies use laptops extensively. As a result, considerable numbers are available to be stolen.
- **Valuable:** Many people are willing to pay large enough sums of money for stolen laptops. Thieves tapping into this lucrative market are willing to go to extremes to satisfy the demand.
- **Enjoyable:** As computers become more essential for both business and pleasure, the demand continues to grow.
- **Disposable:** An illegal market is readily available, allowing thieves to dispose of laptops easily.

Managing the Threat

Repeat victimization

Experienced thieves realize that companies usually replace stolen laptops with new equipment, so they come back. They may even return to steal what they missed the first time.

The Calgary Public Safety Committee survey found that when a laptop theft had occurred, almost all commercial properties were victimized a second time (93%). Nearly two-thirds of the companies reported a second loss (60%). Whitehead and Grey found that 25% of commercial properties were victimized again within 30 days. According to the 2003 BSI Computer Theft Survey, 57% of respondents reported multiple incidents of theft in a twelve-month period.

Farrell and Pease identified two general themes in their study of repeat victimization: crime prevention measures need to be implemented quickly once a company is victimized; and temporary prevention measures are an effective and efficient means of preventing further crime during the high-risk period after victimization.

As identified in Appendix D, a laptop thief must take seven specific actions to be successful. They include identifying likely targets through pre-theft surveillance, defeating all security measures to gain items, leaving successfully with the items, and converting items to something of usable value. Appendix E identifies situational prevention techniques that can be used to counter the seven steps: increasing the effort and risk, reducing the rewards and incentives, and implementing impediments.

Ultimately, preventing laptop thefts and the resulting data loss requires a permanent solution. Countering the threat requires company management to commit to a course of action prescribed by basic security principles. These principles are used by corporations of all types, in all corners of the world, to prevent and deter myriad risks to a company's well-being. Bringing these same principles to bear on this specific crime can reduce the threat from both internal and external sources.

Implementing these principles requires a review of the many resources and options available, including: physical, electronic, and procedural security enhancements; legislation; and product design.

In conjunction with law enforcement, preventive measures should also disrupt the market for the stolen goods.

Legislative recourse

The loss of a laptop with confidential information is a privacy violation, which in turn can lead to civil liability. Many jurisdictions require businesses to report data breaches. As of December 2007, thirty-seven U. S. states have passed data breach legislation. In California, for example, the 2003 Security Breach Information Act states:

"Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

In a recent article in *Canadian Security*, Neil Sutton noted that a Canadian parliamentary committee recommended that "the law be updated to include a new requirement for corporations to notify individuals of security breaches that potentially compromised their personal information." He added that the chance for passage was positive, since "the Canadian federal government recently said it plans to act on this recommendation." However, as late as April 2008, the government appeared to be considering letting businesses themselves determine if disclosure is required in cases of "high risk of significant harm."

In Europe, no comprehensive laws exist that force organizations to inform individuals of data breaches. However, as of December 2007, the European Commission suggested implementing laws to force telecommunication providers to inform consumers of data breaches.

Physical, electronic, and procedural security enhancements

A comprehensive and converged physical, procedural, and information security program is essential for every organization, regardless of size, industry, or ownership. And part of that program must address laptop security and the related loss of potentially sensitive data. Implementing the appropriate security measures requires money, time, and effort. Companies must be committed to supplying all three. Management must realize that a lack of funding is a serious impediment to a comprehensive protection program.

Many companies have implemented successful strategies. But research shows that companies that have failed to do so lack a comprehensive, layered approach to security that takes into account physical, electronic, and procedural measures. Also, these measures must be embraced by all employees, including laptop users, management, and security professionals from both physical and electronic disciplines.

The range of costs associated with these measures, including installation, maintenance, and employee education, must be considered as well. When a loss occurs, organizations must acknowledge that existing security measures are inadequate and must be willing to implement additional security safeguards.

Appendices F, G, and H are detailed lists of the physical, procedural, and electronic security measures that can be considered.

Product design

The high volume of laptop thefts occurring around the world can lead to the conclusion that existing security measures do not deter thieves. Because thieves can come from both inside and outside an organization, measures that may stop one type of thief may be ineffective for another.

While many laptop theft prevention products, whether physical, procedural, or electronic, are effective when used appropriately, not all perform well in specific situations. Also, procedural security measures require discipline, auditing, and commitment on the part of users. If not well thought out, they may interfere with daily operations—and be ignored. Employees inevitably find ways to work around security measures deemed to be onerous, which can make devices, including laptops, more susceptible to theft.

Product design is one method under investigation to counter theft. Two approaches have been put forward: one prevents offenses from occurring in the first place; the second facilitates an effective response.

Clarke and Newman advocate a voluntary code for manufacturers of electronic products, including laptops, whereby security features that meet an established standard are built directly into the product. For example, a Home Office study identified factory-installed radio frequency identification (RFID) tags as a promising way to reduce laptop theft.

New response techniques include installing a software program on a laptop that can be connected to the Internet should that unit be stolen. The software dials a monitoring station with information on the IP address the perpetrators are using on the stolen machine. Another type of software program allows the data on the laptop to be destroyed remotely.

Recommended Responses

Disrupting the markets for stolen goods

Targeting the markets for stolen goods is one potential response to the easy way thieves can dispose of laptops. In an interview, one laptop offender identified his key market for stolen laptops as employees who work in commercial high-rises. A considerable amount of work by law enforcement agencies would be required to reduce demand. Notable research on ways to disrupt theft markets is occurring in the United Kingdom.

The response to laptop losses from both public and private sectors is varied and piecemeal. Case studies, interviews, literature reviews, and media searches reveal considerable inconsistencies. Unfortunately, the response by the owner of a stolen laptop may depend upon whether the media reports the incident, and whether any data of significant corporate value needs to be recovered.

Quite often, organizations respond by simply replacing the laptop and continuing as if nothing had happened. In other cases, response will involve a full investigation and implementation of a range of physical, electronic, and procedural security enhancements.

Legislation on data breaches that require organizations to notify victims when personal information is compromised definitely drives corporate responses.

Setting goals

Two distinct yet overlapping issues require attention from security professionals. First, the laptop itself must be protected. And second, the information on the laptop must be secured. To achieve both, the process of developing physical, procedural, and electronic strategies should meet the following two goals:

1. Multiple security layers should be implemented to prevent unauthorized users from gaining access to laptops at the office, on the road, and at home.
2. A combination of prevention methodologies should be adopted to increase the likelihood that unauthorized users are denied access to the data on a stolen laptop.

Seven steps to prevent loss

These two goals can be achieved by adopting the situational prevention techniques shown in Appendix E. They can be implemented by adopting the following seven steps:

Step 1: Conduct an audit to determine where laptops are used within the organization (see Appendix A). This audit determines specific information about a company's laptops, such as where they are being used in the organization, how many are in the inventory, who is using them, for what purpose, and what type of data is residing on each one.

Step 2: Determine whether specific employees need a laptop to do their jobs. If a laptop is not required, it should be replaced with a desktop unit. If the laptop is an essential part of the employee's work, the next steps should be pursued.

Step 3: Classify data on the laptop according to organizational guidelines. The classification scheme should be specific to the organization and its culture. A number of classification models are available. The one selected should be clearly understood, implemented, and followed by all employees. The example of Sample Identification and Classification of Data Levels in Appendix B can help categorize the relative value of "Public Documents," "Proprietary Information," or "Highly Confidential Information." The latter group includes human resources, financial,

Two distinct yet overlapping issues require attention from security professionals. First, the laptop itself must be protected. And second, the information on the laptop must be secured.

security, and organizational plans and strategies, as well as test results, assessments, surveys, or other information the organization has spent money collecting or developing.

Step 4: Determine if data residing on each laptop is necessary for employees to complete their jobs. If not, the data should be removed. If the data is necessary, the next step should be pursued.

Step 5: Conduct a risk assessment to determine possible theft scenarios for the data stored, processed, or transmitted by laptop. Devise appropriate security measures to protect both the data and the laptop. The assessment puts the required physical, procedural, and electronic security measures into perspective, as well as the necessary security awareness training. Obviously, the higher the classification of the data, the more security measures should be in place. A number of risk assessment methodologies are available, such as the one shown in Appendix C. In addition, ASIS International has published a *General Security Risk Assessment Guideline,* available to download for free at www.asisonline.org.

Step 6: Implement the required protection strategies. Appropriate physical, procedural, and electronic strategies are shown in Appendices F, G and H. These detailed lists provide templates for implementing a comprehensive security program. Protective strategies start with security awareness programs; employees must understand their obligation to use the security measures required to protect laptops and data. Employees should be required to indicate, in writing, that they understand the established laptop and data protection guidelines (see Appendix I). Department managers and senior managers should show their support for the policy by signing similar forms. Both facility and IT security personnel have special responsibilities for implementing the policy, and should indicate their willingness to assist on the appropriate forms.

Step 7: Create a loss response team to monitor laptops and data. Should a loss occur, the affected employees should be required to report the loss in writing (see Appendix J.) The team then responds to the report by investigating the losses and determining the scope of the data breach. In addition, the team should be regularly educating users, conducting audits to ensure compliance, annually assessing data needs, and destroying or removing data when it is no longer required. This process is cyclical, since new laptops and data enter and leave the organization on a regular basis.

Need for Research

Literature that specifically addresses protective measures for laptops and data can be elusive, because it is spread out within diverse organizations and documents. As a result, many companies lack the proper understanding—or even the desire—to implement effective security measures for laptops and data. These same organizations may also lack dedicated physical or IT security professionals who can conduct threat and risk assessments.

The connection between laptop thieves and the stages of laptop and data protection requires constant exploration, study, and assessment. In theory, each action a thief must follow to obtain a laptop and use its data (Appendix D) has a corresponding countermeasure, either in the seven steps of loss prevention, or within situational prevention techniques (Appendix E).

In reality, however, losses continue.

Identifying appropriate physical, electronic, and procedural security measures to protect laptops and data is a never-ending process. Some research has determined that multiple layers of security are effective in deterring thieves. Which measures are most effective in specific situations, and which strategies are most cost effective, has yet to be discovered.

What is known is that protecting laptops and their data must be a corporate priority. And finding adequate solutions calls for continuing security research and experimentation.

References

Absolute Software. (2008). *Endpoint security: Data protection for IT, Freedom for laptop users*. Honeoye Falls, NY: Author.

Adshead, A. (2006, May 9). Private life of data. *Computer Weekly*, p. 39-40.

Alpha-Omega Group, SA. (2005). *New Zealand computer crime and security survey*. Dunedin, New Zealand: Author.

Angelo, J. M. (2006). Protecting campus data. Portability can have its price. *Here's how IT managers deal with stolen laptops*. University Business 9(9), 75-76.

ASIS International Guidelines Commission. (2003). *General Security Risk Assessment Guideline*. Alexandria, VA: ASIS International.

ASIS International Guidelines Commission. (2007). *Information Asset Protection Guideline*. Alexandria, VA: ASIS International.

Australia's National Computer Emergency Response Team. (2006). *2006 Australian computer crime and security survey*. Brisbane, Australia: Author.

Background investigations and pre-employment screening. In *Protection of Assets Manual*. Alexandria, VA: ASIS International.

Bass, S. (2005, March). Stay secure at home and on the road. *PC World*, 23, 39.

Best, C., Bolli, S., Cole, L., Ellsworth, D., Kitteringham, G., Parnell, L., Smith, P., & McPhee, R. (2006). *Laptop theft in the commercial high-rise, 2005 survey.* Calgary, Canada: Building Owners and Managers Association Calgary Public Safety Committee.

Best, C., Kitteringham, G. (2006, October). *Preventative maintenance and the nuisance of access control systems.* Presentation at Security Forum, Alberta, Canada.

Brandt, A. (2006, June). This stolen laptop will self-destruct in 5 seconds. *PC World*, (6), 46.

Brigadoon Software. (2003). *BSI computer theft survey results*. Nanuet, NY: Author.

Chipping of Goods Case Study: Laptop Computers. Retrieved February 17, 2007 from http://www.chippingofgoods.org.uk/download/casestudies/laptopcomputers.pdf.

Clarke, R.V., & Newman, G. R. (2005). Security coding of electronic products. In R. V. Clarke & G. R. Newman (Eds.), *Designing out crime from products and systems* (pp. 231-265). Monsey, NY: Criminal Justice Press.

Clarke, R., & Eck, J. (2003). Crime analysis for problem solvers in 60 small steps. In *Center for problem orientated policing*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.

Clarke, R. (1999). Hot products: Understanding, anticipating and reducing demand for stolen goods. *In Policing & Reducing Crime, Police research series paper 112*. London: Home Office.

Clark, R. (2002). *Problem Oriented Guides for Police Series (No. 10)*. Washington, DC: U.S. Department of Justice.

Credant Technologies. (2005). *Corporate exposure survey: Lost & stolen laptop edition*. Addison, TX: Author.

Computer Security Institute. (2007). *The 12th annual computer crime and security survey*. San Francisco: Author.

Cook, J., & Seff, J. (2004, April). Laptop lockdown. *Macworld*, 21, 72-73.

Cornish, Derek. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies (Vol. 3)*. New York: Criminal Justice Press.

Craighead, G. (2003). *High-Rise Security and Fire Life Safety (2nd ed.)*. Boston: Elsevier Butterworth-Heinemann.

Davis, Tom, & Waxman, Henry. (2006, October 13). *Staff report: Agency data breaches since January 1, 2003.* Washington, DC: Committee on Government Reform.

Demery, P. (2006, September). Safe driving? Is your lap strapped in? *Accounting Technology*, 22(8), 45-49.

DLDOS: Data Loss Database – Open Source. Retrieved April 15, 2008, from http://attrition.org/dataloss/dldos.html

Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk Security and Crime Prevention*, 2, 249-265.

Emigh, J. (2002, December 1). The incredible shrinking laptop. *Access Control & Security Systems,* 44 (12).

Ernst & Young. (2004). *Global Information Security Survey 2004*. New York: Author.

European Commission plans security breach notification law. Retrieved April 12, 2008 from http://www.out-law.com/page-8741

Farrell, G., and Pease, K. (1993). Once bitten, twice bitten: Repeat victimization and its implications for crime prevention. In *Police Research Group: Crime Prevention Unit Series Paper 46.* London: Home Office.

Fay, J. (1993). *Encyclopedia of Security Management (2nd ed.)*. Boston: Elsevier Butterworth-Heinemann.

Federal Trade Commission. (2008). Agency Announces Settlement. Retrieved March 29, 2008 from http://www.ftc.gov/opa/2008/03/datasec.shtm

Fennelly, L. (Ed.). (2004). *Effective Physical Security (2nd ed.)*. Boston: Elsevier Butterworth-Heinemann.

Fennelly, L. (Ed.). (2004). *Handbook of Loss Prevention and Crime Prevention (4th ed.)*. Boston: Elsevier Butterworth-Heinemann.

Finney, A. & Wilson, D. (2005.) Handling stolen goods: Findings from the 2002/2003 British crime survey and the 2003 offending, crime and justice survey. *In Home Office Online Report 38/05*. London: Home Office.

Fischer, R., and Green, G. *Introduction to Security (7th ed.)*. Boston: Elsevier Butterworth- Heinemann.

Fixing broken windows. Retrieved February 15, 2008, from *http://en.wikipedia.org/wiki/Fixing_Broken_Windows*

Frank, K. & Charron, D. (2002, January). Protecting information on laptops, PDAs and cell phones. *Strategic Finance Magazine*, 83(7), 24-29.

Garcia, M.L. (2006). *Vulnerability assessment of physical protection systems*. Boston: Elsevier Butterworth-Heinemann.

George, N. (2004). Cyber traps: An overview of crime, misconduct and security risks in the cyber environment. In *Building Capacity Series, No. 3*. Brisbane, Australia: Crime and Misconduct Commission.

Glass, B., & Gottesman, B. Z. (2003, August). Lock down your computer. *PC Magazine*, 72.

Guard Force Operations. In *Protection of Assets Manual: Part 1*. Alexandria, VA: ASIS International.

Headley, A., Best, C., Ellsworth, D., Kitteringham, G., Cole, L., Parnell, et al. (2007). *Laptop theft in commercial buildings, 2006 Survey.* Calgary, Canada: Building Owners and Managers Association, Calgary Public Safety Committee.

Headley, A., Best, C., Ellsworth, D., Kitteringham, G., Cole, L., Parnell, et al. (2008). *Laptop theft in commercial buildings, 2007 Survey.* Calgary, Canada: Building Owners and Managers Association Calgary Public Safety Committee.

Hesseldahl, A. (2006, October 30). Securing your laptop against theft. *BusinessWeek Online*. Retrieved February 15, 2008 from http://www.businessweek.com

Hines, M. (2006, August 7). Preparation eases pain of stolen laptops. *eWeek*, 23(31), 25, 27.

Home Office. (2000). *Chipping of goods cases study: Laptop computers*. London: Author.

The Information Security Glossary. Retrieved on April 14, 2007 from http://www.yourwindow.to/information-security/gl_dataclassification.htm

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention. In *Police Research Series, Paper 98*. London: Home Office.

The High Cost of Laptop Theft. Retrieved April 13-14, 2008, from http://www.absolute.com/solutions-theft-recovery.asp

How DataDot Protects and Identifies Personal Consumer Items. Retrieved May 11, 2008, from http://www.datadotcanada.ca/video.php

James, Andrea. (2007, February 14) *Biggest threat to corporate information: Ignorance.* Retrieved March 29, 2008, from http://seattlepi.nwsource.com/business/303569_security14.html

Kiernan, V. (2006). *Locking up the laptops. Chronicle of Higher Education, 52(48)*, 35. *Latest information on Veterans Affairs data security*. Retrieved April 13, 2008, from http://www.usa.gov/veteransinfo.shtml#credit

Kitteringham, G. (2006, September 26). *Laptop Theft in the Commercial High-Rise*. Presentation at the meeting of ASIS International, San Diego, CA.

Kitteringham, G. (2006). *Security and Life Safety in the Commercial High-Rise*. Alexandria, VA: ASIS International.

Knoke, M., (2008). *Protection of Assets Manual (Vols. 1-4)*. Alexandria, VA: ASIS International.

Kovacich, G., & Halibozek, E. (2003). *The Manager's Handbook for Corporate Security*. Boston: Elsevier Butterworth-Heinemann.

Levits, J., & Hechinger, J. (2006, March 24). Laptops prove weakest link in data security. *The Wall Street Journal*, p. B1, B2.

Laptop Security Guidelines. Retrieved May 6, 2007, from http://labmice.techtarget.com/articles/laptopsecurity.htm

Louwers, T. J., VanDenburgh, W. M. (2003, March). *Data confidentiality in an electronic environment*. The CPA Journal, 24-27.

McQueen, M. P. (2006, June 28). Laptop lockdown—Companies start holding employees responsible for security of portable devices they use for work. *The Wall Street Journal*, pp. D1, D3.

Now RFID tags to track your laptops. Retrieved May 7, 2007, from http://www.ciol.com/content/enterprise/204/104102902.asp

Patterson, D., (2005). *Implementing Physical Protection Systems: A Practical Guide*. Alexandria, VA: ASIS International.

Piazza, P. (2001, October). Securing laptop data against losses. *Security Management*, 45, 37.

Ponemon Institute. (2005). *Lost customer information: What does a data breach cost companies?* Elk Rapids, MI: Author.

Ponemon Institute. (2006). *2006 annual study: U.S. cost of a data breach.* Elk Rapids, MI: Author.

Ponemon Institute. (2006). *U.S. Survey: Confidential data at risk.* Elk Rapids, MI: Author.

Ponemon Institute. (2007). *2007 annual study: U.S. cost of a data breach.* Elk Rapids, MI: Author.

Research Concepts (2007). *The State of Computer & Data Security in Corporations.* Berlin, MA: Author.

Roberts, B. (2006, October). Risky business: Protect employee data from the security risks posed by the use of laptops and mobile devices. *HR Magazine*, 51, 69-73.

Ryder, J. (2001, July 30). *Laptop security, part one: Preventing laptop theft.* Retrieved February 12, 2007 from www.securityfocus.com/infocus/1186

Ryder, J. (2001, August 13). *Laptop security, part two: Protecting information on a stolen laptop.* Retrieved February 12, 2007, from www.securityfocus.com/infocus/1187

Scott, M. (2002). *Problem Oriented Guides for Police Series (No. 13)*. Washington, DC: U.S. Department of Justice.

Security and Criminal Law. In *Protection of Assets Manual.* Alexandria, VA: ASIS International.

Sutton, M., Johnston, K., & Lockwood, H. (1998). Handling stolen goods and theft: A market reduction approach. In *Home Office Research Study (No. 69)*. London: Home Office.

Sutton, N. (2008, March). *Data breach law doesn't go far enough.* Canadian Security, 30(2), 35.

Taylor, C. (2003, February 3). Stop! Laptop thief! *Time*, 16(5), 71.

Ten Steps to a Layered Approach to Laptop Security. Retrieved October 17, 2007, from http://absolute.com/resources/laptop-security-tips.asp

Theft and Fraud Prevention. In *Protection of Assets Manual, Chapter 11.* Alexandria, VA: ASIS International.

Viollis, P., Braunzell, S., Labardee, L., VandePol, B., Kuh, D., & Davies, R. (Eds.). *Workplace Security Handbook.* Alexandria, VA: Jane's Information Group.

What is laptop insurance? Retrieved December 17, 2007, from http://www.wisegeek.com/what-is-laptop-insurance.htm

Whitehead, P., & Grey, P. (1998). Pulling the plug on computer theft. In *Police Research Group: Series Paper 101.* London: Home Office.

WilonWood, L. (2006). Mobile defense forces. *Computerworld*, 40(37), 32-33.

Bibliography

Alpert, M. (2004). Security at your fingertips. *Scientific American*, 290(6), 108-110.

ASIS International Guidelines Commission. (2004). *General Security Risk Assessment Guideline.* Alexandria, VA: ASIS International.

Australia's National Computer Emergency Response Team. (2006). *2006 Australian computer crime and security survey*. Brisbane, Australia: Author.

Bennett, B. (2006, June 4). Just make it go away. *Time*, 167, 17.

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: a guide for managers.* Gaithersburg, MD: National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division.

Brandt, A. (2006, June). This stolen laptop will self-destruct in 5 seconds. *PC World*, 24, 46.

Brigadoon Software (2003). *2003 BSI computer theft survey results*. Nanuet, NY: Author.

Bumgarner, J. N. (2001, June). Hashing out encryption solutions. *Security Management 45*, 66-71.

Caveo Technology (2001). *Laptop computer security white paper.* Cambridge, MA: Author.

Clarke, R.V., & Newman, G. R. (2005). Security coding of electronic products. In R. V. Clarke & G. R. Newman (Eds.), *Designing out crime from products and systems* (pp. 231-265). Monsey, NY: Criminal Justice Press.

Clarke, R.V. & Newman G.R., (2005). Security coding of electronic products. *Crime Prevention Studies Vol. 18*. Criminal Justice Press: Monsey, New York.

Clarke, Ronald V. & Eck, John E. (2003). Crime analysis for problem solvers in 60 small steps. *Center for Problem Oriented Policing*: Office of Community Oriented Policing Services, U.S. Department of Justice.

Clarke, Ronald V. (1999). Hot Products: understanding, anticipating and reducing demand for stolen goods. *Policing & Reducing Crime Police Research Series Paper 112*. Home Office, London, England.

Clarke, Ronald V. (Ed.) (1997). Situational crime prevention: *Successful case studies, (2nd ed.)*. Guilderland, New York: Harrow and Heston.

Conkey, C. (2006, June 23). PTC reports laptop is stolen in the latest U.S. data breach. *The Wall Street Journal*, p. B2.

Credant Technologies (2005). *Corporate exposure survey: Lost & stolen laptop edition*. Addison, TX: Author.

Del're, D. (2006, November 27). Studies find companies failing to secure data on laptops, PDAs; Many lack any policy; More portable devices being used to carry key corporate information. *Investor's Business Daily*, p. A4.

Demos, T. (2007, January). The biggest lost-laptop incidents of 2006. *Fortune*, 155, 36.

Design Council (2003). *Think thief: A designer's guide to designing out crime*. London: Author.

Dewberry, E. (2003). Designing out crime: Insights from ecodesign. *Security Journal*, 16(1), 39-49.

Dunn, R. (2003). Mitigating laptop theft. *Security: For Buyers of Products, Systems & Services*. 40(10), 38-39.

Dvorak, P. (2006, June 22). Spike in laptop thefts stirs jitters over data. *The Washington Post*, p. B1.

Ecker, K. (2006, June). Hot hardware: Rise of corporate laptop thefts creates need for increased security. *InsideCounsel*, 16, 40-42.

Ekblom, P. (1997). Gearing up against crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world. *International Journal of Risk Security and Crime Prevention*, 2, 249-265.

Erol, R., Press, M., & Cooper, R. (2002). Designing-out crime: Raising awareness of crime reduction in the design industry. *Security Journal*, 15(1), 49-61.

Farrell, G., and Pease, K. (1993). Once bitten, twice bitten: Repeat victimization and its implications for crime prevention. Police Research Group: *Crime Prevention Unit Series, Paper No. 46*. London, England: Home Office.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention. *Police Research Series, Paper 98*. London: Home Office.

Fenton, J. (2001, March). Security at your fingertips—New notebooks offer biometric protection. *PC World*, 19, 60.

Frank, K., & Charron, D. (2002, July). Protecting information on laptops, PDAs, and cell phones. *Strategic Finance Magazine*, 83, 24-29.

Friedberg, E., & McGowan, M. (2006). Lost back-up tapes, stolen laptops, and other tales of data breach woe. *Computer & Internet Lawyer*, 23(10), 6-10.

Garcia, M.L. (2001). *The design and evaluation of physical protection systems*. Boston: Elsevier Butterworth-Heinemann.

Garcia, M.L. (2006). *Vulnerability assessment of physical protection systems*. Boston: Elsevier Butterworth-Heinemann.

George, N., & Gordon, P. (2005). Information security: Keeping sensitive information confidential. *Building Capacity Series, No. 7*. Brisbane, Australia: Crime and Misconduct Commission.

Glass, B., & Gottesman, B. Z. (2003, August). Lock down your computer. *PC Magazine,* 22, 72.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2006). *Eleventh annual CSI/FBI computer crime and security survey*. San Francisco: Computer Security Institute.

Gottesman, B. Z. (2006, May). Lock it down. *PC Magazine*, 25, 85.

Greenemeier, L. (2006, December 4). Tomorrow's security today—Security systems of the future must be smarter, faster, and, above all, proactive. *Information Week*, 45, 1117.

Harrington, V., & Mayhew, P. (2001). Mobile phone theft. *Home Office Research Study 235*. London: Home Office.

Headley, A., Best, C., Ellsworth, D., Kitteringham, G., Cole, L., Parnell, L., Smith, P., Bolli, S., and McPhee, R. (2007). *Laptop theft in commercial buildings, 2006 survey*. Calgary: Canada: Building Owners and Managers Association Calgary Public Safety Committee.

Hayes, F. (2006). Hey, Problem-solver. *Computerworld*, 40(36), 50.

Hines, M. (2006). Preparation eases pain of stolen laptops. *eWeek*, 23(31), 25, 27.

Hines, M. (2006). Experts: Response speed is key. *eWeek*, 23(31), 25, 27.

Kandra, A. (2004, August). Keep your hands on your handhelds. *PC World*, 22, 49-51.

Learmount, S., Anderson, J., & Haake, S. (2000). *Design against crime*. Cambridge, UK: The Judge Institute of Management Studies, University of Cambridge.

Lester, A. (2001). Crime reduction through product design. *Trends and Issues in Crime and Criminal Justice, No. 206*. Canberra: Australia. Australian Institute of Criminology.

Louwers, T. J., VanDenburgh, W. M. (2003). Data confidentiality in an electronic environment. *The CPA Journal*, 73(3), 24-27.

McQuate, C. (2002, December). Penning effective policies. *Security Management*, 46, 107-111.

Mitchell, R. L. (2005). Lost laptops sink data. *Computerworld*, 39(29), 24.

Patterson, D.G. (2005). *Implementing physical protection systems: A practical guide.* Boston: Elsevier Butterworth-Heinemann.

PGP Research Report (2005). *Lost customer information: What does a data breach cost companies?* Menlo Park: CA: PGP Corporation.

Phifer, L. (2004, December). Portable security: Safeguarding PDAs and smartphones. *Business Communications Review*, 34, 19-23.

Phifer, L. (2003, September). Securing wireless access to mobile applications. *Business Communications Review*, 33, 47.

Piazza, P. (2006, January). Arming the road warrior. *Security Management*, 50, 78-85.

Piscitello, D. M., & Phifer, L. (2002, December). Best practices for securing enterprise networks. *Business Communications Review*, 32, 32-37.

Ponemon Institute. (2005). Lost customer information: *What does a data breach cost companies?* Traverse City, MI: Author.

Ponemon Institute. (2005). *National survey on data security breach notification*. Traverse City, MI: Author.

PR Newswire (2005, June 27). Absolute Software and LoJack Corporation announce branding partnership to introduce LoJack for Laptops. Retrieved February 5, 2007 from http://www.prnewswire.com

PR Newswire (2006, October 23). Ponemon report shows sharp rise in the cost of data breaches; Sponsored by PGP Corporation and Vontu, study shows 31% increase in financial impact of data loss incidents since 2005. Retrieved February 5, 2007 from http://www.prnewswire.com

Premo, R. (2001, March). Laptop locator. *Security Management*, 45, 24-25.

Quinn, K. J. S. (2006). 2005 *New Zealand computer crime and security survey.* Dunedin, New Zealand: Alpha-Omega Group, South Australia.

Radding, A. (2007, February). Protecting Laptop Data. *Storage Magazine*. 7(1).

Rapoza, J. (2006, November 6). Laptop losses loom. *eWeek*, 24, 50.

Roberts, (2006, October). Risky Business: Protecting Employee Data. *HR Magazine*. 51(10) 68-73.

Sisk, M. (2006, October). Protecting laptops is now affordable, easy. *U.S. Banker*, 116, 20-21.

Spangler, T. (2006, July). Don't spring a data leak. *Baseline*, 61, 15-18.

Stasiak, K. (2008, April). Avoiding mistakes. *Security*, 45, 88-89.

Stroud, J. (2006, February 7). What's on your laptop? And if someone stole it, would it damage the company you work for? *St. Louis Post Dispatch*, p. A1.

Vijavan, J. (2006). Federal breaches spark security review push. *Computerworld*, 40(25), 12.

Weinberg, S. (2006). Software helps find stolen computers. *The Wall Street Journal—Eastern Edition*, p. B3.

Whitehead, P., & Gray, P. (1998). Pulling the plug on computer theft. *Police Research Series, Paper 101*. London: Home Office.

About the Author

Glen W. Kitteringham, CPP, is a security professional, environmental criminologist, and writer with experience in the security industry dating back to 1990. He earned a Master of Science from the University of Leicester, and the Certified Protection Professional (CPP) designation through ASIS International.

Kitteringham has conducted research on a variety of security topics, including crime pattern analysis, retail theft, and laptop theft. He has been published in an array of media on security management, physical security, emergency response planning, and guard force operations. ASIS International published his first book, *Security and Life Safety in the Commercial High-Rise*, in 2006.

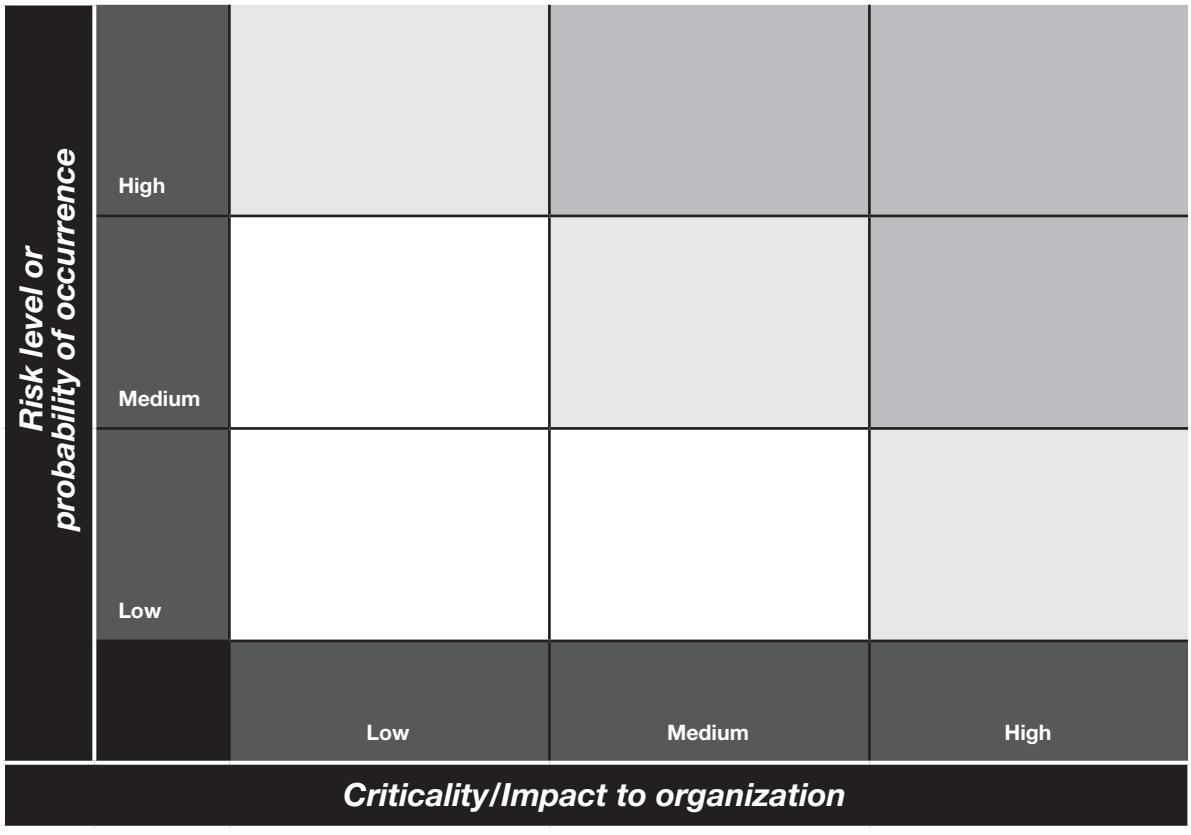
Kitteringham is a member of the International Foundation for Protection Officers; Building Owners and Managers Association, Calgary; the National Fire Protection Association; and ASIS International.

Appendix A: Threat and Risk Matrix Model

The following model can help management define what level of risk they are willing to assume and how various losses would affect ongoing operations. As a start, management must confront its worst-case scenario and then sort through alternatives.

The following model, with related questions, can help management make critical decisions that affect not only how the company will react to the loss of a laptop and the data it contains but also how it will establish its ongoing loss prevention strategy. Answers that denote a high, medium, or low level of probability and criticality can be charted on the following graph.

Threat and Risk Matrix Model



Probability: Measures the level of risk that a theft will occur.

Low: There is no or little history of the threat occurring, and it is not considered likely.

1. Laptops never leave work areas and are inaccessible to unauthorized users.
2. Multiple levels of security are in place.

Medium: There is a moderate history of the threat occurring, and/or information is available that would lead management to reasonably believe that there is a 50/50 chance of the event reoccurring.

1. Laptops are only moved occasionally between home, road, and business.
2. Some security measures are in place.

High: There is a significant history of the threat occurring, and/or available information leads management to reasonably believe the threat will occur in the foreseeable future.

1. Laptops are highly mobile.
2. No security measures are in place.
3. Other company laptops have been stolen.
4. Company has been targeted in the past.

Criticality: Measures the financial impact to the organization.

(Note: Dollar values and categories assigned here are subjective. One company may see a $5,000 loss as the cost of doing business, while another may find the same value unacceptable.)

Low: Loss of $1,000 to $4,999

1. Replacement cost per individual laptop, recovery of data (if necessary), repair of physical damage (if required), downtime of employees, other associated costs are acceptable.
2. The theft affects few people inside the organization, and none outside the organization.

Medium: Loss of $5,000 to $99,999

1. Vital personal and business information is lost that, if released to the public or accessed by others, will have a serious effect on individuals personally and the company financially.
2. The loss affects employee morale.

High: Loss of $100,000 or more

1. Privacy laws are breached. The organization is found to be negligent, is sued in class action suits, and loses market share. The public is warned of the potential for identity theft.
2. The information lost is irreplaceable.
3. The company loses the confidence of the public, media, and/or shareholders.
4. Employees are physically assaulted or worse during the incident.
5. The loss compromises national security and hinders ongoing investigations.
6. Organizational operations will have to be suspended while laptops and/or data are replaced.

Questions to assist in determining criticality of data:

1. What competitive advantage does this information provide?
2. What is the likelihood that competitors are seeking this information?
3. What is the potential damage to
   - the organization's operations?
   - an individual?
   - to the organization's reputation or image?
4. What is the potential for the loss of
   - customer, shareholder, or business partner confidence?
   - trade secret or patent protection?
   - ability to be first to market?
   - market share?
5. What is the effect on stock value or venture capital support?
6. What is the potential privacy violation impact?
7. What is the potential financial impact of fines the company may be subjected to?
8. Can the data be easily recreated?
9. What is the potential impact on employees if data is exposed?
10. Does the loss of data compromise any kind of investigation?
11. Must the data reside on a laptop?

Questions to assist in determining probability of a laptop loss:

1. How mobile is the laptop?
2. What protective security measures are in place?
3. Do security measures consider available physical, electronic, and procedural processes?
4. Are employees trained in security measures?
5. Does the company have a security awareness program?
6. Are employees and company senior management aware of the ramifications of a loss?
7. Is a data recovery team available?
8. Are other thefts occurring with coworkers?
9. Are other thefts occurring on the premises?
10. Is the company a potential target because of the nature of its business?
11. Has the organization considered that its laptops could be stolen simply as laptops, regardless of the information on them?
12. Is the organization aware that it could suffer a loss in the future, even if one has not occurred so far?

Appendix B:
Laptop Inventory Checklist

Laptop inventory number: _____

Laptop serial number: _____

Description of laptop: _____

Location of laptop: _____

Employee(s) using the laptop: _____

Purpose for which the laptop is being used: _____

_____

_____

_____

Type of data residing on the laptop: _____

_____

_____

_____

Classification of data type: _____

Person conducting inventory: _____

Date: _____

Appendix C: Data Identification and Classification Levels

Level	*Classification of document/Data*	*Identification/Description*
3	Highly confidential	Information that, if made public or even shared around the organization, could seriously impede the organization's operations. Information considered critical to its ongoing operations and could seriously damage the organization if it were lost or made public. Examples include accounting information, business plans, sensitive customer information, and medical records. Sensitive internal documents would also be included such as those describing pending mergers and acquisitions; investment strategies; and architectural plans or designs. Information classified as Highly Confidential has very restricted distribution and must be protected at all times. **Security at this level is the highest possible.**
2	Proprietary	Information that is not approved for general circulation outside the organization. Its loss would inconvenience the organization or management, but disclosure is unlikely to result in financial loss or serious damage to credibility. Information of proprietary nature to be used by authorized personnel only. Examples include procedures, operational work routines, project plans, and designs and specifications that define the way the organization operates. **Security at this level is high.** Other examples include internal memos, minutes of meetings, and internal project reports. **Security at this level is controlled but normal.**
1	Public documents	Information in the public domain that has been approved for public use, such as annual reports and press releases. **Security at this level is minimal.**

Implementing the 25 techniques of situational prevention described in Appendix E can reduce the chance that a determined thief will gain access to a company's laptops and data.

Appendix D: Stages and Steps in Laptop Theft; Recommended Responses

To counter the stages of a laptop theft and implement an appropriate response, companies must institute specific security measures that meet the probability and criticality tests described in Appendix A and protect the proprietary and highly confidential information identified in Appendix C.

Stages in a theft	*Steps thief follows*	*Company response*
1. Preparation	Develop access methods to defeat physical and procedural security measures. Options include breaking and entering, social engineering, and piggybacking on legitimate access cards.	Laptop owners and users must realize they are targets, and identify the thief's tools and methods. Appropriate physical and procedural security countermeasures should be implemented.
2. Identify likely targets	Conduct pre-theft surveillance to determine appropriate targets, test defenses, and access the site. This stage may include observing and testing staff, taking photos, stealing uniforms, unlocking doors for later re-entry, and hiding in closets.	Laptop owners and users must follow company security measures, challenge and confront unauthorized users, and deny access to unauthorized users.
3. Access the target location: work, home, road, vehicle, hotel room, person, etc.	Travel to wherever the laptop is located.	Harden the target by implementing countermeasures.
4. Defeat all security measures to gain item	Defeat all physical and procedural security defenses.	Harden the target by implementing countermeasures.
5. Successfully leave with item	Elude all remaining countermeasures, whether deliberate or accidental.	Harden the target by implementing countermeasures.
6. Defeat all electronic protective measures	Hack passwords; replace hard drive; unencrypt programs and drives; find, erase, and/or remove security programs; make laptop fully functional.	Implement high levels of security, such as password protection, encryption, and tracking software.
7. Convert product to a useable value: drugs, money, equipment, data/information, revenge	Sell or trade device; access and utilize data; deny equipment to owner; access and utilize hardware.	Vital information must not be stored on laptops. Owners and users should conduct an equipment and data risk profile and ensure that laptops and data are useless if stolen. They should attempt to retrieve data and activate the loss team.

Appendix E: Reducing the Threat from Determined Laptop Thieves— 25 Situational Prevention Techniques

Increase the Effort

1. **Target harden (both premise and laptop itself)**
   - Install astragals and latch guards.
   - Install metal doors and frames.
   - Harden doors and doorframes.
   - Install high-quality hardened steel lock devices.
   - Lock doors accessing secure spaces.
   - Lock laptops in secure areas.
   - Install laminated glass on windows and doors.
   - Use laptop-locking devices regularly.
   - Eliminate access to externally mounted electromagnetic locks with a cover.
   - Watch for pre-theft surveillance.
   - Install local audible door alarms on doors, rooms, and device.
   - Keep all doors locked.
   - Reinforce doorjamb with screws.
   - Install deadbolts on doors and screens.
   - Lock washrooms/closets to deny hiding places.
   - Implement full disc encryption.
   - Repair any damage from a break-in immediately.
   - Determine if a laptop is appropriate and necessary for employee. Use requirements.

2. **Control access to facilities**
   - Reduce the number of access points.
   - Install an access control system, including individual floor select in elevators.
   - Install burglar alarm.
   - Investigate installation of barriers to all access points.
   - Install main floor lobby doors to deny unauthorized after-hours access.
   - Install electronic turnstiles.
   - Use security to monitor and control access.
   - Program elevators to wait in the tower after hours so thieves cannot jump onto waiting elevators.
   - Maintain strict key and access card control.

3. **Screen exits**
   - Consider installing electronic article surveillance on laptops.
   - Conduct searches of people exiting.
   - Permanently lock perimeter doors.
   - Conduct audits of access control points and CCTV to monitor door activity.

4. **Deflect offenders**
   - Conduct background checks on employees and contractors.
   - Ensure that, if required, contractors and others are appropriately licensed.
   - Never leave laptop alone or unguarded.
   - Stay informed of emerging theft schemes.
   - Keep laptops inconspicuous by using simple carrying cases.

5. **Control tools/ weapons**
   - Do not leave bags behind for thieves to carry laptops away in.
   - Put away laptop paraphernalia such as docking stations, power cords, and cables.
   - Lock tools and keys that can be used to cut cables or open drawers.
   - If possible, disable audible tones on card readers near stairwell doors. They can act as a signal for waiting thieves that the door will be opening.

Increase the Risks

6. Extend guardianship

- Make department and/or employee responsible for laptops and replacements.
- Secure devices when not in use.
- Install GPS (Global Positioning System) monitoring.
- Arrest offenders.
- Seize stolen property from offenders.
- Ban known offenders from premises.
- Share theft information, techniques, and theft activities between business and law enforcement.
- Jointly with property management and tenants, conduct lobby vulnerability assessments.
- Reward contractors who enforce rules about accessing company space.
- Fix multiple I.D. labels on laptops.
- Have IT and facility security work together to secure data and devices.

7. Assist natural surveillance

- Improve street and office lighting.
- Encourage staff to monitor work areas for suspicious activity.
- Call building security or police when suspicious activity is identified.

8. Reduce anonymity

- Challenge visitors.
- Institute visible I.D. program for employees and visitors.
- Sign in all visitors.
- Escort all visitors.
- Do not leave visitors unattended.
- Report all thefts to security and police.
- Monitor personal information if laptop is stolen, as it has identity theft implications.
- Report data breaches.
- Implement a reporting system for stolen and lost laptops.

9. Use place managers

- Reward vigilant staff for informing security and/or police of incidents.
- Educate contractors to assist.
- Advise employees about thieves' techniques.
- Train employees in protecting data and laptop devices.
- Monitor use of laptops to ensure legitimate users are using them appropriately.

10. Strengthen formal surveillance

- Install CCTV on main access points into space.
- Actively monitor burglar alarms.
- Monitor access control alarms.
- Institute or increase security guard patrols.
- Conduct audits on laptops regularly (daily, weekly, monthly) to ensure none has gone missing.
- Implement policies and standards regarding information and laptop device protection.
- Restrict access to sensitive data.

Reduce the Rewards

11. Conceal targets

- Determine what the real target is (data or device?)
- Lock laptops and other electronic items in secure area after hours, and when left unattended for periods of time.
- Investigate use of security devices to ensure they work as promised.
- Seek restitution.
- Back up data off laptop drive regularly.
- Store all vital information away from laptop drive.
- Conduct risk assessment on laptop and data to determine relative value and corresponding security measures.
- Identify and classify data.
- Keep confidential information confidential.

12. Remove targets

- Consider locking laptops in a secure vault.
- Evaluate company needs to ensure laptops are necessary.
- Conduct security laptop audits frequently to identify employees not following procedures.
- Have employees take laptops home.

13. Identify property

- Mark company logo in more than one location.
- Maintain specific records of laptops, including receipts, manufacturer, model, and serial number for recovery purposes.
- Keep user manuals and warranty cards.
- Register laptop with manufacturer.
- Implement microdot serial number system.

14. Disrupt markets

- Monitor pawnshops.
- Arrest fences.
- Seize stolen property.

15. Deny benefits

- Install password protection devices using complex alphanumeric passwords. Change them regularly.
- Do not store vital company data directly on laptop.
- Install software that dials a central monitoring station if activated and reports IP address.
- Install biometric protection on USB thumb drive to secure against unauthorized software access.
- Install BIOS password.
- Activate login password.
- Install 'kill' switches to erase data remotely and deactivate device requiring repair and activate 'stolen property' message.
- Render machine unusable via endless reboot.
- Use password-protected screensavers.
- Ensure all software patches are installed regularly.

Reduce Provocation

16. Reduce frustrations and stress

- Reduce workplace hostility.

17. Avoid disputes

18. Reduce temptation

- Lock away equipment when not in use.

19. Neutralize peer pressure

- Educate potential end users of stolen laptops.

20. Discourage imitation

- Punish thieves.
- Seek restitution.
- Punish employees who violate rules.
- Hold management accountable.

Remove Excuses

21. Set rules

- Have documented and specific policies in place regarding responsible use of, and expectation for, protecting company equipment (laptop security guidelines).
- Enforce rules.
- Hold employees accountable for failing to follow procedures.
- Make individuals accountable for laptops.
- Establish and enforce property removal procedures.
- Investigate all laptop theft incidents.
- Identify true value of data by conducting risk assessment of data and equipment.
- Investigate all theft and attempted theft incidents.
- Purchase laptop theft insurance.

22. Post instructions

- "Private property"
- "Inspect badges"
- "Lock up your valuables"
- "Unauthorized entrance not allowed"
- "All visitors must report to Reception"

23. Alert conscience

- Submit "Victim Impact Statements" to courts.
- Educate employees on company and personal responsibility.

24. Assist compliance

- Educate employees on theft techniques.
- Institute a security awareness education program.

25. Control drugs and alcohol

Appendix F: Implementing Physical Security Measures—35 Strategies

#	*Response*	*Resource*	*Responsible person*	*How it works*	*Considerations*
1	Install astragal & latchguards.	*Introduction to Security, 7th Ed.,* Fischer & Green, p. 171	Property owner	Denies immediate access to lock mechanism.	Too much space between mechanism and door still allows thief to defeat door hardware. Will slow down but not stop all thieves.
2	Install hardened door and frame.	*Vulnerability Assessment of Physical Protection Systems,* Garcia, p. 216-222	Property owner	Decreases "give" in door and frame. Making it harder to spread frame apart keeps lock mechanism from being accessed.	Increased weight of door may mean adjustment to closure and door mechanisms.
3	Harden doors and frames.	*Effective Physical Security, 2nd Ed.* Fennelly, p. 147	Property owner	Similar to #2.	Similar to #2.
4	Install high-quality hardened steel lock hardware.	*Effective Physical Security, 2nd Ed.* Fennelly, p. 148	Property owner	Increases delay time for thief to defeat door. Poorer quality mechanism is easier to break and penetrate.	Increased cost. Is not 100% guaranteed to stop all thieves.
5	Lock doors accessing private space.	*Effective Physical Security, 2nd Ed.* Fennelly, p. 90	Property owner	Denies access to opportunists.	People must be trained to always lock doors and confirm regularly, especially at day's end.
6	Lock laptops in secure areas.	*Effective Physical Security, 2nd Ed.* Fennelly, p. 90	Laptop owner and property owner	Adds an additional barrier thieves must defeat.	Increased costs in creating secure area. Staff must be trained to use. Increases delays in staff accessing device.
7	Install laminate glazing on glass.	*Vulnerability Assessment of Physical Protection Systems* Garcia, p. 222-224	Property owner	Increases delay time to thief who may try to kick in doors and windows.	Increased cost. Quality of laminate must be confirmed.

#	Response	Resource	Responsible person	How it works	Considerations
8	Use laptop locking devices regularly.	"Lock down your computer," *PC Magazine*, May 6, 2003, Glass, p. 72	Laptop owner/user	Adds additional barriers for thieves to defeat. Increases delay time, which increases risk for thief.	Increased cost. Decreased employee productivity. Some devices work better than others. Not 100% guaranteed effective.
9	Eliminate access to externally mounted electro-magnetic locks with a cover.	*Laptop Theft in Commercial Buildings 2006 Survey,* Headley, et al., p. 31	Owner of EML	Denies access to thieves who can easily defeat EML if they know how. In order to defeat it, they must be able to access it. By covering it, access is severely reduced.	Additional cost. Aesthetics may be an issue. Equipment must be correctly installed.
10	Consider locking laptops into a secure vault or safe.	*Laptop Security, Part 1, Preventing Laptop Theft* Ryder, p. 3	Senior management	Central vaults are one consideration for protection. Adds another layer the thief must defeat in order to access device.	Size and location of vault, a responsible party to manage access issues, how it is or can be secured, accessing after hours, and effectiveness.
11	Install local audible door alarms on doors, rooms, and device.	*Effective Physical Security, 2nd Ed.* Fennelly, p. 199	Property owner	Sends out an audible alarm when an attempted theft is underway. Brings attention to location and thief.	Minor additional cost. Need a response procedure and people to respond.
12	Reinforce doorjamb with screws.	*Handbook of Loss Prevention and Crime Prevention, 4th Ed.,* Fennelly, p. 151	Property owner	Stops door jamb from being pried away from frame, thereby exposing lock mechanism.	Minor additional cost. Long, heavy-duty (2-4 inch) wood screws are required. Avoid wood screws longer than the width of the door frame, as they penetrate behind it.
13	Install long throw deadbolts on doors and screens.	*Handbook of Loss Prevention and Crime Prevention, 4th Ed.*, Fennelly, p. 176	Property owner	Adds additional barrier thief must defeat in order to access area.	Minor additional cost. Staff must be trained to ensure deadbolts are always used properly. Self-locking deadbolts should be considered. Life safety may be an issue.
14	Lock lavatories and closets to deny hiding places.	*Effective Physical Security, 2nd Ed.*, Fennelly, p. 53-54	Property owner, employees	Denies hiding space to thieves waiting for employees to leave.	Personal safety may be an issue for those confronting thieves hiding. Locked washrooms cost money and require a code, card, or key.
15	If possible, disable audible tones on card readers near stairwell doors.	*Laptop Theft in Commercial Buildings 2006 Survey,* Headley, et al., p. 30-33	Access control system owner	Tones can act as a signal for waiting thieves that the door will be opening. By disabling the tones, it will be difficult to access the door before it closes.	Requires the system administrator to disable the alarms.

#	*Response*	*Resource*	*Responsible person*	*How it works*	*Considerations*
16	Connect audible motion sensor alarm to laptop.	*The Incredible Shrinking Laptop, Access Control & Security Systems* Emigh, p. 2	Laptop owner/user	An audible alarm activates when the laptop is moved by an unauthorized person (thief).	Alarm must be activated and installed. Some thieves may not be deterred. Alarm must be within hearing range of the laptop owner.
17	Have alarm activated when laptop disconnected from network.	*The Incredible Shrinking Laptop, Access Control & Security Systems,* Emigh, p. 2	Senior management	When laptops are disconnected from the network, an alarm activates information monitoring staff.	Network must be monitored in real time. Responder must be dispatched. Procedure required, as legitimate user could be disconnecting.
18	Repair any damage from a break-in immediately.	"*Fixing Broken Windows*" http://en.wikipedia.org/wiki/Fixing_Broken_Windows	Property owner	Eliminates an obvious method of entry.	Thieves may attempt or succeed again, so simply repairing an existing weakness may not be enough deterrence. May be an opportunity to upgrade security features.
19	Reduce the number of access points into property.	*Effective Physical Security, 2nd Ed.,* Fennelly, p. 97	Property owner	Reduces vulnerable points. Increases effort on part of thieves.	May call for review and redesign of facility. Will likely cost money. Will likely change procedures.
20	Install electronic access control system.	*Vulnerability Assessment of Physical Protection Systems*, Garcia, p. 173-199	Property manager/ owner	Creates defense-in-depth with additional layers and barriers.	Designing and implementing will cost money. System requires ongoing management.
21	Install interior intrusion sensors with appropriate response.	*Vulnerability Assessment of Physical Protection Systems*, Garcia, p. 87-112	Property owner	Provides real time monitoring of property	Will cost money. Effectiveness dependent upon number of alarms being monitored. Requires timely response usually from security force.
22	Install and harden barriers at all access points.	*Effective Physical Security, 2nd Ed.,* Fennelly, p. 96	Property owner	Creates obstacles for thieves to overcome.	Thieves will attack barriers and, depending upon the quality and quantity of barriers, may or may not be successful. Barriers should be considered delay only.
23	Install main floor lobby doors to deny unauthorized after hours access.	*Effective Physical Security, 2nd Ed.*, Fennelly, p. 96	Property owner	Before thieves get to laptops or conduct pre-theft surveillance, they face an additional barrier.	Installation of barriers potentially costly. May not stop thieves from accessing space before closing hours.

#	*Response*	*Resource*	*Responsible person*	*How it works*	*Considerations*
24	Install electronic turnstiles.	*Vulnerability Assessment of Physical Protection Systems,* Garcia, p. 209-210	Property owner	Controls pedestrian traffic in and out of a facility. Funnels pedestrians through specific points.	Waist-high turnstiles considered delay barriers only.
25	Install RFID (Radio Frequency Identification) for tracking.	"*Now RFID Tags to Track Your Laptops*" http://www.ciol.com/content/enterprise/2004/104102802.asp	Senior management	RFID tags can be installed on laptops. When the laptop is moved past 'gates,' an alarm is generated, bringing the theft to the attention of employees.	RFID has been used extensively in retail for many years. Expensive equipment must be installed for the alarm to sound. There is the chance of false alarms. In addition, employees must be ready to respond. As seen in the retail field, employees can learn to ignore alarms. Requires administrative set-up and ongoing monitoring.
26	Install keychain alarm.	"Stop! Laptop Thief!" *Time*, Taylor, p. 71	Laptop owner	An audible device sounds when the keychain and laptop get more than 40 feet apart.	Owners must be prepared to do something when seeing their laptops walk away.
27	Lock laptops and other electronic items in secure area after hours and when left unattended for short and extended periods of time.	"Preparation eases pain of stolen laptop" *eWeek,* Hines, p. 25	Laptop owner/user	Laptop must not be left alone as this is when it is most vulnerable to theft.	Inconvenient to constantly keep an eye on device or to find fully secure area after hours.
28	Affix identification labels on laptops.	"Data Confidentiality in an Electronic Environment" *The CPA Journal*, Louwers & VanDenburgh, p. 26	Laptop owner	A permanently affixed label is attached using a 'superglue' to the body of the laptop with clear identification marking on the steel plate.	Labels may be a deterrent but are more seen as aiding recovery. They clearly identify ownership.
29	Ensure perimeter doors have permanently locked function activated.	*Workplace Security Handbook* Viollis, et al., p. 66-74	Property owner	Ensure doors have permanently locked function activated. Increases access control as it channels people through a central point where they can be identified, and reduces access points for thieves to gain entrance.	Can be inconvenient for legitimate place users who will sometimes wedge doors open for a variety of reasons. Doors must be checked regularly to ensure they are locked.

#	Response	Resource	Responsible person	How it works	Considerations
30	Install and conduct audit of the CCTV system to ensure system is in proper working order. System needs to be monitoring specific laptop locations.	*Implementing Physical Protection Systems: A Practical Guide,* Patterson, p. 60-63	CCTV system owner/user	CCTV systems should be designed to detect thieves. In order for them to achieve this function, they must work as specified and then periodically audited to maintain this expectation.	Audits cost money and require repairs. Also, in order for CCTV to work as designed, people must respond. CCTV does not necessarily stop thefts from occurring but can be an important investigative aid.
31	Improve street and office lighting to increase surveillance capabilities.	*Protection of Assets Manual, Vol. III* p. 19-IV-1 to 19-IV-17	Property owner/user	Provides proper lighting for personnel and CCTV identification purposes.	Proper lighting will not deter all thieves. Lighting outside the property line will be outside the control of the property owner. If required to increase and/or upgrade lighting, there may be additional long-term costs.
32	Install device to secure laptop in trunk of car, if appropriate.		Laptop owner/user	For protecting laptop on the road when it must be left in a vehicle, consider installing a safe or other securing device.	Device must be considered for delay purposes only. Car may be stolen. Not appropriate for rental vehicles. Best to keep the laptop with the person but it may not always be realistic so securing it in the vehicle may be the best alternative. Each situation must be evaluated individually.
33	Keep laptop out of sight.		Laptop owner/user	Keep the laptop hidden when not needed. Thieves conduct pre-theft surveillance looking for laptops to steal.	Thieves may break into a vehicle just to look even if they do not know there is a laptop in it.
34	Keep laptop with user. Do not leave in vehicle.		Laptop owner/user	The ideal situation is to keep the laptop with the person who uses it.	It may not always be appropriate to carry the laptop with the person but the best protection is to keep the laptop and person together.
35	Place micro-dots with serial numbers on units for identification purposes.	"*How DataDot Protects and Identifies Personal Consumer Items.*" http://www.datadotcanada.ca/video.php	Laptop owner	Provides identification if laptop is stolen and recovered.	Product may be removed. Must be registered and in place on unit.

Appendix G: Implementing Procedural Security Measures—61 Strategies

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
1	Develop written procedures for protecting laptops in unique settings: in the office, on the road, and at home.		Company	Laptop owners and users require written details for specific protection strategies. Strategies are most effective when communicated in writing.	Every situation will not be covered so the laptop owner/user will have to use common sense when following protective strategies.
2	Ensure contractors are appropriately licensed.	"Guard Force Operations, Part I" *Protection of Assets Manual,* p. 9-I-7 to 9-I-8	Client and contractor management	By ensuring contract staff are appropriately licensed, an organization helps weed out contractors with criminal backgrounds.	Not all thieves have been caught, arrested, and convicted so this will not eliminate everyone with a propensity to steal, but it will go a long way in eliminating those with criminal tendencies from positions where they can steal.
3	Watch for pre-theft surveillance.	*Laptop Theft in Commercial Buildings 2006 Survey* Headley, et al., p. 25	Property owner, laptop owner	Monitoring suspicious activities, challenging thieves, and banning from sites, sends a message that security and company are watching out for such activity.	Not all thieves will be obvious and it may be dangerous, depending upon location, to approach individuals.
4	Investigate use of security devices (hardware, software, and physical) to ensure they work as promised.	"Safe Driving? Is your laptop strapped in?" *Accounting Technology,* Demery, p. 47	Person wishing to implement measures	Often products do not live up to marketing. Therefore when devices are used, they provide a false sense of security.	Conducting tests of equipment can be expensive and take time but well worth the effort.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
5	Search people exiting.	"Security and Criminal Law," *Protection of Assets Manual* Chapter 20, p. 20-24 to 20-26	Property owner	Staff conducting searches may find stolen laptops. People may not steal laptops if they know they will be searched upon exit.	There are legal and cultural (societal and company) ramifications to searching people.
6	Conduct risk assessment to determine if a laptop is appropriate and necessary for employee, data, and use requirements.	"Private Life of Data" *Computer Weekly* Adshead, p. 2	Company laptop distributor	Places laptops only with those absolutely requiring one. Potentially reduces target numbers.	May require periodic fine-tuning. Potential to impede work flow if not properly implemented.
7	Restrict access to those on company business only.	*Laptop Theft in Commercial Buildings 2005 Survey* Best, et al., p. 19	Company officials	Denies access to unauthorized users and also denies possible pre-theft surveillance.	Requires effective physical security barriers as well as proper procedures reinforced by educated staff.
8	Conduct background checks on employees and contractors.	"Background Investigations and Pre-employment Screening" *Protection of Assets Manual,* p. 1-IV-1 to 1-IV-18	Employer and contractor management	By conducting a thorough background investigation, those with criminal backgrounds will not be hired.	Not all thieves have been caught, arrested, and convicted. So this will not eliminate everyone with a propensity to steal, but it will eliminate those with criminal records from positions where they can steal.
9	Conduct an audit of the access control system to ensure it is in proper working order.	"*Preventative Maintenance and the Nuisance of Access Control Systems*" Best & Kitteringham	Access control system owner/user	Ensures that the system used to monitor door activity is working properly. As many nuisance alarms have been eliminated from the system, allows security to quickly identify legitimate alarms.	Access control systems require constant care and attention through preventive maintenance. Additionally, unless all devices and points attached to the system are confirmed to work as designed, an audit is required to ensure they are in proper working order. Loud nuisance alarms can quickly overwhelm monitoring staff.
10	Maintain strict key and access card control.	*Handbook of Loss Prevention and Crime Prevention, 4th Ed*. Fennelly, p. 183-184	System owner and users	Keeps keys out of the hands of thieves who can use such keys and cards to easily access secure areas.	Active key and card management are vital aspects of a protection program. Requires discipline, time, effort, and organizational skills.

#	Response	Source and further information	Who is responsible	How it works	Considerations
11	Use security to monitor and control access.	*Vulnerability Assessment of Physical Protection Systems,* Garcia, p. 87-112	Property owner	Security personnel detect, deter, delay, and respond to suspected or real security violations.	Security department personnel required. Costs money and ongoing commitment.
12	Conduct risk assessments on laptop and data to determine relative value and corresponding security measures.	*Information Asset Protection Guideline*, ASIS International, p. 11	Senior management	Laptop and data must be considered two separate yet inter-related assets. If non-vital information is stored on the laptop, then the laptop becomes the prime asset. If data is more vital and must be stored on laptop, then both assets must be protected equally.	There are a variety of protective strategies and the owner/user must determine the appropriate level of protection for the assets. There must be a consistent approach to data classification, which requires discipline. There may be other considerations to data beyond value of data.
13	Institute a security awareness education program.	*The Manager's Handbook for Corporate Security* Kovacich and Halibozek, p. 247-272	Senior management	By educating employees and contractors about their duties relative to asset protection, all staff can be utilized in protecting laptops and data.	An awareness program takes time, energy, commitment, and a champion in order for it to succeed.
14	Hold staff and management accountable for not following company policies.	"Laptop Lockdown" *The Wall Street Journal* McQueen, p. 1-3 *The Manager's Handbook for Corporate Security* Kovacich and Halibozek, p. 163-184	Senior management	Staff must be held accountable for following policies; otherwise policies are ineffective. Employees must follow established procedures and be taken to task if they do not.	Documentation is vital, for staff to be held accountable. Staff need written policies and procedures to follow. Staff must be educated regarding company expectations. Enforcing procedures will create a culture of protection within the organization.
15	Have documented and specific policies in place regarding responsible use of, and expectation for, protecting company equipment (laptop security guidelines).	*Information Asset Protection Guideline,* ASIS International, p. 12-14	Senior management	Protective strategies are most effective when they are consistent, valid, and in writing. It removes the guesswork.	Staff can be expected to follow written policies and procedures.

#	Response	Source and further information	Who is responsible	How it works	Considerations
16	Enforce procedures.	"Laptops Prove Weakest Link in Data Security" *The Wall Street Journal,* Levitz and Hechinger	Company management	Laptop and data will be protected to a higher degree when employees follow established guidelines.	Guidelines must be in writing, available, logical, reasonable, and auditable.
17	Establish and enforce property removal procedures.	*High-Rise Security and Fire Life Safety, 2nd Ed.* Craighead, p. 59	Company management	Property removal procedures should be developed and written.	All staff, including security, must be aware of the policy in order for them to follow and enforce it.
18	Investigate all theft and attempted theft incidents, as well as all data breaches.	*The Manager's Handbook for Corporate Security* Kovacich and Halibozek, p. 323-327	Company management	By investigating thefts and attempted thefts, the organization may find how, when, where, why, who, and what happened to ensure thefts or attempts will not happen again. Countermeasures can then be developed.	Someone with previous investigative experience is best suited to conduct an investigation. All answers may not be found.
19	Program elevators to wait in tower and not sit with doors open on ground floor.	*Laptop Theft in Commercial Buildings 2005 Survey* Best, et al., p. 19	Property owner	Stops unauthorized individuals from walking into elevators and waiting for them to move up into office space.	Programming change required of elevator software. Some elevator software may be too old to accept programming requirements.
20	Ensure that contractors are appropriately insured.	"Guard Force Operations, Part I" *Protection of Assets Manual,* p. 9-I-18	Client and contractor management	If insured contract staff do steal and are caught, the victim has the ability to sue for damages.	Staff have to be caught stealing.
21	Never leave laptop alone or unguarded.	"Mobile Defense Force" *Computer World* Wood, p. 33	Laptop owner/user	By having a guardian in direct view of the laptop at all times, it reduces opportunity for thieves to steal without being seen.	Can be inconvenient at times and requires constant attention by laptop owner to maintain vigilance.
22	Stay informed of emerging theft schemes.	"Preparation eases pain of stolen laptops" *eWeek* Hines, p. 25	Laptop owner/user	Provides education to users of how thieves are stealing laptops. Users can develop countermeasures to theft schemes.	Theft schemes evolve and change. Keeping informed requires work, time, and effort. This information then must be disseminated to other users.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
23	Keep laptops inconspicuous by using simple carrying cases.	"Mobile Defense Forces," *Computer World*, Wood, p. 33	Laptop owner/user	Helps laptop user maintain low profile as thieves conduct pre-theft surveillance. If thieves do not know if user is carrying a laptop, they are less likely to target that individual.	It can be difficult to hide the fact that a user is carrying/using a laptop. Thieves may not be deterred by not knowing exactly what someone is carrying.
24	Do not leave bags behind for thieves to carry laptops away in.	Kitteringham	Laptop owner/user	Thieves will conceal a stolen laptop if possible and they will use whatever is handy. Eliminating bags may reduce the number of laptops they are willing to steal at any one time.	Thieves may bring their own bags. Not all laptop thieves will be deterred by not finding bags to conceal laptops.
25	Put laptop paraphernalia such as docking stations, power cords, cables, away.	"Laptop lockdown," *Macworld*, Cook and Seff, p. 1	Laptop owner/user	Laptop paraphernalia signals that there are laptops in the vicinity. Thieves will break into drawers and cabinets looking for them.	It is not always convenient or easy to eliminate all traces of a laptop or accessories. Even eliminating all traces of the laptop may not be enough to dissuade the thief from looking. The absence of a desktop will indicate the use of a laptop.
26	Lock away tools and keys that can be used to cut cables, open drawers, etc.	Kitteringham	Laptop owner/user	Thieves will often look for tools at the location of the crime to assist them in the act.	Some thieves will be prepared by bringing their own tools to the location. However, there is no point making things easy for them.
27	Make department and/or employee responsible for laptops and replacing them.	"Laptop Lockdown," *The Wall Street Journal,* McQueen, p. 1-3	Company which owns the laptops	Often neither departments nor employees are held accountable for lost or stolen laptops. Making them accountable, in theory, means they will take more responsibility for protection.	May be difficult to hold individuals accountable. Depends upon labor laws, collective agreements, and/or company culture.
28	Secure devices when not in use.	*Laptop Security, Part 1, Preventing Laptop Theft,* Ryder, p. 1-4	Laptop owner/user	Laptops should be locked up when not in use. They can 'disappear' and be gone for a considerable time before they are noticed missing or reported missing.	Individuals, not departments or groups, should be made responsible for laptops to ensure devices are adequately looked after.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
29	Register laptop with manufacturer.	*Laptop Security Guidelines* http://labmice.techtarget.com/articles/laptopsecurity.htm	Laptop purchaser	An index card is usually provided upon the purchase of the laptop. All pertinent information requested should be provided. It identifies the owner of the laptop. If the laptop goes missing and later contact is made with the manufacturer, then it can be determined to be stolen. Identification can be made.	Nothing may come from identifying a laptop as being stolen. Registration must actually take place.
30	Arrest offenders, both laptop thieves and those receiving stolen goods.	*Pulling the Plug on Computer Theft Police Research Papers 101,* Whitehead and Grey, p. 16-20	Police	Police investigate crimes and arrest offenders.	Considerable amount of time and work required to successfully complete a case. Potential high cost of investigating. May be difficult to prove cases.
31	Prosecute offenders.	*Pulling the Plug on Computer Theft Police Research Papers 101* Whitehead and Grey, p. 24	Police and courts	Punishes offenders, and keeps them off the streets for a certain amount of time. May deter others.	Concentrated effort required between police, prosecutors, and judges. Offenders are sometimes not deterred by sentencing. Offenders share theft successes while incarcerated.
32	Seize stolen property from offenders.	*Pulling the Plug on Computer Theft Police Research Papers 101,* Whitehead and Grey, p. 23	Police	Recovery of laptops negates the effect of stealing them.	Identification often difficult as many property owners fail to record property. Potential to 'mix and match' equipment thereby making it difficult to prove ownership. Lack of a central database may inhibit property identification and recovery.
33	Ban known offenders from premises.	Panhandling *POP Guide #13,* p. 32	Security, property owners, police, judges, and probation officials	Banning offenders and arresting them if they come back to the property may avert thefts.	It is sometimes difficult to identify offenders. Banning may not deter some offenders. Confronting offenders may lead to potentially dangerous situations for security and property owners. Requires the cooperation of all parties.

#	Response	Source and further information	Who is responsible	How it works	Considerations
34	Target persistent offenders for arrest and prosecution.	Thefts of and from Cars in Parking Facilities *POP Guide #10* Clarke, p. 22 and 23	Police and prosecutors	A relatively small number of offenders can be responsible for a high number of incidents. Targeting persistent offenders may likely have an impact on overall incidents.	Concentrated effort required between police, prosecutors, and judges. Offenders are sometimes not deterred by sentencing. Offenders share theft successes while incarcerated.
35	Seek restitution.	*Encyclopedia of Security Management* Fay, p. 448	Laptop owner/user	Take away the financial incentive to steal.	Seeking restitution can be costly in time, effort, and human resources and may not result in success as often thieves do not have money or other assets.
36	Submit "Victim Impact Statements" to courts.	*Pulling the Plug on Computer Theft Police Research Papers 101* Whitehead and Grey, p. 24	Laptop owner/user	Courts must understand the financial impact thefts have upon the business community. This may lead to increased penalties.	Victim impact statements take some time to prepare and submit.
37	Monitor pawnshops.	*Handling Stolen Goods and Theft: A Market Reduction Approach Research Findings No. 69* Sutton, p. 3 and 4	Police	By monitoring pawnshops, police can help eliminate a source where thieves take their stolen goods.	Pawnshops are not the only receivers of stolen goods. Monitoring pawnshops may be time consuming. Can be effective if properly employed.
38	Share theft information, mode of operation, and theft activities between business and law enforcement.	*Pulling the Plug on Computer Theft Police Research Papers 101* Whitehead and Grey, p. 24	Property owners and law enforcement	By sharing information, business can better protect themselves while law enforcement can gather intelligence in advance of launching investigations.	Privacy issues may impede sharing of information. Either party or both may be hesitant about sharing intelligence and information. Positive working relationships must be built in advance.
39	A qualified person should conduct a lobby vulnerability assessment.	*Laptop Theft in Commercial Buildings 2006 Survey* Headley, et al., p. 31	Person(s) responsible for lobby	The lobby assessment identifies vulnerabilities that thieves can use to access office space.	The identification of vulnerabilities should lead to correcting them. This may likely cost money.
40	Search for your stolen laptop on the Stolen Computer Registry by entering your serial number.	"Stop! Laptop Thief!" *Time* Taylor, p. 71	Laptop owner	Access: Stolencomputer.org Enter your serial number to determine if your laptop was recovered by the FBI.	You need to record your serial number before the laptop goes missing.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
41	Have IT and facility security work together to secure data and device.	*Information Asset Protection Guideline* ASIS International, p. 9	Company management	Overlapping protective strategies must work in tandem.	Strategies are less effective if parties are not working as a team. Both departments must recognize that laptop theft is a serious issue. Both physical and electronic strategies must be made in tandem.
42	Encourage staff to monitor work areas for suspicious activity.	*Handbook of Loss Prevention and Crime Prevention, 4th Ed.* Fennelly, p. 73	Senior management	Alert staff must feel empowered in reporting suspicious activity to police or security.	There must be someone to report the suspicious activity to. There must also be a list of what constitutes 'suspicious behavior'.
43	Call building security or police when suspicious activity is identified.	*The Design and Evaluation of Physical Protection Systems* Garcia, p. 223-238	All employees	Staff must report suspicious activity when observed. It does no good to call several hours later.	Everyone: staff, police and/or security, must be prepared for 'false alarms'.
44	Challenge visitors.	*Laptop Theft in Commercial Buildings 2006 Survey* Headley, et. al., p. 21-22	All employees	Staff must be prepared to challenge unknown visitors to company space. Thieves often take advantage of the anonymity of large offices.	Often, legitimate visitors are moving about. Incorrect challenges can lead to confrontations. Staff must be prepared to deal with thieves who have been stopped and challenged.
45	Institute visible I.D. program for employees and visitors.	*Workplace Security Handbook,* p. 75	Business owner	Identify all legitimate users authorized to be on site through the effective use of pre-authorized credentials.	A process must be implemented whereby all place-users must wear identification. This includes an authorization process pre-approving place-users. In addition, a person or persons must be responsible to ensure that all staff adhere to the system. Appropriate sanctions must respond to those refusing to utilize the system.
46	Sign in all visitors.	*Workplace Security Handbook,* p. 76	Business owner	All visitors must report to a central location, provide identification of some sort for verification, then be provided with visitors' badges.	There must be a process in place for verifying identification, i.e. the person is who they say they are.

#	Response	Source and further information	Who is responsible	How it works	Considerations
47	Escort all visitors.	*Workplace Security Handbook,* p. 76-77	Person being visited	Preferably, those whom visitors are meeting must escort visitors.	An authorization process system must be in place whereby the employee meeting with the visitor must be able to be contacted and to also make them responsible for maintaining constant supervision of the visitor.
48	Do not leave visitors unattended.	*Workplace Security Handbook,* p. 76-77	Person being visited	Visitors must be escorted at all times.	Employees meeting with visitors must understand their responsibilities as they relate to company policies and procedures.
49	Report all thefts to security and police.	"Theft and Fraud Prevention" *Protection of Assets Manual* p. 11-1 to 11-18d, Chapter 11	Employees and senior company officials	Informing security and police alerts them that thefts are occurring. Countermeasures can be developed to protect company employees and property.	Some employees, especially if they are held personally accountable for lost or stolen laptops, may be hesitant about reporting incidents. Some companies feel stolen laptops are the cost of doing business and may choose not to report.
50	Monitor personal information if laptop is stolen. It has identity theft implications.	"Laptops Prove Weakest Link in Data Security" *Wall Street Journal* Levitz and Hechinger, p. 2	Company and/or individual who had personal information on stolen laptop	By monitoring personal information, people will be alerted if their identity has been compromised. The sooner one learns of the compromise, the sooner one can take steps to limit exposure.	Monitoring personal information requires time, effort, and money. It may be some time before compromised personal information has actually been accessed and abused.
51	Implement a reporting system for stolen and lost laptops.	*Security and Life Safety for the Commercial High-Rise,* Kitteringham, p. 32	Company senior management	Often, staff do not know how or where to report a laptop theft. Without a system for recording and responding to incidents, security or senior management may be inconsistent in their responses.	Thought must be given to creating a reporting system. Senior management or security must be prepared to respond to reported incidents.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
52	Educate contractors to assist.	"Data Confidentiality in an Electronic Environment" *The CPA Journal* Louwers & VanDenburgh, p. 26	Employees who work with contractors. Senior Management is responsible to develop education material	Clarifies expectations for contractors as to what policies and procedures are relative to laptop security.	Policies and procedures must be developed first. Employees must be given responsibility to educate contractors. Contractors and employees must be held accountable for following them.
53	Train employees in protecting data and laptop devices.	"Data Confidentiality in an Electronic Environment" *The CPA Journal*, Louwers & VanDenburgh, p. 26	Senior company management	Staff must be educated to help protect data and laptop devices.	An education program must be developed, implemented, effective, and reinforced.
54	Institute or increase security guards' patrols.	*Handbook of Loss Prevention and Crime Prevention 4th Ed.* Fennelly, p. 253-265	Senior company management	Provides a visible deterrent to potential laptop thieves. The physical presence of uniformed officers adds a layer of security.	There are financial and operational considerations when instituting or increasing security patrols. Some staff may feel threatened that their worksite requires uniformed security officers. Other employees may feel increased feelings of safety and security.
55	Conduct audits on laptops regularly (daily, weekly, monthly) to ensure they are being used appropriately or are still in place.	"*Cyber Traps: An Overview of Crime, Misconduct and Security Risks in the Cyber Environment*" George, p. 4	Security staff	While conducting their company rounds, security staff makes a detailed list of all laptops left out unprotected. This list is passed onto senior management, who bring it to the employee's attention.	Staff need to be educated about the existing company policy. They also must be given the appropriate tools to protect the laptops after hours. Further, employees must be encouraged to follow the rules.
56	Implement policies and standards regarding information and laptop device protection.	"Data Confidentiality in an Electronic Environment" *The CPA Journal* Louwers & VanDenburgh, p. 26	Senior management	Creates expectations and checklist for employees to follow.	Considerable thought must go into developing policies and standards to ensure they are appropriate, effective, and fair. Staff must be informed and kept updated on a regular basis.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
57	Restrict access to sensitive data.	"Data Confidentiality in an Electronic Environment" *The CPA Journal* Louwers & VanDenburgh, p. 26	Senior management	A primary rule of protection is to first ensure that as few people as possible know what the asset is and where it resides. It is far easier to protect something that no one knows exists.	There must be policies and procedures in place and enforced. The challenge of protecting data is that it is so easy to move around. Data is often valuable only because it can be accessed.
58	Purchase laptop theft insurance.	What is laptop insurance? http://www.wisegeek.com/what-is-laptop-insurance.htm	Laptop owner	Insurance used if laptop is stolen.	Like other kinds of insurance, there are always conditions, which must be thoroughly investigated before insurance is purchased.
59	Post instructions: "Private property" "Inspect badges" "Lock up your valuables" "Unauthorized entrance not allowed" "All visitors must report to Reception"	"Laptop Theft in the Commercial High-Rise" Kitteringham	Senior management	Posting instructions reinforces rule-setting for both employees and thieves. It sends a message to both about the level of security in place.	There may be mixed feelings. Some employees may object to the messages as they feel they create a hostile or unsafe environment.
60	Consider having employees carry laptops instead of checking them or leaving in hotel rooms.	"Protecting Information on Laptops, PDAs, and Cell Phones" Wilson, Web, Frank and Charron, p. 3	Employee	The laptop is removed entirely from the workplace.	Laptop may be stolen on the way to or from the office. May be inconvenient to take laptop home every night.
61	Mark more than one location with company logo	"The Incredible Shrinking Laptop" Access Control & Security Systems Emigh, p. 2	Person implementing program	Company logo should be firmly attached in more than one location to make it more difficult for thief to remove.	Thief may not care. Logo may not be effective. The laptop may look less attractive to employees.

Appendix H: Implementing Electronic Security Measures— 21 Strategies

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
1	Implement password protection on files.	"Securing Laptop Data Against Losses," *Security Management* Piazza, p. 37	Laptop owner/ user	Denies access to files without password.	People may forget password or fail to activate file protection system. Is inconvenient and subject to defeat.
2	Install product which, if activated, will physically destroy the hard drive.	"This Stolen Laptop Will Self-Destruct in 5 Seconds" *PC World,* Brandt, p. 46	Property owner	'Dead on Demand' technology contains software which detects tampering, and a canister filled with a corrosive chemical.	A very drastic solution, which will not allow the data owner to retrieve data. It will be destroyed. As with any solution, it needs thorough investigation to ensure it will work as promised.
3	Back up data off laptop drive regularly.	"Preparation eases pain of stolen laptop," *eWeek*, Hines, p. 25	Laptop owner/ user	Data must be saved and backed up regularly away from the device. In case of theft, data is not lost.	Requires discipline to back up regularly. Does not stop data from the laptop from being accessed and compromised.
4	Install GPS (Global Positioning System) monitoring.	"Data Confidentiality in an Electronic Environment" *The CPA Journal*, Louwers & VanDenburgh, p. 26	Laptop owner	In the eventuality of a loss, GPS can be used to locate the device.	Installation will cost money. May not be 100% effective in retrieving laptop. Someone must physically retrieve the laptop. GPS does not work everywhere.
5	Implement automatic data auditing capability.	"Risky Business" *HR Magazine* Roberts, p. 71	Senior management	Software monitors laptop usage when it is on the company network. Tells how it is being used and if there is data that should not be on it.	As with any software, there are administrative issues. Software must be purchased and tested. May be issues of 'Big Brother' monitoring. Organizational culture or collective agreement may pose challenges. Training is required, as are policies and procedures.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
6	Maintain specific records of laptops including receipts, make, model, serial number, user manual, and warranty card.	*Pulling the Plug on Laptop Theft Police Research Series Paper 101* Whitehead and Grey, p. 25	Laptop purchaser	Records can be used in the recovery of stolen laptops.	Records must be kept in a secure place but accessible when required.
7	Password protect device using complex alphanumeric passwords, changed regularly.	"Preparation eases pain of stolen laptop" *eWeek*. Hines, p. 25	Laptop owner/ user	Password must be used in order to be effective.	People often fail to activate password protect. Passwords can be defeated.
8	Encrypt hard drive.	"Locking up the Laptops" *Chronicle of Higher Education* Kiernan, p. 1–4	Laptop owner	Hard drive encryption activated so if incorrect passwords are entered, data stays encrypted.	Installing software can be complex and time consuming. Requires dedicated staff to supervise system. Users can forget passwords. There are various software available. All must be assessed before implementation. Encryption can be expensive. Data can be lost if user makes errors. Software failures can cause loss of data. Key management vital. If machine is stolen when it's running, thief may be able to access files. Machine is useless to thieves unless they swap out drive or reformat it. Loss of key will make it difficult to access information by legitimate users/owners. Some encryption programs are not user friendly and may lead to people not using it.

#	*Response*	*Source and further information*	*Who is responsible*	*How it works*	*Considerations*
9	Install software that dials a central monitoring station if activated and reports IP address.	"Protecting Campus Data" *University Business* Angelo, p. 75-76	Laptop owner	If stolen then connected to the Internet, laptop will call automatically to a central monitoring station providing IP address.	Separately-purchased software may be required. Some new laptop manufacturers are installing it in factories. Laptop must be connected to the Internet for it to dial central monitoring station. Police services are required to retrieve laptops. Monitoring services require fees.
10	Install biometric protection on USB thumb drive to secure against unauthorized access.	"Stay Secure at Home and on the Road" *PC World* Bass, p. 39	Laptop owner/ user	A USB biometric fingerprint reader allows only those preapproved to access the files on the laptop.	Devices have varying prices. Can still be defeated. Lost or stolen readers make accessing the files difficult. Fingerprint reported to be relatively easy to copy. May reject legitimate thumbprint.
11	Install BIOS password.	"Locking down sensitive data" *The CPA Journal* Louwers and VanDenburgh, p. 27	Laptop owner	Prevents the laptop from booting without a password.	Can be bypassed by removing hard drive or battery. Methods of bypassing BIOS easily found on Internet.
12	Activate login password.	Protection Information on Laptops, PDA's, and Cell Phones Wilson Web Frank and Charron, p. 1–4	Laptop owner	Prevents access to laptop programs. Password lockout program should be activated to ensure that, after only so many attempts to enter a password, the computer locks up and sends a help message to the IT department.	Methods to bypass passwords easily found on Internet. Older software programs do not have password protection. Employees must be encouraged not to choose simple passwords. Hackers can use dictionary programs to crack passwords. "Shoulder surfers" watch for people entering passwords.
13	Install 'kill' switches to erase data remotely.	"Protecting Campus Data" *University Business* Angelo, p. 75–76	Laptop owner	If stolen laptop is monitored and connected to the Internet, data from hard drive can be erased remotely.	Laptop must be connected to the Internet.

#	Response	Source and further information	Who is responsible	How it works	Considerations
14	Install software to remotely deactivate device requiring repair, and activate "stolen property" message.	"Protecting Campus Data" *University Business* Angelo, p. 75–76	Laptop owner	Laptop can be remotely deactivated so thief will take it to a repair shop. Upon attempts to repair, a message declaring the laptop to be stolen will activate.	Laptop must be connected to the Internet. Thief must take laptop into repair shop. Repair shop must inform authorities.
15	Render machine unusable via endless reboot.		Laptop owner	Laptop can have program installed.	Methods to bypass can easily be found on Internet.
16	Use a biometric voice identification system to activate laptop.	"The Incredible Shrinking Laptop" *Access Control & Security Systems* Emigh, p. 3	Laptop owner/ user	Voice-activated system acts much like USB fingerprint scanner.	All biometrics are subject to multiple conditions. Biometrics are rapidly improving but not perfect. Thorough investigation required to determine if solution suits users.
17	Ensure that all software patches are installed regularly.	The High Cost of Laptop Theft http://www.absolute.com	Laptop owner/ user	Allows all up-to-date security programs to be utilized to their utmost.	Requires discipline to update regularly. Someone must be identified as responsible.
18	Use a removable hard drive.	Protection Information on Laptops, PDAs, and Cell Phones Wilson, Web, Frank, and Charron p. 3	Laptop owner/ user	The hard drive can be removed from the laptop and kept separately.	Potential for the hard drive to be stolen or lost. Hard drive must still be fully protected.
19	Use an external encryption device.	"The Incredible Shrinking Laptop" *Access Control & Security Systems* Emigh, p. 3	Laptop owner/ user	Device plugs into USB. When device is pulled from laptop, screen goes blank while operating system works in background.	Thorough investigation required to determine user friendliness, and whether encryption provides an appropriate level of security.
20	Install software that allows camera to take photo of thief using laptop.	"Securing your laptop against theft" *Business Week Online* Hesseldahl, P. 4-4	Laptop owner/ user	Every few minutes, a photo of the person using the laptop is taken.	Needs a camera in working order connected to the laptop. May only work on certain brands. Taking a photo will not retrieve a laptop, but will identify thief.
21	Install RFID tags for asset protection.	Chipping of Goods Case Study: Laptop Computers Home Office	Laptop owner/ user	With RFID readers connected to the access control system, access to exit with a tagged laptop is denied without appropriate authorization.	Installation requires infrastructure of hardware, software, and procedures for it to be effective. Further exploration of anyone wishing to implement is strongly suggested. According to the study conducted, was highly effective in its first year of operation.

Appendix I: Security Awareness Employee Sign-off Sheets

Procedure:

Staff members are expected to read and follow the [company's name] Laptop and Data Protection Policy. Each employee is responsible to learn and become familiar with company and departmental expectations.

Laptop User

All employees using portable laptop devices shall abide by all written documentation. Laptop users are required to read, understand, and abide by all procedures as they relate to protecting the laptop and the information in it. Upon completion of review of this procedure, the employee shall sign off on the [company's name] Laptop Device and Data Protection Policy.

I,_____ ,(printed name of employee) have read and understand the responsible use and protection guidelines as they pertain to me.

Date: _____

Signature:_____

Department Manager

Person designated with the responsibility to ensure that their staff members who are assigned laptop computers abide by all written documentation. Department managers are required to read, understand, and abide by all procedures as they relate to protecting the laptop and the information on it. Upon completion of review of this procedure, department managers should sign off on the [company's name] Laptop Device and Data Protection Policy.

I, _____ ,(printed name of employee) have read and understand the responsible use and protection guidelines as they pertain to me.

Date: _____

Signature:_____

Senior Management

Senior managers designated with the responsibility to ensure the Laptop Device and Data Protection Policy is developed, implemented, and followed; and that all staff assigned various responsibilities abide by all written documentation. Senior management is required to read, understand, and abide by all procedures as they relate to protecting the laptop and the information on it. Upon completion of review of this procedure, the senior management representative shall sign off on the [Company's Name] Laptop Device and Data Protection Policy.

Senior managers are responsible for mandating written guidelines on:

- Mobile data
- Proprietary data
- Employee responsibility towards laptops and data

Senior managers should also create a security awareness environment that includes:

- Documentation
- Education
- Training

I, _____, (printed name of employee) have read and understand my responsibility towards ensuring the creation and implementation of the use and protection guidelines as they pertain to me.

Date: _____

Signature:_____

Facility Security

Persons designated with the responsibility for the physical protection of portable devices shall abide by all written documentation. Facility security personnel are required to read, understand, and abide by all procedures as they relate to protecting the laptop and the information on it. Upon completion of review of this procedure, facility security personnel shall sign off on the [Company's Name] Laptop Device and Data Protection Policy.

Facility security personnel are responsible for the following:

- Obtaining senior management support
- Creating and providing physical and electronic security guidelines
- Implementing physical and electronic security measures
- Educating users through security awareness training
- Conducting periodic audits
- Updating security guidelines as required

I, _____,(printed name of employee) have read and understand the expectations of and responsible use and protection guidelines as they pertain to me.

Date: _____

Signature:_____

Information Technology (IT) Security

Persons designated with the responsibility for the electronic protection of portable devices shall abide by all written documentation. IT security personnel are required to read, understand, and abide by all procedures as they relate to protecting the laptop and the information on it. Upon completion of review of this procedure, IT security personnel should sign off on the [Company's Name] Laptop Device and Data Protection Policy.

IT security personnel are responsible for the following:

- Obtaining senior management support
- Creating and providing physical and electronic security guidelines
- Implementing physical and electronic security measures
- Educating users through security awareness training
- Conducting periodic audits
- Updating security guidelines as required

I, _____, (printed name of employee) have read and understand the expectations of and responsible use and protection guidelines as they pertain to me.

Date: _____

Signature:_____

Appendix J:
Laptop Incident Reporting Form

The following three-part form should be used to report the loss and eventual recovery of laptops.

Section A should be used by victims reporting the loss of the laptop. They should know who to report the theft to, what information was on the laptop, when they were first aware that the laptop was missing, and the circumstances surrounding the loss/theft.

Section B should be filled out by the person to whom the loss is reported. That person should be aware of the security procedures in place for the missing laptop and the data on it.

Section C should be filled out by the recovery team after the laptop is secured.

Section A: To be filled in by victim reporting the loss:

Date: _____ Name of report taker: _____

Name of victim: _____ Date reported stolen: _____

Description of laptop with serial number and other identifying marks:_____

_____

_____

_____

_____

_____

Location where laptop was lost: _____

_____

_____

_____

_____

Circumstances of loss:_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Signature of person submitting report: _____

Date: _____

Section B: To be filled out by security personnel or senior manager who receives the report of the laptop loss.

Security measures in place:

Electronic: _____

_____

_____

Physical: _____

_____

_____

Procedural: _____

_____

_____

_____

Classification of data on laptop: _____

_____

_____

_____

Specific files with description of information on laptop: _____

_____

_____

_____

Does data reside elsewhere? (If so, provide location and file name) _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Signature of person submitting report: _____

Date: _____

Section C: To be filled out by the recovery team:

Recovery team members: _____

What implemented security measures will facilitate recovery?

_____

_____

_____

Who will facilitate recovery? _____

_____

Has local law enforcement been alerted and called in to investigate? What actions have they taken?

_____

_____

Has senior management been alerted? _____

_____

_____

What is the (potential) scope of the laptop loss? _____

_____

_____

What is the (potential) scope of the data breach? _____

_____

_____

_____

Person authorizing decision to terminate: _____

_____

_____

Actions taken: _____

_____

_____

_____

Disposition (laptop destroyed, recovered or irretrievable?): _____

_____

_____

_____

Decision to terminate recovery, with reason(s)? _____

_____

_____

Signature of person submitting report: _____

Date: _____

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 36,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine—*Security Management*—ASIS leads the way for advanced and improved security performance.

ASIS International Foundation

The ASIS International Foundation, a 501(c)3 charitable organization, provides funding and manages endowments for a wide range of academic, strategic, and professional development activities. The purpose of the Foundation is to enhance the security profession worldwide by establishing, developing, delivering, and promoting programs that advance security through education, research, and training. Foundation scholarships ensure that those pursuing a career in security management are able to realize the highest academic achievements. Financial contributions from individuals, chapters, companies employing ASIS members, and corporations with an interest in security support the Foundation.

ASIS FOUNDATION™

1625 Prince Street
Alexandria, VA 22314-2818
USA
703-519-6200
Fax: 703-519-6299
www.asisonline.org